1-2016

Empirical Assessment of Cyber Harassment Victimization via Cyber-Routine Activities Theory

Sinchul Back

Empirical Assessment of Cyber Harassment Victimization via Cyber-Routine Activities Theory

A THESIS

Presented to the Department of Criminal Justice

Bridgewater State University

In Partial Fulfillment of the

Requirements for the Degree

Master of Criminal Justice

Sinchul Back

Bridgewater State University

January 2016

Empirical Assessment of Cyber Harassment Victimization via

Cyber-Routine Activities Theory

Thesis Presented

By

Sinchul Back

Content and style approved by:

Dr. Kyung-shick Choi
(Chairperson of Thesis Committee)

Dr. Mitch Librett
(Member)

Dr. Robert Grantham
(Member)

Abstract

Over the decades, the advance of the social networking sites and computer-mediated communication tools has facilitated cybercriminals to expand their scope of criminal activities from the physical world to the virtual realm. Cybercriminals can easily leverage the Internet to operate sexual crime such as cyber-harassment. This study aims to empirically assess cyber-harassment victimization in South Korea via Cyber-Routine Activities Theory (2008). Cyber-Routine Activities Theory includes five major tenets: 1) digital capable guardianship, 2) motivated offender online, 3) suitable target online, 4) online risky behavior, and 5) online vocational and leisure activities. Data were derived from the 2013 Korean Institute of Criminology's survey, which is dedicated to examining Koreans' social networking sites usages and its related online behaviors. The results suggest that risky online behaviors and inadequate cyber security on social networking sites substantially contribute to the overall cyber harassment victimization.

Acknowledgements

I would like to thank Dr. Kyung-shick Choi for his invaluable mentorship. During my time as a graduate student at Bridgewater State University, he has taken me under his wing and helped me to immensely better myself as a scholar, professional, and improve myself as a person in general. He did this not only by teaching me as a professor, but by guiding me and creating great opportunities for me as a mentor. It has been a wonderful experience working with him and learning from him as a professor and mentor. I am honored to be his 1st Korean mentee at BSU.

I want to thank Dr. Mitch Librett and Dr. Robert Grantham for their sincere advice. I truly appreciate their willingness to help me, not only by working with me as committee members on this thesis, but for shaping me as a scholar and by helping me plan for my future endeavors.

I would also like to thank Dr. Carolyn Petrosino for being an amazing professor during my directed study at Bridgewater State University. Her support has definitely helped me get to where I am today. She believed in me and helped create some fantastic opportunities for me along the way.

I wish to thanks, Dr. Faviana Olivier, professor, at Northeastern University, for her encouragement, which made me pursue my Master's degree.

The entire faculty and staff, Moira O'Brien, in the Criminal Justice Department has been great to me during my time at Bridgewater State University. I would like to thank everyone in the department for making my experience a memorable one.

I am grateful to many individuals who shared their experiences and insights, Senator Jinha Hwang, Senior Officer Jaehwi Park, Dr. Seokmin Shin, Dr. Kyungseok

Choo, Dr. Yongeun Sung, Gyobeom Kim, Congressman EungCheol Yun, and Dr. Minseok Kim.

There were many people who showed me tremendous support during this process. I would like to thank all my family in South Korea (parents, mother-in-law, sister-in-law, brother-in-law, Inyong Back, and Bocheon Kim) and thank all my friends (Dr. Byeongoh An, Kiho Kim, Dongjin Park, Hyunjin Lee, Hyunmin Yang, Sangjin Lee, Jackelyn Wilson, Timothy Scott, Ruban Ortiz, Corrie, and Danielle) that helped me along the way.

I would like to take this opportunity to thank the Earl family in Upton, Massachusetts, who shared their experiences and lives.

Finally, my very special thanks to Hyobin Sung, my wife and Ryan D. Back, my future son. I fully acknowledge that her dedication and love toward my academic life was invaluable and has shaped me to be the person I am today. Thank you for everything.

Table of Contents

CHAPTER 1

INTRODUCTION

After the advent of the information era, a number of cybercrimes have been committed by cybercriminals in South Korea. In the beginning of the information era virus attacks were dominant in the scene of crime in cyberspace. Thompson (2004) stated that the main types of cybercrime or computer crime were the basic level of computer virus attacks instead of online interpersonal crime (cyber-harassment, cyber-stalking, and online sexual crime) until the 1990s. Cybercrime became more complicated with the highly advanced intimating skills such as the stuxnet virus, distributed denial of service (DDOS) attack, ransomware, scams, identify theft, Internet fraud, and online interpersonal crime (Internet Crime Report, 2014). Choi (2015) describes that the development of IT technologies facilitate cybercriminals to obtain more efficient toolkits such as high-speed Internet connection speed, decrypted software, and malware programs.

In addition, due to the advanced technologies - Internet services, computer systems, social networking services, and smart phones - online users are actively engaging in utilizing social networking sites such as Facebook, Twitter, KakaoStory, and Instagram. Social networking sites (SNSs) connect us with friends and family, sharing our personal interests and experiences (George, 2014). However, cybersecurity professionals argue that the next wave of cybercrime will be committed through social media channels (George, 2014). The number of online interpersonal crime, especially cyber-harassment, has been consistently increased in cyberspace. It is considered a side effect of cutting-edge technology that threats South Korean citizens. According to the

Korean National Policy Agency (KNP, May 2015), 7,873 perpetrators were arrested for cyber-harassment in 2013. Cyber-harassment causes victims to experience physical or emotional stress, a sense of helplessness, fear for victims, and even suicide (Bocij, 2004; Finn, 2004; Wall, 2001; National Center for victims of crime, 2007; Bossler & Holt, 2010).

Cyber-harassment not only affects Korean society, but it is also a controversial issue for the world. Due to the features of cyberspace – no limitation of temporality and spatiality – cyber harassment and online prostitution are proliferating across the world. Hence, the international and national levels of law enforcement are demanded to prevent cyber harassment. It seems that law enforcement struggles to deter cyber harassment (Hazelwood & Koon-Magnin, 2013). In addition, most online users may not be fully aware of cyber harassment.

While cyber harassment became a controversial and transnational issue in South Korea, few studies have been conducted to investigate cyber harassment. Thus, this study aims to empirically assess cyber-harassment victimization in South Korea through the application of Cyber-Routine Activities Theory.

The following sections will present an overview of SNSs and a cyber harassment case in order to have better understanding of the cyber harassment phenomenon in South Korea.

Background of Cyber-harassment on SNSs

Social Networking Sites

Social Networking Sites launched to be operated for certain purposes such as communication and interaction among online users in the mid-1990s (Yoon & Park, 2014). Boyd and Ellison (2008) found that the first SNS (SixDegrees.com) was launched in 1997 and the main function was to enforce one's social connections between seller and buyer for business markets. Furthermore, SNSs became popular with diverse activities and entertainment in the 2000s (Boyd & Ellison, 2008). In recent years, millions of users have used SNSs such as KaKaoStory, Facebook, and Twitter in South Korea (Boyd & Ellison, 2008).

SNSs are defined as web-based services that provide opportunities to reinforce pre-existing social networks and help strangers connect to each other by allowing them to share interests, political views, and activities (Boyd & Ellison, 2008; McCuddy & Vogel, 2014; Yoon & Park, 2014). After joining social networking sites, an individual is able to set his or her personal information, which typically include age, location, interests, cell phone number, e-mail address, etc. (Boyd & Ellison, 2008). SNSs can connect with communication tools such as smartphone connectivity, blogging, and photo/video-sharing (Boyd & Ellison, 2008). They provide a mechanism for online users to leave messages to their friends' SNSs as well as using private messenger functions similar to webmail (Boyd & Ellison, 2008).

According to Statista (2015), the statistics indicate that there are 1.79 billion social network users around world as of 2014. Also, the statistics show that 27.9 million social network users in South Korea and 173.6 million social network users in the United

States registered as active users in 2014 (Statista, March 2015). Based on the 2015 statistics data from Statista, the majority of social network users in South Korea were interested in using Facebook, Twitter, KaKaostory, and Cyworld; the social networking users in the United States mainly favored the use of Facebook, Twitter, Instagram, and Pinterest in 2014 (Statista, 2015 March). Two major SNSs (e.g., KaKaoStory and Facebook) in South Korea will be introduced in this paper in order to understand the Koreans' SNS usages.

KakaoStory was invented in 2012 as a mobile-based web service, which has features such as uploading multimedia contents, built-in blogging, and instant messaging technology (Yoon & Park, 2014). The number of KaKaoStory users dramatically increased and there were approximately 44 million users in 2014; moreover, it is currently one of the most popular SNSs in South Korea (Yoon & Park, 2014). Generally, KaKaoStory is a mobile-specific SNS, which allows users to actively interact with each other within the SNS applications; however, the mobile interaction can be confined with KaKaoStory's security settings. In other words, the limited mobile interactions with the security settings may reduce the victimization rates of cybercrime (Jagatic et al., 2007).

Facebook was launched in 2004 as both a web-based service and mobile-based web service. Facebook allows users to do the following: share personal profiles, leave messages, blog, and share photo/videos (Kim et al., 2014). Online users can decide their Facebook's cyber security level, which prohibits accessing from unknown online users. Facebook is the most popular SNS around the globe; however, it is ranked second following KaKaoStory in South Korea. The number of Facebook users was estimated to be approximately 10 million in 2014.

In a few ways, significant differences exist between online social networks and conventional social networks (Acar, 2008; McCuddy & Vogel, 2014). First, the size of online social networks is typically greater than traditional social networks (McCuddy & Vogel, 2014). McCuddy and Vogel (2014) suggest that whereas the quality of relationships in both the physical and the cyber world is similar, online users can actively connect with important friends via SNSs rather than physical world peer group connection. According to Pempek's et al. (2009) research, the majority of online users spend more time observing other users' content on SNSs rather than posting their own content on SNSs. Without doubt, social networking sites strengthen social networks through the interaction among individuals. On the other hand, social network users are more likely to be exposed to deviant acts online. For example, online users can be victims of cyber-harassment or stalking by cybercriminals at all times of the day regardless of the proximity and temporality (Holt & Bossler, 2014; Marcum, 2010; McCuddy & Vogel, 2014).

Unfortunately, general SNS users have still not recognized the overall seriousness of cybercrime victimization, especially with cyber-harassment. It is very important to protect us from cyber-harassment, therefore, our society is demanded to shed light on the seriousness of cyber-harassment. Nonetheless, to date, little research has been conducted on this topic. As a result, new criminological terms and conceptual definitions with cyber-harassment will be discussed in the next section.

Cyber-harassment on Social Networking Sites

With the pervasive growth of Internet and computer communication systems, cyber-harassment has become a serious issue in South Korea (Hwang, October 2015). While law enforcement in South Korea has been attempting to implement procedures and policies to reduce online criminal activity, including cyber-harassment and cyber-stalking, it appears that there is still a lack of an agreed upon definition of both cyber-harassment and cyber-stalking.

In South Korea, there are two pieces of legislation that pertain to these types of illicit behaviors: Korean Telecommunication Act of 2011 and Korean National Sexual Offenses Law, both of which attempt to regulate cyber-harassment. Under the Korean Telecommunication Act of 2011, cyber-harassment is defined as an act or behavior that repeatedly terrorizes or threatens an individual via unwanted e-mails, instant messages, or other means with the intention of harming that person (Hazelwood & Koon-Magnin, 2013). According to the Korean National Sexual Offenses Law, cyber-harassment is a behavior in which a perpetrator sends unwanted e-mails, instant messages, pictures, and video files via SNSs with the intent to cause sexual shame and aversion.

In general, cyber-harassment can be interpreted as a delinquent behavior that repeatedly sends unwanted contents such as e-mails, instant messages, and sexually shameful pictures or video files (Holt & Bossler, 2009). These unwanted files may negatively influence a victim's life, especially their mental or emotional state (Kunz & Wilson, 2004). Kunz and Wilson (2004) explain that cyber-stalking is a common form of cyber-harassment. Thus, based on the two aforementioned Korean national laws, cyberstalking is regarded as a form of cyber-harassment. With that in mind, the

measurement of cyber-harassment victimization in this paper will include cyber-stalking variables due to the empirical nexus between cyber-harassment and cyberstalking. Some suggest that cyber-bullying is quite similar to cyber-harassment. However, this paper is not concerned with measuring cyber-bullying variables since the majority of cyber-bullying victimization tends to focus solely on children under age 18, rather than capturing the entire national population.

In order to have a better, more comprehensive understanding of cyber-harassment, the *Yoo v. Cho* case will now be represented as an explicit example of cyber-harassment that has recently occurred in South Korea. The purpose of sharing this case is to demonstrate how these crimes have proliferated, and the ultimate negative effect that they can have on victims. Yoo was the student of Cho in a high school in South Korea (KBSnews, September 2014; MKnews, January 2014). Yoo was in unrequited love with his teacher. Yoo had solicited his former teacher to date him, but Cho rejected him. After this rejection, Yoo dropped out of the school and spread a vicious rumor through email to high school staff that he was in a secret relationship with his former teacher, Cho (Lawtime, January 2014; MKnews, January 2014). He persistently stalked and harassed Cho offline and online. Yoo then attempted to rape his teacher but failed in February 2011 (KBSnews, September 2014; Lawtime, January 2014). He was later diagnosed with a psychological delusional disorder and has since received specialized treatment in a hospital (KBSnews, September 2014; Lawtime, January 2014).

This story did not end with Yoo's hospitalization. In fact, Yoo went on to study nursing in a U.S. college, but still remained fixated on his former teacher. After hearing a rumor that his former teacher was going to get married, Yoo began to become unraveled

psychologically and began looking for his former teacher (KBSnews, September 2014, Lawtime, January 2014). Yoo specifically tried to contact Cho's family and his friends, but had no luck. He eventually found Cho's personal information using the Internet where he then proceeded to harass and threaten to kill Cho, specifically using her SNSs — sending approximately four hundred unwanted e-mails (KBSnews, September 2014; Lawtime, January 2014). Yoo then took a leave of absence from nursing school in the U.S. and decided to visit Cho's actual office in South Korea. At first, he asked Cho to date him but she vigorously refused. Finally, out of his inability to win Cho's heart, Yoo murdered Cho in her office elevator (KBSnews, September 2014; Lawtime, January 2014).

A Seoul city prosecutor in South Korea charged the offender with homicide and both offline and online stalking. In July 2014, Yoo was sentenced to a thirty-five-prison sentence (KBSnews, September 2014; Lawtime, January 2014). It is important to note, this particular criminal case is only one example of hundreds of cases that has transpired in South Korea, further warranting a deeper understanding of this type of criminal behavior.

The next chapter includes two phases. Phase 1 presents routine activities theory and lifestyle exposure theory. Phase 2 presents cyber-routine activities theory along with a review of the relevant empirical studies designed to assess the tenets that apply to the cyber harassment victimization model.

CHAPTER 2

LITERATURE REVIEW

Although cyber-criminologists have attempted to assess the empirical tests of cybercrime in many countries, there are few empirical assessments on cyber harassment in South Korea. Therefore, the main purpose of this study is to empirically assess cyber harassment victimization via Choi's Cyber-Routine Activities Theory (2008).

In this chapter, traditional routine activities theory (Cohen & Felson, 1979), life-exposure theory (Hindelang et al., 1978), and cyber-routine activities theory (Choi, 2008) will be discussed. As a next step, certain tenets of cyber-routine activities theory – capable guardianship, online risky behavior, and online vocational and leisure activities – will be interpreted into cyber-harassment.

Routine Activities Theory

Cohen and Felson (1979) claimed that routine activities theory could explain why crimes occurred. Cohen and Felson's traditional routine activities theory consists of three major tenets: (a) motivated offenders, (b) suitable targets, and (c) the absence of capable guardianship (Cohen & Felson, 1979; Cohen, Felson, & Land, 1980; Felson, 1986, 1988; Kennedy & Forde, 1990; Massey, Krohn, & Bonati, 1989; Miethe, Stafford, & Long, 1987; Roneck & Maier, 1991; Sherman, Gartin, & Buerger, 1989). Cohen and Felson (1979) assumed that the likelihood of crime is increased when three tenets of routine activities theory are convergent in space and time (Akers & Sellers, 2013). Studies that examine routine activities theory often concentrate on general offending crime patterns reflecting the conjunction of these elements of crime (motivated offenders, suitable targets, and absence of guardians). Akers and Sellers (2013) stated that routine activities

theory is also employed to investigate specific types of offending, such as homicide, sex offending, robbery, burglary, and cybercrime victimization.

Hindelang et al. (1978) proposed the lifestyle exposure theory, which mainly focuses on the victims' daily social interactions, rather than concentrating on the characteristics of individual offenders or individual causal variables. Hindelang et al. (1978) found that individuals' vocational and leisure activities is directly associated with crime victimization. In short, Hindelang et al. (1978) asserted that differential lifestyle patterns are correlated with "role expectations, structural constraints, and individual and subcultural adaptations" (Choi, 2008; Hindelang et al., 1979, p. 245).

Cyber-Routine Activities Theory

Choi (2008) mainly argued that Cohen and Felson (1979) incorporated the lifestyle-exposure theory (Hindelang et al., 1978) into their routine activities theory by expanding upon the existent tenet: individual's vocational and leisure activities. In Cohen and Felson's (1979) view, target suitability is created and influenced by an individual's vocational and leisure activities, which reflect the individuals' routine activities such as social interaction and social activities (Choi, 2008). Also Cohen and Felson (1979) developed two other tenets – capable guardianship and motivated offender – and integrated these two tenets with the suitable target tenet from lifestyle-exposure theory. The theoretical integration is essential to help explain the new crime phenomenon. Choi (2008) argues that routine activities theory and lifestyle-exposure theory are originally not two disconnected theories, but that routine activities theory is extended from the lifestyle-exposure theory.

Choi (2008) developed cyber-routine activities theory in order to assess the computer-crime victimization reflecting both traditional routine activities theory and lifestyle exposure theory. Choi (2008) combines routine activities theory and lifestyle exposure theory. His conceptual model posits that digital-capable guardianship and online lifestyle directly influence computer-crime victimization.

Digital Capable Guardianship

Choi (2008) stressed that digital capable guardianship is one of the most crucial elements to prevent computer crimes. Digital capable guardianship is defined as a protection tool that helps online users secure themselves from cyber criminals. Choi (2008) clarifies that there are two types of digital capable guardians: physical digital guardians and cyber security guardians. The physical digital guardians – antivirus software, firewalls, and antispyware – protect the computer systems and personal assets against computer criminals. The cyber security guardian – security on SNSs and security applications on SNSs – protect online users against interpersonal criminals online. In related sense, cybersecurity is an essential feature (Archer et al., 2014) on SNSs, which can be prevented from misuse of personal data such as cyber-harassment, sextortion scams, and online prostitution. Both physical digital guardianship and cyber security guardianship are associated with target hardening to enforce the level of inertia from criminals. In the real world, lighting on areas, using locks, alarms and barriers are regarded as means of target hardening (Choi, 2008; Tseloni et al., 2004).

Recently, Choi (2008) has empirically assessed computer crime victimization by measuring the physical digital guardians. As an extension of the perspective, this study tests cyber-harassment victimization by measuring the degree of cyber security

guardianship. Holt (2011) similarly claimed that physical digital guardians have rarely influenced the victimization of interpersonal violence such as cyber harassment. Holt's statement was somewhat contradictory to the measure of digital capable guardians. The reason is that the digital capable guardian factor should not be limited with physical digital guardians – antivirus software, firewalls, and antispyware – which mainly influence computer crime victimization, not cyber-harassment victimization. In other words, cyber security guardians such as cyber security on SNSs and security application on SNSs must be measured for the accurate model of interpersonal cybercrime victimization, including cyber-harassment and cyberstalking.

Formal and Informal Capable Guardianship

Yar (2005) asserts that formal/ informal capable guardians seem to not effectively minimize the occurrence of cybercrime victimization. In other words, formal/ informal agents have difficulty in dealing with cybercrime. Other studies (Holt, 2009; Reyns, 2011) indicate that formal/ informal capable guardianship factors did not influence the rate of online sexual crime victimization, including cyber stalking and cyber harassment.

In general, most online sexual crime victims tend not to report their criminal incidents to law enforcement and SNS providers. According to the Korean Institute of Criminology (KIC) survey (2013), SNS users in South Korea have the lowest level of reliability for formal/informal guardianship to solve the cyber-harassment issue(s). With respect to formal guardianship, 180 of 1000 SNS users in the survey indicated that they have never reported cyber-harassment issue(s) to the police; 135 of 180 SNS users in the survey did not report it to the police because they believed that their victimization was

not serious; 28 of 180 SNSs users in the survey did not report it to the police because they did not feel like taking the time to report it. Only 3 of 1,000 in the survey who reported cyber-harassment issues were satisfied with the service of the police, but the offender was not captured. With regard to informal guardianship, 173 of 1000 SNS users in the survey did not report to SNS providers after cyber-harassment victimization on SNSs; 105 of 173 SNS users in the survey who did not report it to providers believed that their victimizations were not serious; 48 of 173 SNS users in the survey who did not report it to providers believed that they did not feel like taking the time to report it to providers. Only 12 of 1,000 SNS users reported the cyber-harassment issue(s) to providers; 8 of 12 SNS users who reported it to providers were not satisfied with the service of the providers; 4 of 12 users who reported it to providers were satisfied with the providers' solution for the cyber-harassment issue(s).

In short, there is no significant relationship between formal/informal guardianship and minimizing the occurrence of cyber-harassment victimization based on the previous studies by Yar (2005), Holt (2009), and Reyns (2011) and the descriptive analysis in this study. Therefore, this study will only focus on measuring digital guardianship in order to assess the accurate guardianship element for cyber-harassment victimization.

Motivated Offenders

According to cyber-routine activities theory (Choi, 2008), motivated offenders in the virtual world are a given situation. Individual cyber criminals are motivated by various factors (Grabosky, 2015). Moreover, Grabosky (2015) asserts that cyber criminals' motivation may be complex, or mixed. Plenty of motivated cyber criminals seek to catch valuable targets in the form of online users who connect to the Internet website with a lack of computer security level (Grabosky, 2015). Normally, hackers are motivated by their satisfaction of how they can control cyberspace and computer networking system (Grabosky, 2015). Hackers plant malicious viruses and worms on social networking sites or web forum sites to receive individuals' information when online users click a pop-up window without precaution (Choi, 2008; Piazza, 2006, p.54).

However, the characteristics of individuals engaged in the online interpersonal crimes (cyber-harassment and cyber-stalking) may be different from that of cybercrime perpetration in general (UNODC, 2013). Online interpersonal criminals search for attractive targets on SNSs or online dating sites. Cyber harassers and stalkers may seek to "exert power over their victims" via giving them fear (McGrath & Casey, 2002, p. 89). By increasing their knowledge of the victim, the perpetrator can terrorize and control them. Specifically, cyber harassers and stalkers utilize or post on SNS victims' personal information: cellphone numbers, addresses, e-mail addresses, personal preferences, and photos, including nude photos in order to threaten their victims' lives (McGrath & Casey, 2002). As a result, sharing the information online may place the victim in danger (Maras, 2015).

Suitable Target

Many suitable targets exist in the cyber world. Choi (2008) utilized Felson's VIVA (1998) assessment to explain the nature of suitable targets online.

Value. Yar (2005) states that the targets' value in cybercrime cannot be simply defined because the perpetrator's motivation or purpose to commit cybercrime is very complex (Choi, 2015). However, research indicates that the main targets of cybercrime are individuals, or an organization and cyber criminals attempt to gain digital properties such as digital information and codes. When individuals access the Internet, the valuable information and assets in their computer are exposed to computer criminals (Choi, 2008; Felson, 1979). The valuable targets online can be violated by a broad realm of perpetration such as trespassing, identity theft, cyber harassment, cyber stalking, or vandalism (Brikbeck and LaFree, 1993; Bernburg and Thorlindsson, 2001; Choi, 2015; Yar,2001).

Inertia. Yar (2005) and Choi (2015) state that inertia and suitability have an inverse relationship. When the level of the inertial resistance increases, the level of target suitability for cybercrime will be decreased. Choi (2008, 2015) argues that target suitability in the virtual world is more active than the physical world because cyber criminals' technologies and committing cybercrime skills are being advanced at a breaking rate when compared to the advancement rate of cybersecurity technologies (Yar, 2005; Choi, 2008, 2015). In other words, the level of inertia in virtual space is very low; pools of computer perpetrators and cybercriminals easily attack suitable targets online.

Visibility. According to Yar (2005), targets of cybercrime can be globally exposed and visible to cyber criminals in cyberspace. In other words, the characteristic of

visibility within the cyber-environment accelerate cyber criminals to find attractive targets and commit deviance "from anywhere in the world" (Choi, 2008, p. 21). Cybercriminals can obtain the digital data from online users by utilizing efficient tools such as I.P. Trackers or Password Sniffers, Spyware, and Scams software (Choi, 2008, 2015; Internet Crime Report, 2014).

Accessibility. The accessibility of crime targets is defined as the ability of cyber criminals to approach the target and then escape from the cybercrime scene without any difficulty (Choi, 2015; Kubic, 2001). Since national and international boundaries are not circumscribed in cyberspace, cyber perpetrators can access and get away from the scene of cybercrimes without limitation of time and borders.

Plenty of motivated offenders and suitable victims are at "zero distance" from all others in the virtual environment and online interpersonal crimes are remotely committed from across the country or even across the world (Yar 2005, p. 415; Hazelwood & Koon-Magnin 2013). With that in mind, motivated offenders and suitable target factors are apparently a fully given situation. Therefore, this study will not include the measurement of motivated offenders and suitable targets reflecting Choi's (2008) cyber-routine activities theory assumption.

Online Lifestyle

Choi (2008) linked the lifestyle exposure theory to cyberspace such as "vocational activities and leisure activities in cyberspace, online risk-taking behavior, and properly managing computer security systems" (p. 26). A person's vocational and leisure activities are the key factors to making him/her a suitable target (Choi, 2008). During online activities in cyberspace, individuals can persistently interact with other online users

through online toolkits and smartphone apps such as e-mail, online messengers, and SNSs. Also, the online users set up their own lifestyle by joining "various cyber communities based on their particular interests, such as cyber-café's, clubs, and bulletin boards" (Choi, 2008, p. 13). Similarly, the individuals may also join smartphone apps for dating and SNSs. They are more likely to be suitable targets for online sexual crime than someone who does not join such smartphone apps.

According to Choi (2008), online risky behaviors such as illegally downloading programs or media files and visiting unknown websites increased the students' risk of virus victimization (Reyns, 2011). Also, individuals who perform risk-taking behaviors on social networking sites are likely to become victims of cybercrime.

In addition, cyber-harassment is easily committed in the virtual world due to the features of cyber space. Sherman et al. (1989) argue that there is certain "hot spots" in the physical world where crimes routinely occur. Sherman et al. (1989) explain that the places - bars, liquor stores, bus depots, homeless shelters, downtown malls, and theaters - are regarded as the hot spots for crime in the physical world. Like the physical world's hot spots for crimes, Holt (2012) posited that there exist some hot spots in the virtual world. For example, online users who frequently go to hot spots (e.g., online dating sites, SNSs, and sexual web forum sites) are more likely to be victimized by cybercrime (Choi, 2005; Holt, 2007).

The Ashley Madison case is a representative example that demonstrates how online users and social networking service providers can jeopardize themselves in a hot spot (online dating site) due to their online risky behavior. In fact, the popular online dating service company, Ashely Madison, was hacked by cybercriminals who have

threatened to release the personal data of 37 million members of the site such as financial transaction information, user profiles, passwords, and nude photos (NewYorkTimes, July 2015). Cybercrime professionals analyzed that this case was a phishing attack: An employee at Ashley Madison may have clicked a link that allowed a hacker to collect the customers' information from the company database (BBC, July 2015).

Similar to cyber-routine activities theory, other cyber criminologists such as Holt, Reyns, Marcum, and Hinduja have conducted risky online lifestyle studies that contribute to online sexual crime victimization. Holt (2009) mainly focuses on using a cyber-routine activities framework to examine the causal factors for online harassment victimization for college students and his study found that risky online activities increased college students' risks for online harassment (Holt, 2009; Reyns et al., 2011). Reyns (2012; 2013) also empirically tests the cyber-routine activities theory for assessing cyberstalking and cyber-harassment. He found that online risk-taking behavior contributed to the phenomenon of cyberstalking victimization.

This study seeks to analyze the behaviors of Korean SNS users regarding the core concepts of the following statements: "what you are doing to protect yourself, where you are, what your behaviors are" during online activities (Mustain & Tewksbury, 1998, p. 852; Choi, 2008). Unlike the previous studies, that used physical digital guardianship measures, this study measures specifically cybersecurity guardianship measures on SNSs in order to assess interpersonal crime victimization online.

CHAPTER 3

METHODOLOGY

This chapter presents the research methods that are used to empirically assess the cyber harassment victimization of South Korean citizens. The specific sampling techniques, procedures, and the method of data analysis are presented below.

Sampling and Procedures

This study utilizes secondary data from the 2013 Korean Institute of Criminology (KIC) survey. Survey research is a research design that reflects a standard tool, as "a systematic way to take measures from a large number of units" (Maxfield & Babbie, 2011, p. 256). Also, survey research can be utilized for descriptive, explanatory, exploratory, and applied research (Maxfield & Babbie, 2011). The unit of analysis for this study is individual online users in South Korea.

The KIC's original survey was designed to examine Koreans' SNS usages and its related online behaviors. Individual in urban areas: Seoul, Gyeongki, and Incheon in South Korea were chosen to participate in the survey. The sample consisted of 1000 SNS users from age 14 to age 59 in South Korea because these people were able to fully understand survey questions and were the majority to use social networking sites. 11.7% of respondents were in their teens; 31.4% of respondents were in their 20's; 28.5% of respondents were in their 30's; 19.4% of respondents were in their 40's; and 9% of respondents were in their 50's (KIC, 2014). The survey was conducted by the Korean Institute of Criminology from July of 2013 to August of 2013.

Hypotheses and Measures

The specific measures for the assessment of the cyber harassment victimization are demonstrated in this section. In that sense, the cyber-routine activities theoretical components (Choi, 2008; Cohen & Felson, 1979; Hindelang, 1978): (1) capable guardianship and (2) online lifestyles will be utilized to determine cybercrime victimization data that were collected from the Korean Institute of Criminology. The survey contained a series of questions gauging respondents' online behavior, exposure to online risk-taking behavior, self-reported victimization, and demographic characteristics.

With that in mind, the current study seeks to address the major deficiencies in the criminological literature, especially as it pertains to cybercrime victimization through SNSs. The specific hypotheses in this study include:

Hypothesis 1. Strict cybersecurity settings on SNSs minimize cyber-harassment victimization.

Hypothesis 2. Active engagement in vocational and leisure activities on SNSs increase cyber-harassment victimization.

*Hypothesis 3***.** Engagement in online risky behaviors increases cyber-harassment victimization.

Hypothesis 4. Formal and informal capable guardianship reduces cyber-harassment victimization.

Dependent Variable

This study used four items adapted from the 2013 Korean Institute of Criminology survey. Respondents were asked within the last 12 months: (a) Despite your rejection of his or her messages, someone consistently sent you messages; (b) you have

repeatedly been threatened by receiving fearful messages, pictures and/or movies; (c) someone has used swearwords at you or threatened you on SNSs; (d) you have received sexual content through the Internet without your consent. Responses to these survey items were dichotomized (0=No, 1=Yes) and created a dependent variable: cyber-harassment.

Table 1. *Descriptive Statistics for Study Measures*

VARIABLES	Mean	SD	Minimum	Maximum
Response Variable				
Cyber Harassment	.16	.51	.00	4.00
Online Vocational and Leisure				
Activities				
Usage of SNS (Facebook)	1.86	1.10	1	7
Usage of SNS (KaKaostory)	1.55	.85	1	7
Number of updates to SNS (Facebook)	2.07	.86	1	4
Number of updates to SNS (KaKaostory)	1.89	.78	1	4
Uploading number of photos on SNS (Facebook)	1.71	.67	1	4
Uploading number of photos on SNS (KaKaostory)	1.71	.63	1	4
Proximity to Crime				

Unknown Friend	.00	.00	.00	.00
Digital Guardianship				
Cyber security setting on SNSs + Security application on SNSs	2.35	1.18	.00	6.00
Online Risky Activities				
Illegally downloading software online + Downloading porn videos/movies + Slandering someone online	.12	.32	.00	1.00
Control Variables				
Age	32.75	11.47	14	59
Gender	.51	.50	.00	1.00

Independent Variables

Three sets of independent variables in the subsequent analyses: (a) digital guardian measure, (b) online lifestyle measure, and (c) demographic information assessed in the subsequent analyses.

Digital Guardianship. Cyber Security on SNSs: The researchers argue that digital-capable guardianship is the most important tenet to prevent computer crime and cyber crime (Choi, 2008; Holt & Bossler, 2009). This study measured the degree of cyber security on SNSs and using security applications on SNSs as digital guardianship. Respondents were asked to indicate their level of agreement with each statement using a Likert Scale: (a) I set my security of SNSs so that strangers can access my SNS accounts

without my permission; (b) I use an application to make new friendships on SNSs. The items were anchored by strongly disagree, disagree, agree, and strongly agree. A measure of the respondent's mean cyber security on SNSs was created (Cronbach's alpha = .724)

Online Vocational and Leisure Activities. Following Choi's (2008) study, online lifestyle measure is composed of two observed facets: vocational and leisure activities, and risky activities. First, the researcher will utilize ten survey items for the measure of vocational and leisure activities. Specifically, respondents were asked how they used the SNSs in their daily life within the previous 12 months: (1) what kinds of SNSs you belong to; (2) how many accounts of SNSs you have; (3) what the usage rate of SNSs is; (4) how many hours/minutes a day you spend time on SNSs; (5) how many photos and video clips you upload within a week; (6) how many postings you upload within a week; (7) what your main purposes for using SNSs are; (8) what your main activities for using SNSs are; (9) how many unknown friend connections you have on SNSs; (10) what kinds of personal information you open to the public.

Online Risky Behavior. Individuals' online risky behaviors measured in KIC's survey. These include using the Internet for the following purpose: (1) illegally downloading software online, (2) watching or downloading porn videos/movies online, or (3) slandering someone online. Respondents will be coded (options: 1=Strongly disagree, 2=Disagree, 3=Agree, 4=Strongly agree). A measure of the respondent's online risky behavior was created (Cronbach's alpha = .68).

This study controlled for age and gender. Age is measured in years at the time of the survey. The respondents were asked: "How old are you?" Gender is a dichotomous

variable differentiating male (51%) and female (49%) respondents (0=female and 1=male).

Choi, Choo, & Sung (2015) study results demonstrate that gender difference is associated with risky leisure and vocational activities and security management (Choi et al., 2015). Also, Choi et al. (2015) found that age difference is statistically associated with online lifestyle factors and computer crime victimization. For example, younger online users were more likely to become engaged in risky vocational and leisure activities. Other studies (Holt, 2009; Reyns, 2011) indicated that age and gender variables did significantly influence the likelihood of online sexual crime victimization, including cyber stalking and cyber harassment.

Interestingly, although age and gender differences statistically contributed to the computer crime/cybercrime victimization in previous research (Choi, 2015; Holt, 2009; Reyns, 2011), age and gender factors in this current study do not significantly influence cyber harassment victimization of South Korean online users.

Analytic Plan

Through the Statistical Package for the Social Sciences (SPSS) program, negative binomial regression was used to assess cyber harassment victimization. Because of the skewed nature of the data, negative binomial regression is an appropriate statistical technique for measuring the relationships between cyber routine activities theory and cyber harassment victimization. Usually, negative binomial regression can be utilized for over-dispersed count variables, especially when the conditional variance exceeds the conditional mean (UCLA, January 2015). In addition, it can be employed to "predict the value of the dependent variable on the basis of the independent variables" (Fox, Levin, &

Shively, 2002, p. 335). It was hypothesized that measures of digital capable guardianship, online risky behavior, and online vocational and leisure activities from cyber-routine activities theory can be predictive of cyber harassment victimization.

CHAPTER 4

RESULTS

We estimated negative binomial regression models with cyber harassment victimization as the dependent variable. The significant results based on the negative binomial regression analysis can be seen in Table 2.

Table 2. *Analysis of Maximum Likelihood Parameter Estimates of Cyber Harassment by Negative Binomial Regression Model*

		Negative Binomial Regression Model			
	Parameter	B	SE	Wald Chi-Square	Odds Ratio (Exp(B))
Digital Guardianship	Cyber security and security application on social networking sites	0.24	0.09	5.71	1.27***
Online Risky Behavior	Illegally downloading software + Downloading porn videos + Slandering online	0.18	0.05	11.81	1.20***

Online vocational and leisure activities	Unknown Friend	0.03	0.01	30.43	1.03**

Note: The Negative Binomial dispersion parameters were estimated by maximum likelihood.

*p < .05. **p < .01. ***p < .001

Cyber Security on Social Networking Sites

The cyber security setting on SNSs that can block a stranger access, and the security application allows social networking users to make friends on SNSs. As Table 2 illustrates, the cyber security on SNS variable was found to have a significant effect on the likelihood of cyber harassment victimization. The cyber security setting and security application are designed to increase the level of cyber security on SNSs against cyber deviance. Our models indicate that those who have a lower level of cyber security on SNSs are 26% more likely to be cyber harassed (b = .24 and Odds Ratio = 1.27 with p < .001). Age and gender were not significant in this relationship.

Risky Online Behavior

As Table 2 shows, risky online behavior is a significant predictor of cyber harassment victimization. Online risky behavior refers to illegally downloading software, porn movies from an unknown website and is characterized with slandering others online. The online users who display the online risky behaviors are 20% more likely to be victimized by cybercriminals (b = .18 Odds Ratio = 1.20 with p < .001). Age and gender were not significant in the relationships between social networking users participating in online risky behaviors and cyber harassment.

Online Vocational and Leisure Activities

Among ten online vocational and leisure activities variables, only one variable is moderately significant: the relationship between cyber harassment victimization and the number of unknown friends on social networking sites. The more relationships with unknown friends online users had, their cyber-harassment victimization was increased by about 3% ($b = .03$ Odds Ratio = 1.03, and $p < .01$). Also, age and gender were not significant in this relationship.

The following chapter discusses the findings of this study and provides policy implications and directions for future research on cybercrime victimization.

CHAPTER 5

DISCUSSION

This study tested cyber-routine activities theory (Choi, 2008), which was originally derived from Hindelang et al. (1978) lifestyle-exposure theory and Cohen and Felson's (1979) routine activities theory. Most studies on cyber-harassment and cyber-stalking have focused on the specific demographic range of college students (Choi, 2008; Finn2004; Higgins et al., 2014; Holt, 2009; Reynes et al., 2011). Interestingly, this study focused on the broad demographic range, from age 14 to age 59, in South Korea.

The results of the study demonstrate that two causal factors from cyber-routine activities theory – lack of cyber security on SNSs and online risky behavior – have impacted the likelihood of cyber harassment victimization (Choi, 2008; Finn2004; Higgins et al., 2014; Holt, 2009; Reynes et al., 2011). In general, the computer security software (Choi, 2008; Holt, 2009; Higgins, 2007) and the computer user's security awareness (Arachchchilage & Love, 2014) should decrease the likelihood of victimization by digital piracy, malware infection, and hacking. However, they do not decrease the likelihood of online sexual crime (e.g., cyber-harassment and cyber-stalking). These findings support previous research that found cyber security settings on SNSs instead of computer security software is directly related to preventing cyber harassment.

With respect to targets' online exposure activities, spending a lot of time on SNSs increases the risk of diversified victimization online (Bossler & Holt, 2009; Ngo & Paternoster, 2011; Wilsem, 2013). Reyens et al. (2011) found that four online exposure variables: Number of social networks, number of social network updates, photos on social network, and AOL instant messenger, are associated with statistically significant

increases in the likelihood of victimization. Although the study expected similar findings to what Reyens et al. (2011) previously examined, the actual findings from this empirical study show that the majority of variables from online vocational and leisure activities are not significantly related with cyber-harassment victimization. Only one of the ten variables (e.g., number of unknown friends on social networking sites) from online vocational and leisure activities is significantly associated with victimization.

Age was a significant demographic factor in the previous studies on this subject (Bossler et al., 2012; Holt & Bossler, 2009; Wilsem, 2013). Youth had higher possibilities of being harassed online, whereas cyber-harassment victims in this study were distributed over a wide demographic range. Our findings indicate that the various ages of SNS users and cyber-harassment victims in South Korea implied a unique cyber-culture and online social environment when compared to other studies focused on younger generation (e.g., youth or college students) of individual nations.

Overall, the results of the analysis provide noteworthy insights into the capable guardian and online risky behavior tenets from cyber-routine activities theory. These vital aspects can contribute to the development of crime prevention programs in various ways. Based on this study, policy implications can be derived from the two elements of cyber-routine activities theory: capable guardians and online risky behavior.

The first step to prevention is Cybersecurity and Protection programs on SNS. This research indicates that the individuals who had a lower level of cyber security settings on SNSs were more likely to be harassed. Cybersecurity experts suggest the best way to prevent individuals from becoming cyber-harassment victims is to educate online users on how to enforce cyber security on SNSs (Donkersley, April 2013). Features of

cyber-security on SNSs provide users with authorizations, including the following: (1) defining in considerable detail how their personal profiles are displayed online; (2) controlling who accesses their social networking accounts (Hogben, 2007, p1). In this sense, the program should have efficient practices that individuals could learn how to set the cyber security setting so that only those users who were linked to their accounts as "friends" could view their profile information on social networks and access to their accounts (Henson et al., 2011). Recently, some SNS providers managed social network security programs such as Stay Secure on Facebook Program in order to build better security awareness for online users (Facebook, July 2015). As discussed above, KaKaoStory is one of the most popular SNSs in all of South Korea, but does not currently have a cyber security program. This research suggests that KaKaoStory Corporation should implement some such cybersecurity and protection on SNS programs to better protect its users from online threats. If the Korean society utilized these types of security programs to educate online users, cyber-harassment victimization in South Korea can be minimized.

In addition, while individual SNS users may strengthen their cyber security levels on SNSs, cyber criminals are potentially able to commit a breach of SNS users' information because of the advanced technologies utilized in stealing individuals' information (Federal Communications Commission, 2015). Therefore, as a related step with cyber security setting on SNSs, this study suggests that SNS providers supplement the cryptographic functions that support SNS users' encryption in order to enhance the cyber security level on SNSs. Some public web servers have recently offered cryptographic techniques as an aim of protection for sensitive personal data such as birth

date, job, photos, group membership, cell phone number, and e-mail address (Donkersley, 2013; Federal Communications Commission, 2015). Hopefully, SNS providers can improve protection of SNS users from the breach of personal information that is possibly utilized for committing potential cybercrime, especially online interpersonal crime. In short, if both cyber security setting and cryptographic functions are accurately implemented to reinforce SNS users' security, it may help to minimize cyber-harassment victimization in South Korea.

The second step to prevention is Don't Click programs. Don't Click programs mainly promote identification and avoidance of malicious situations (Choi et al., 2015; Microsoft, December 2015; Terry and Ackerman 2008; Wortley and Smallbone 2006). The results of this study indicate that online users who have a tendency to become involved in risky online behaviors were more likely to be victimized by cyber-harassment than individuals with non-risky online behaviors. Thus, the prevention programs should include how to identify and control risky online behaviors that can trigger a malicious situation on SNSs. It is highly recommended that online users become educated about the specific risky online behaviors via utilizing the effective guidelines so that they are aware of the potential for victimization (Marcum et al., 2010). For example, online users can realize the fact that clicking pop-up advertisement, digital icons, or hyperlinks on web sites or SNSs impact the likelihood of cybercrime victimization, including online interpersonal victimization (Choi, 2008; Holt & Bossler, 2009; Marcum, 2010; Reyns, 2010; Wolak et al., 2007). According to the Symantec "2015 Internet Security Threat Report", the cyber threats leveraging social network scams such as manual sharing, fake offering, like-jacking, comment-jacking, and fake apps are serious problems in the virtual

world (InfoSec Institute, September 2015). In fact, some social network users tend to click on malicious links or fake offers posted by a friend or stranger without concerns of risks (InfoSec Institute, September 2015). Therefore, the risk-taking behavior instigates online users to get involved with online interpersonal violence. The Don't Click program can enhance the Korean SNS users' knowledge level about the various types of risky online situations as delineated above.

The third step to prevention is Cyber-security Awareness Culture programs. The Cybersecurity Awareness Culture programs consist of sharing and operating cybersecurity on SNSs so that online users can easily be educated about cyber security and safe online lifestyle on SNSs. Public sector, private sector, and academia are all important stakeholders in preventing cyber-harassment (Ybarra el al., 2007; Kraft & Wang, 2009). Hence, their cooperation is necessary to build a better security awareness culture in Korean society. The prevention programs could be categorized as school-based prevention programs because the school-based programs may be the first stage that students could learn specific guidelines for preventing cyber-crime in the classroom and the community at large (Choi, 2015). If the prevention program could be interactive and have an interesting environment with cyber-security and online lifestyle issues instead of fear, students would feel comfortable with conversations about cyber-security and risky online lifestyle on social networks and raise potential concerns without hesitation. Moreover, students would effectively learn cyber-security lessons (Facebook, November 2014). In other words, when we educate students with an adequately structured cyber prevention program, the beneficial outcomes should be expected by establishing

individuals' appropriate online lifestyle and establishing their own protections during the usage of social networks (Choi, 2015).

This study had a number of limitations that should be considered for future research. Since the purpose of KIC data was to delineate the Koreans' social networking usages and their related behaviors, the theoretical assessment for cyber-security, online lifestyle, cyber-harassment measures was imperfect. In addition, measuring more accurate individual victimization patterns using online lifestyle and the use of cyber-security requires longitudinal data. However, this survey was the first national data collection on the response of social networking services in South Korea, which was collected as a cross-sectional format. We hope to see longitudinal data on the social networking service survey and use more refined measures for the assessment of cyber-harassment victimization in the near future.

Also, assessing formal/informal guardianship factors were limited in this study. Some researchers in previous studies did not believe that the formal/informal guardianship factors substantially minimized the likelihood of interpersonal cybercrime (Holt, 2009; Reyns, 2011; Yar, 2005). However, formal/informal capable guardianship may be very imperative factors that can effectively help to minimize cybercrime, including cyber-harassment, if it accurately works. Therefore, future research needs to consider formal/informal guardianship factors as major measures in research for cybercrime issues.

CHAPTER 6

CONCLUSION

The cyber-harassment victimization model demonstrates the relationships between capable guardianship and online lifestyle variables with cyber-harassment victimization. In terms of capable guardianship variables, the cyber security and the security applications on SNSs are significant factors in preventing cyber-harassment victimization. Also, the model shows that risky online behavior is significantly associated with an increase in cyber-harassment victimization. Finally, the online vocational and leisure activities are moderately associated with an increased likelihood of victimization. Our current study is a substantial theoretical test of cyber-routine activities theory (2008), which provides a sense of understanding of the recent cyber harassment phenomenon.

References

Acar, A. (2008, October 11). Antecedents and consequences of online social networking behavior: The care of Facebook. *Journal of Website Promotion*, *3*(1-2).

After the implementation of anti-prostitution law. (2014, December 1). *Korean Lawyer Association News*, *1*, pp. 1, 2. Retrieved from http://news.koreanbar.or.kr/news/articleView.html?idxno=11872

Akers, R. L., & Sellers, C. S. (2013). *Criminological theories: Introduction, evaluation, and application* (6th ed., pp. 137-159). New York, NY: Oxford University.

Ashley Madison attack prompts spam link deluge. (2015, July 31). *BBC News*. Retrieved from http://www.bbc.com/news/technology-33731183

Bernburg, J. G., & Thorlindsson, T. (2001). Routine activities in social context: A closer look at the role of opportunity in deviant behavior. *Justice Quarterly*, *18*, 543-567.

Birkbeck, C., & LaFree, G. (1993). The situational analysis of crime and deviance. *Annual Review of Sociology 19*(2), 113-37.

Bossler, A., & Holt, T. J. (2009, January). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400-429.

Boyd, D. M., & Ellison, N. B. (2008). Social network sites: Definition, history and scholarship. *Journal of Computer-Mediated Communication*, *13*, 210-230.

Briggs, P., Simon, W. T., & Simonsen, S. (2011). An exploratory study of Internet-initiated sexual offenses and the chat room sex offender: Has the Internet enabled a new typology of sex offender? *Sexual Abuse: A Journal of Research and Treatment*, *23*(1), 72-91.

Building better security awareness (2015, November). In *Facebook*. Retrieved November 12, 2014, from https://www.facebook.com/security

Chambers, J. (2014, June 25). South Korea number 1 for on UN e-government ranking 2014. *FutureGov Magazine*. Retrieved from http://www.futuregov.asia/articles/south-korea-number-1-for-online-participation-un-e-government-rankings-2014

Cohen, L. E., & Felson, M. (1979, August). Social change and crime rate trends: A routine activities approach. *American Sociological Review*, *44*(4), 588-608.

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

Choi, K. (2015). *Cybercriminology and Digital Investigation*. El Paso: LFB Scholarly Publishing LLC.

Choi, K., Choo, K., & Sung, Y. (2015, December 19). Demographic variables and risk factors in computer-crime: An empirical assessment. *Cluster Computing: The Journal of Networks, Software Tools and Applications*, *18*(4).

Clifford, R. D. (2006). *Cybercrime: The investigation, prosecution and defense of a* communications infrastructure (n.d.). In *The Whitehouse*. Retrieved January 19, 2015, from http://www.usdoj.gov/criminal/cybercrime/01ccma.pdf. *computer crime victimization* Doctoral dissertation, Indiana University of Pennsylvania, Indiana.

Cox, L., & Speziale, B. (2009, February). Survivors of Stalking: Their voices and lived experiences. *Journal of Women and Social Work*, *24*(1), 5-18.

Cybersecurity planning guide (n.d.). In *Federal Communications Commission*. Retrieved December 23, 2015, from https://transition.fcc.gov/cyber/cyberplanner.pdf

Cyberspace policy review: Assuring a trusted and resilient information and *Enforcement*, *5*(1-2).

Cyberstalking victim was others danger (n.d.). In *The National Center for Victims of Crime*. Retrieved October 21, 2015, from http://victimsofcrime.org/our-programs/stalking-resource-center/search-results?indexCatalogue=stalking-resource-center&searchQuery=cyberstalking+victim&wordsMode=0

Donkersley, T. (2013, April 22). Cybersecurity 2 - protecting your social media networks. In *AZTECHBEAT*. Retrieved December 23, 2015, from http://aztechbeat.com/2013/04/cyber-security-protecting-your-social-media-networks/

Enhancing security with a quick checkup (2015, July 30). In *Facebook*. Retrieved November 12, 2014, from https://www.facebook.com/security

Facebook users in South Korea from 2012 to 2018 (in millions) (2015). In *Statista*. Retrieved October 22, 2015, from http://www.statista.com/statistics/304833/number-of-facebook-users-in-south-korea/

Farley, M., Franzblau, K., & Kennedy, A. M. (2014, October 8). Online prostitution and trafficking. *Albany Law Review*, *1*, 101-157.

Finklea, K. M., & Theohary, C. A. (2012). Cybercrime: Conceptual issues for congress and U.S. law enforcement. *Congressional Research Service.*

Finn, J. (2004, April). A survey of online harassment at a university campus. *Journal of Interpersonal violence*, *19*(4).

Fox, J. A., Levin, J., & Shively, M. (2015). *Elementary statistics in criminal justice research* (2nd ed., pp. 334-340). Boston, MA: Allyn & Bacon.

Fox, K. A., Nobles, M. R., & Akers, R. L. (2011). Is stalking a learned phenomenon? An empirical test of social learning theory. *Journal of Criminal Justice*, *39*, 39-47.

George, T. (2014, December 1). The next big cybercrime vector: Social media. In *Security Week*. Retrieved December 23, 2015, from http://www.securityweek.com/next-big-cybercrime-vector-social-media

Grandoni, D. (2015, July 20). Ashley Madison, a dating website, says hackers may have data on millions. *The New York Times*. Retrieved from http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html

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.

Harthaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2011, November 16). The law of cyber-attack. *California Law Review.*

Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminology*, *7*(2).

Heinonen, J. A., Holt, T. J., & Wilson, J. M. (2012). Product counterfeits in the online environment: An empirical assessment of victimization and reporting characteristics. *International Criminal Justice Review*, *22*(4), 353-371.

Higgins, G. E. (2007, January). Digital piracy, self-control theory, and rational choice: An examination of the role of value. *International Journal of Cyber Criminology*, *1*(1).

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 Publishing Co.

Hogben, G. (2008, September). Security issues in the future of social networking. In *W3C*. Retrieved October 18, 2015, from http://www.w3.org/2008/09/msnws/papers/Future_of_SN_Giles_Hogben_ENISA.pdf

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime shcolarship. *Deviant Behavior*, *35*(1), 20-40.

Holt, T. J. (2011). *Crime online: Correlates, causes, and context*. Durham, NC: Carolina

Holt, T. J., & Blevins, K. R. (2007). Examining sex work from the client's perspective: Assessing johns using on-line data. *Deviant Behavior*, *28*, 333-354.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine In *Computer Security Institute*. Retrieved February 17, 2015, from

Hong, J. (2013, July 4). Cyworld attempts to save their mini-home page. *Kyunghyang News*. Retrieved from http://bizn.khan.co.kr/khan_art_view.html?artid=201307042118495&code=930100&med=khan

How social networking security awareness saved a company's reputation (2015, September 8). In *Inforsec Institute*. Retrieved October 18, 2015, from http://resources.infosecinstitute.com/how-security-awareness-saved-a-companys-reputation/

Hwang, I. (2015, October). Online sexual violence in social networking sites. *Kukmin News*. Retrieved from http://news.kmib.co.kr/article/view.asp?arcid=0009651687&code=61121111&cp=nv

Internet Crime Complaint Center. (2014). 2014 Internet crime report. In *Federal Bureau of Investigation. https://www.fbi.gov/news/news_blog/2014-ic3-annual-report*

Jagatic, Tom N., Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. "Social phishing." *Communication of the Acm* Oct. 2007: 10-50. Print.

Jang, B. (2012, December 6). The fear of cyber stalking is being expanded via social networking sites. *Munhwa News*. Retrieved from http://www.munhwa.com/news/view.html?no=2012120601071027295002

Kabay, M. E. (2001). *Studies and surveys of computer crime*. Norwich, CT.

Ki, S. (2013, November 12). The society recommemded for online prostitution. *Moneytoday News*, *1*, pp. 1, 2. Retrieved from http://www.mt.co.kr/view/mtview.php?type=1&no=2013111208480618872&outlink=1

Kim, D., Chun, H., Kwak, Y., & Nam, Y. (2014). The employment of dialogic principles in Website, Facebook, and Twitter platforms of environmental nonprofit organizations. *Social Science Computer Review*, *32*(5), 590-605.

Kim, S. (2014, January 14). Unrequited love is finished with homicide. In *MKNews*. Retrieved October 22, 2015, from http://news.mk.co.kr/newsRead.php?year=2014&no=70953

Korean National Sexual Offenses Law (2015). In *Department of Government Legislation* . Retrieved July 1, 2015, from http://www.law.go.kr/lsInfoP.do?lsiSeq=165492&efYd=20150701#0000

Korean Telecommunication Act of 2015 (2015). In *Department of Government Legislation* . Retrieved April 21, 2015, from http://www.law.go.kr/lsInfoP.do?lsiSeq=167388&efYd=20150421#0000

Kraft, E. M., & Wang, J. (2009, July). Effectiveness of cyber bullying prevention strategies: A study on students' perspectives.*International Journal of Cyber Criminology*, *3*(2), 513-535.

Kubic, T. (2001, June). *The FBI's perspective on the cyber crime problems*. Washington, DC: Congressional Testimony, Federal Bureau of Investigation.

Kunz, M., & Wilson, P. (2004, September). Computer crime and computer fraud. In Legislation in the United States: A qualitative analysis. *International Journal*

Leading social networks worldwide as of August 2015, ranked by number of active users (in millions) (2015, August). In *Statista*. Retrieved October 18, 2015, from http://www.statista.com/statistics/248863/number-of-registered-kakaotalk-users/

Lindberg, D. (2012). Prevention of cyberstalking: A review of the literature. In *Portland State University*. Retrieved October 18, 2015, from http://pdxscholar.library.pdx.edu/cgi/viewcontent.cgi?article=1000&context=ccj_capstone

Liu, F., & Lee, H. (2009). Use of social network information to enhance collaborative filtering performance. *Expert Systems with Applications*, *37*, 4772-4778.

News. Retrieved from http://www.npr.org/2014/02/23/281167415/fed-

of computer information systems.

of Cyber Criminology, *7*(2), 155-168.

McGrath, M. G., & Casey, E. (2002). Forensic psychiatry and the Internet: Practical perspectives on Sexual Predators and Obsessional Harassers in Cyberspace. *Journal of American Psychiatry Law*, *30*(1).

McCuddy, T., & Vogel, M. (2014). More than just friends: Online social networks and offender. *Criminal Justice Review*, 1-12.

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review*, *35*(4), 412-437.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2014, January). Juvenile and cyberstalking in the United States: An analysis of theoretical predictors of patterns of online perpetration. *International Journal of cybercriminology*, *8*(1).

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

Number of KakaoTalk's registered users from September 2010 to August 2014 (in millions) (2015). In *Statista*. Retrieved October 18, 2015, from http://www.statista.com/statistics/248863/number-of-registered-kakaotalk-users/

Parsons-Pollard, N. (2009). Cyberstalking: Utilizing what we do know. *Victims and Offenders*, *4*, 435-441.

Pempek, T. A., Yermolayeva, Y. A., & Calvert, S. L. (2009). College students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology*, *30*, 227-238.

Protection your personal Information: Social networks (2015, October). In *StaySafeOnline*. Retrieved October 18, 2015, from https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks

Reyns, B. W., & Englebrecht, C. M. (2012). The fear factor: Exploring predictors of fear among stalking victims throughout the stalking encounter. *Crime & Delinquency*, *59*(5), 788-808.

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*.

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offering among college students. *Deviant Behavior*, *33*, 1-25.

Richadson, R. (2010). 15th annual 2010/2011 computer crime and security survey. http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf

Roberts, L. (2008, January). Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An analysis on cyberstalking. *International Journal of Cyber Criminology*, *2*(1), 271-285.

Seo, Y. (2014, September 25). Unrequited Love with Teacher: Committing homicide. In *KBS News*. Retrieved October 22, 2015, from http://news.kbs.co.kr/news/view.do?ref=A&ncd=2936642

Sherman, L. W. (1989, February). Hot spots of crime and criminal careers of places. *Criminology*, *27*(1), 27-56.

Stata data analysis examples negative binomial regression (2015). In *UCLA: Institute for Digital Research and Education*. Retrieved January 26, 2016, from http://www.ats.ucla.edu/stat/stata/dae/nbreg.htm

State cyberstalking and cyberharassment laws (2015, January 12). In *National Conference of State Legislatures*. Retrieved October 18, 2015, from http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx

Statistic data for crime rates (2013, December). In *National Police Agency*. Retrieved December 15, 2014, from http://www.police.go.kr/portal/main/contents.do?menuNo=200197 *Strategies & Management*, *27*(3).

Social Networks (2015). In *Stay Safe Online*. Retrieved October 18, 2015, from https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks

Terry, K. J., & Ackerman, A. R. (2008, May 1). Child sexual abuse in the catholic church how situational crime prevention strategies can help create safe environments. *Criminal Justice and Behavior*, *35*(5), 643-657.

The sexual victimization of college women (2000, December). In *U.S. Department of Justice*. Retrieved October 22, 2015, from https://www.ncjrs.gov/pdffiles1/nij/182369.pdf

Thomas, D., & Loader, B. (2000). *Introduction-cyber crime: Law enforcement, security and surveillance in the Information age*. London, United Kingdom: Routledge.

Tseloni, A., Wittebroad, K., Farrell, G., & Peace, K. (2004). Burglary victimization in England and Wales, the United States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology*, *44*(1), 66-91.

UN e-government survey 2014 (2014). In *UNPACS*. Retrieved October 21, 2015, from http://unpan3.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014

United States of America, appellee, v. Shawn Sayer, defendant, appelant (2014, May 2). In *United States Court of Appeals for the First Circuit*. Retrieved February 24, 2015, from http://www.ca1.uscourts.gov/

University of Maryland.

up-with-harassment-author-reveals-her-cyberstalker

victimization. *Criminal Justice and Behavior*, *38*(11).

WHOA's 2006 cyberstalking statistics (2006). In *Working to Halt Online Abuse*. Retrieved February 24, 2015, http://www.haltabuse.org/resources/stats/2006Statistics.pdf

WHOA's 2011 cyberstalking statistics (2011). In *Working to Halt Online Abuse*. Retrieved February 24, 2015, http://www.haltabuse.org/resources/stats/2011Statistics.pdf

www.gocsi.com

Wilsem, J. V. (2013). Hacking and Harassment - Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437-453.

Wolak, J., Mitchell, K., & Finkelhor, D. (2007, February). Unwanted and wanted exposure to online pornography in a national sample of youth Internet users. *American Academy of Pediatrics*, *119*, 247-257.

Wortley, R., & Smallbone, S. (2006). *Situational prevention of child sexual abuse (Crime prevention strategies)* (Vol. 19). Monsey, NY: Criminal Justice Press.

Yar, M. (2005, October). The novelty of cybercrime: An assessment in light of routine activities theory. *European Journal of Criminology*, *2*(4), 407-427.

Ybarra, M. L., Mitchell, K. J., Finkelhor, D., & Wolak, J. (2008, February). Internet prevention messages: Targeting the right online behavior. *American Psychologist*, *63*(2), 111-128.

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

Number of social network users worldwide from 2010 to 2018 (2014). In *Statista*. Retrieved March 28, 2015, from http://www.statista.com/statistics/226768/social-networking-usage-in-south-korea-by-service-type/

11 tips for social networking safety (2015). In *Microsoft: Safety & Security Center*. Retrieved December 23, 2015, from https://www.microsoft.com/security/online-privacy/social-networking.aspx

2015 Internet Security Threat Report (2015). In *Symantec Corporation*. Retrieved October 18, 2015, from https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

2013 Police Statistics Report (2014, November). In *Korean National Police Agency*. Retrieved October 22, 2015, from http://www.police.go.kr/portal/main/contents.do?menuNo=200141

Appendix I: Survey Instrument

The Korean Institute of Criminology, which mainly focuses on researching criminal phenomenon and policy implications, is under the Prime Minister office in South Korea. Recently, the Korean Institute of Criminology has researched using status and victimization of Social Networking sites. Based on these surveys, KIC will establish an alternative to prevent cybercrime. Therefore, your participation will be valuable and helpful to conduct this research. Your survey data will be anonymously used for the processing of the statistical analysis. Also, KIC will only use your survey data for academic purposes. KIC will absolutely keep your personal information private. On behalf of the Korean Institute of Criminology, we appreciate your participation.

Recognition of Social Network Service and Victimization Survey

Instructions

Demographics

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

SQ1. Which region do you live?

(1) Seoul Metropolitan City

1) Jongno-gu 2) Jung-gu 3) Yongsan-gu 4) Sungdong-gu 5) Gwanjin-gu 6) Dongdaemun-gu 7) Jungnang-gu 8) Seongbuk-gu 9) Gangbuk-gu 10) Dobong-gu 11) Nowon-gu 12) Eunpyeong-gu 13) Seodaemun-gu 14) Mapo 15) Yangcheon-gu 16) Gangseo-gu 17) Guro-gu 18) Geumcheon-gu 19) Yeongdeungpo-gu 20) Dongjak-gu 21) Gwanak-gu 22) Seocho-gu 23) Gangnam-gu 24) Songpa-gu 25) Gangdong-gu

(2) Incheon City and Gyeonggi Province

26) Incheon city 27) Suwon city 28) Seongnam city 29) Uijeongbu city 30) Anyang city 31) Bucheon city 32) Gwangmyeong city 33) Pyeongtaek city 34) Dongducheon city 35) Ansan city 36) Goyang city 37) Gwacheon city 38) Guri city 39) Namyangju city 40) Osan city 41) Siheung

city 42) Gunpo city 43) Uiwang city 44) Hanam city 45) Yongin city 46) Paju city 47) Icheon city 48) Anseong city 49) Gimpo city 50) Hwaseong city 51) Gwangju city 52) Yangju city 53) Pocheon city SQ2. What is your gender? (1) Male (2) Female
SQ3. How old are you?_____ Write down what year you were born _____. 1) 10s (_____, _____) 2) 20s (_____, _____) 3) 30s (_____, _____) 4) 40s (_____, _____) 5) 50s (_____, _____)

Part A: Social Networking Sites

For the following questions, please note that:
Social Networking Sites: *websites that connect people together by allowing them to share interests and activities with friends, family, colleagues, as well as people with similar interests.*
Smartphone: *phones that have abilities similar to computers allowing users to access the Internet as well as download applications or programs onto their phone.*

Q1. Firstly, the survey question will start with the status of using Social Network sites.

Q1-1. Do you use Social Networking sites?

(1) Yes

(0) No

If you answer 'yes', what kinds of Social Network sites do you belong to?

Facebook	Twitter	KaKaostory	Cyworld
(1) Yes (2) No	(1) Yes (2) No	(1) Yes (2) No	(1) Yes (2) No

Q1-2. How many accounts (e.g., ID) of Social Networking sites do you have?

Facebook	Twitter	KaKaostory	Cyworld
( )	( )	( )	( )

Q1-3. Which device do you use for Social Networking sites the **most**? Please pick only one

Facebook	Twitter	KaKaostory	Cyworld
(1) Smartphone (2) Tablet PC (3) Desktop/Notebook (4) Computer in public places	(1) Smartphone (2) Tablet PC (3) Desktop/Notebook (4) Computer in public places	(1) Smartphone (2) Tablet PC (3) Desktop/Notebook (4) Computer in public places	(1) Smartphone (2) Tablet PC (3) Desktop/Notebook (4) Computer in public places

Q1-4. If the total usage of SNS is 100%, what is the usage rate of each social network site?

Facebook	Twitter	KaKaostory	Cyworld
( )%	( )%	( )%	( )%

Q1-5. Do you have a specific time to use Social Network sites? Or just randomly use it?

Facebook	Twitter	KaKaostory	Cyworld
(1) Specific time (2) Random time	(1) Specific time (2) Random time	(1) Specific time (2) Random time	(1) Specific time (2) Random time

Q1-6. On average, how many hours/minutes a day do you spend time on Social Networking sites?

Facebook	Twitter	KaKaostory	Cyworld
(1) 0 ~ 30min (2) 30min ~ 1hour (3) 1hour ~ 2hours (4) 2hour ~ 3hours (5) 3hours ~ 4hours (6) 4hours ~ 5hours (7) Over 5hours	(1) 0 ~ 30min (2) 30min ~ 1hour (3) 1hour ~ 2hours (4) 2hour ~ 3hours (5) 3hours ~ 4hours (6) 4hours ~ 5hours (7) Over 5hours	(1) 0 ~ 30min (2) 30min ~ 1hour (3) 1hour ~ 2hours (4) 2hour ~ 3hours (5) 3hours ~ 4hours (6) 4hours ~ 5hours (7) Over 5hours	(1) 0 ~ 30min (2) 30min ~ 1hour (3) 1hour ~ 2hours (4) 2hour ~ 3hours (5) 3hours ~ 4hours (6) 4hours ~ 5hours (7) Over 5hours

Q1-7. On average, how many photo and video clips do you upload within a week?

Facebook	Twitter	KaKaostory	Cyworld
(1) 0 (2) 1~ 5 (3) 6 ~10 (4) Over 11	(1) 0 (2) 1~ 5 (3) 6 ~10 (4) Over 11	(1) 0 (2) 1~ 5 (3) 6 ~10 (4) Over 11	(1) 0 (2) 1~ 5 (3) 6 ~10 (4) Over 11

Q1-8. On average, how many postings do you upload within a week? (The methods of posting include posting content, commenting, clicking the button for like or dislike, tweeting and re-tweeting).

Facebook	Twitter	KaKaostory	Cyworld
(1) 0 (2) 1~ 5 (3) 6 ~10 (4) Over 11	(1) 0 (2) 1~ 5 (3) 6 ~10 (4) Over 11	(1) 0 (2) 1~ 5 (3) 6 ~10 (4) Over 11	(1) 0 (2) 1~ 5 (3) 6 ~10 (4) Over 11

Part B: Purpose and Activity on Social Networking Sites

Q2. What is your main purpose for using Social Networking sites? Please choose your top 2 choices from the list below.

(1) Friendship and conversation (2) Building-up new relationships (friend and dating)
(3) Information and Knowledge (4) Marketing for company
(5) Entertainment and leisure (6) Following trends
(7) Removing stress (8) Self-expression
(9) Others _____

Q3. What are your main activities for using Social Networking sites? Please choose your top 2 choices from the list below.

(1) Recording personal life (2) Sharing Information and knowledge
(3) Sharing a personal idea (4) Only monitoring other's posting
(5) Reading and responding to others' postings
(6) Promoting personal events and advertisements
(7) Building-up new relationships (requesting friendship and followership)
(8) Others _____

Q4. The following questions are in regard to the function and characteristic of Social Networking sites. Please select the response that best fits you.

	Contents	Strongly Disagree	Disagree	Agree	Strongly Agree
Q4-1	Social Networking sites can strengthen relationships with people I already know	(1)	(2)	(3)	(4)
Q4-2	Social Networking sites can strengthen relationships with people I don't know	(1)	(2)	(3)	(4)
Q4-3	Social Networking sites can offer useful information for ordinary life, work, and schoolwork.	(1)	(2)	(3)	(4)
Q4-4	Social Networking sites can offer reliable information.	(1)	(2)	(3)	(4)
Q4-5	Social Networking sites can strengthen the level of interest regarding social phenomenon and issues.	(1)	(2)	(3)	(4)
Q4-6	Social Networking sites can offer chances to understand another's emotional status and life.	(1)	(2)	(3)	(4)
Q4-7	Social Networking sites are necessary to interact with others.	(1)	(2)	(3)	(4)
Q4-8	Social Networking sites can be effective as marketing tools.	(1)	(2)	(3)	(4)

	Contents	Strongly Disagree	Disagree	Agree	Strongly Agree
Q4-9	Social Networking sites are helpful to remove stress.	(1)	(2)	(3)	(4)
Q4-10	Social Networking sites are useful tools to promote me to others.	(1)	(2)	(3)	(4)

Q4-11	Social Networking sites can be used to commit crime.	(1)	(2)	(3)	(4)
Q4-12	Social Networking sites can incite students to commit school bullying.	(1)	(2)	(3)	(4)
Q4-13	Social Networking sites can incite people to commit suicide.	(1)	(2)	(3)	(4)
Q4-14	Social Networking sites can intensify intrusions of privacy.	(1)	(2)	(3)	(4)
Q4-15	Social Networking sites can make an inappropriate sexual culture.	(1)	(2)	(3)	(4)
Q4-16	Social Networking sites create exposure to sensational information.	(1)	(2)	(3)	(4)
Q4-17	Social Networking sites are consecutively correlated with the physical world.	(1)	(2)	(3)	(4)
Q4-18	Social Networking sites are virtual places outside of the physical world.	(1)	(2)	(3)	(4)

Q5. **How many connections do you have on Social Networking sites? Please write in the appropriate answer based on <u>mostly using</u> social networking sites. Please pick one in each question.**

Content		**SNS Name**
Q5-1	Family/Relative	( ) people
Q5-2	Friend/Peer	( ) people
Q5-3	Coworker/Work related person	( ) people
Q5-4	Person who has the same hobby and interests	( ) people
Q5-5	Celebrity/Sports star	( ) people

Q5-6	Famous person (except celebrity/sports star)	( ) people
Q5-7	Friendship that was built on the Internet	( ) people
Q5-8	Company/Media company/Government/ Government-owned corporation	( ) people
Q5-9	Unknown person	( ) people
Q5-10	Other_____	( ) people

Q6. Do you usually make friendships via Social Networking Sites on the Internet? Or do you meet most of your friends in the real world before having friendships on Social Networking Sites?

(1) I met most of them online sites first.

(2) I met most of them via offline sites first.

(3) The ratio of meeting friends is half online and half offline.

Q7. Do you open your personal information to the public? Please check it, based on the <u>mostly using</u> Social Networking sites. Please pick one in each question.

Content		**SNS Name**	
		Open information	**Closed information**
Q7-1	Real name	(1)	(2)
Q7-2	Gender	(1)	(2)
Q7-3	Age	(1)	(2)
Q7-4	Profession	(1)	(2)
Q7-5	Company/School	(1)	(2)
Q7-6	Residential address	(1)	(2)
Q7-7	Interests	(1)	(2)
Q7-8	E-mail address	(1)	(2)
Q7-9	Cell number	(1)	(2)
Q7-10	Messenger ID	(1)	(2)
Q7-11	Other SNS address	(1)	(2)
Q7-12	Photo	(1)	(2)

Q7-13	Relationship status	(1)	(2)

Q8. The following questions focus on capable guardianship. Please pick one in each question.

Contents		Strongly Disagree	Disagree	Agree	Strongly Agree
Q8-1	I set my security of SNS so that strangers can access my social networking sites without my permission.	(1)	(2)	(3)	(4)
Q8-2	I use an application to make new friendships on social networking sites.	(1)	(2)	(3)	(4)

Part C: Knowledge level about Social Networking sites

Q9. What is your knowledge level about using Social Networking?
(1) Basic level

(2) Intermediate level

(3) Advanced level

Q10. Instruction: The following questions are regarding your use of SNS. Please pick one in each question.

Content		Yes	No
Q10-1	I understand the meaning and concept of SNS	(1)	(2)
Q10-2	I spend more time on my social networking sites than using e-mail and text message.	(1)	(2)
Q10-3	I can easily communicate with most of my acquaintances by using Social Networking sites.	(1)	(2)
Q10-4	I can use various types of devices (e.g., laptop, smartphone, tablet PC) for operating Social Networking sites.	(1)	(2)
Q10-5	I can use games, programs, and services that are provided by Social Networking sites.	(1)	(2)
Q10-6	I have several management programs and applications for my Social Networking sites accounts.	(1)	(2)
Q10-7	I understand the fact that even though I delete postings on Social Networking sites; it is possible to save the content on	(1)	(2)

	network servers.		
Q10-8	I recognize the fact that even though I delete postings on Social Networking sites; it is possible to save the content on search engines and specific website servers.	(1)	(2)
Q10-9	I know how to use security programs for logins on Social Networking sites.	(1)	(2)
Q10-10	When I try to register onto Social Networking sites, I always read about the terms of using the services and using personal information.	(1)	(2)

Part D: Victimization on Social Networking sites

For the following questions, please note:
Cyber-Friends: *Friends who you only interact with in an online setting (not in person).*

Q11**. The following questions are only for middle and high school students. Please pick one based on the statements below regarding your mostly using Social Networking sites in the past 12 months. Please pick one in each question.**

Content		Yes	No
Q11-1	Have your schoolmates bullied you by using unpleasant nicknames on Social Networking sites.	(1)	(2)
Q11-2	Have your schoolmates uploaded unwanted postings, pictures and video clips?	(1)	(2)
Q11-3	Have your schoolmates released your secrets without your permission?	(1)	(2)
Q11-4	Have your schoolmates shared some interesting information with each other excluding you?	(1)	(2)
Q11-5	Have your schoolmates spread rumors or untruthful facts about you?	(1)	(2)

Q12. The following questions focus on asking your experiences on Social Networking sites in the past 12 months.

Content		Yes	No
Q12-1	Have you been consistently rejected by someone in the application of friendship and membership on Social Networking sites?	(1)	(2)
Q12-2	Have you experienced deception with a great prize and coupons on Social Networking sites?	(1)	(2)

Q12-3	Has your personal information been stolen because you were deceived on Social Networking sites?	(1)	(2)
Q12-4	Have you ever been impersonated on Social Networking sites?	(1)	(2)
Q12-5	Has someone used your pictures and movies or personal information without your permission on Social Networking sites?	(1)	(2)
Q12-6	Has someone spread rumors or untruthful facts about you on Social Networking sites?	(1)	(2)
Q12-7	Has someone damaged your reputation by slandering you (without the use of swearwords) on Social Networking sites?	(1)	(2)
Q12-8	Has someone used swearwords at you or threatened you on Social Networking sites?	(1)	(2)
Q12-9	Despite your rejection of his or her messages, has someone consistently sent you messages?	(1)	(2)
Q12-10	Have you ever been threatened by receiving fearful messages, pictures and/or movies?	(1)	(2)
Q12-11	Have you received illegal sexual content through the Internet without your consent?	(1)	(2)
Q12-12	Has anyone suggested prostitution to you on Social Networking sites?	(1)	(2)

Q13. The following questions focus on asking about your experiences in the physical world in the past 12 months. Please pick one in each question.

Content		Yes	No
Q13-1	Has your house been broken into when you were not home?	(1)	(2)
Q13-2	Have you ever been robbed at home?	(1)	(2)
Q13-3	Have you ever been pickpocketed in public?	(1)	(2)
Q13-4	Has you ever been assaulted or threatened by anyone in public?	(1)	(2)
Q13-5	Has anyone deprived you of money or valuables in public?	(1)	(2)
Q13-6	Have you been sexually assaulted by anyone in public?	(1)	(2)

Part E: After the experience of victimization on Social Networking sites

Instructions: If you answered 'yes' at least more than once from the part D questions, please answer the following questions.

Q14. Have you reported the criminal issue(s) related to the part D questions to a police officer?

(1) I have never reported it (2) I have reported it

Q14-1. If you did not report it, what was the reason?

(1) I did not feel like taking the time to report it to the police

(2) I thought the evidence of the crime was not enough to catch the offender

(3) I felt like the police don't have the ability to catch the offender

(4) I was worried about what my personal life might have been like under the exposure of police

(5) I thought it was not an issue to report to the police

(6) My victimization was not serious

(7) I worried about revenge from the offender

Q14-2. If you reported it, what was the result after reporting it?

(1) I was totally satisfied with the service of the police and the offender was captured

(2) I was satisfied with the service of the police, but the offender was not captured

(3) I was not satisfied with the service of the police, but the offender was captured

(4) I was not satisfied with the service of the police and the offender was not captured

Q15. **After victimization on SNS, have you ever reported it to the provider of SNS?**
(1) I did not (2) I did

Q15-1. If you did not, what was the reason?

(1) My victimization was not serious

(2) I did not feel like taking the time to report it to the provider

(3) I thought it was not an issue to report to the company

(4) I thought even if I report it, it might not be changed

Q15-2. If you reported it, how satisfied were you in doing so?

(1) Strongly not satisfied (2) Not satisfied

(3) Satisfied (4) Strongly satisfied

Q16. Did you change any online behavior in your SNS activity after victimization? Please pick some.

(1) Stopped using SNS
(2) SNS deregistration
(3) Changed level of personal Information released
(4) Changed SNS address and name
(5) Changed your SNS password
(6) Made a new SNS account
(7) Canceled SNS friendships
(8) None

Q17. The following questions focus on difficulty and pain after victimization. Please pick one in each question.

Contents		Yes	No
Q17-1	I had depressive disorder.	(1)	(2)
Q17-2	I felt lonely.	(1)	(2)
Q17-3	I had fear of victimization.	(1)	(2)
Q17-4	I had insomnia, headaches and nightmares.	(1)	(2)
Q17-5	I experienced difficulty in having relationships with others.	(1)	(2)
Q17-6	I have moved to another place or transferred to another school.	(1)	(2)
Q17-7	I felt like committing suicide.	(1)	(2)
Q17-8	Other pains(Please explain about it:)	(1)	(2)

Q18. After victimization on SNS, what specific emotional status was changed? Please pick one in each question.

Contents		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Q18-1	When someone attacks me, I am confident to protect myself.	(1)	(2)	(3)	(4)	(5)
Q18-2	I feel that I am a very important person.	(1)	(2)	(3)	(4)	(5)
Q18-3	Level of belief in others	(1)	(2)	(3)	(4)	(5)
Q18-4	Level of belief in the police or criminal justice agents	(1)	(2)	(3)	(4)	(5)
Q18-5	Respect for our law enforcement system	(1)	(2)	(3)	(4)	(5)

Part F: The Fear of Social Networking sites

Q19. Please pick one based on how seriously you feel afraid of the situations below.

Contents		Never Afraid	Not Afraid	Afraid	Strongly Afraid
Q19-1	When you are at home alone…	(1)	(2)	(3)	(4)
Q19-2	When you walk around your neighborhood alone…	(1)	(2)	(3)	(4)

Q20. Please pick one based on how seriously you feel afraid of the situations below.

Contents		Never Afraid	Not Afraid	Afraid	Strongly Afraid
Q20-1	I am afraid of being victimized on Social Networking sites.	(1)	(2)	(3)	(4)
Q20-2	I am afraid of my family members being victimized on Social Networking sites.	(1)	(2)	(3)	(4)
Q20-3	I am afraid of my friends being victimized on Social Networking sites.	(1)	(2)	(3)	(4)

Q21. Please pick one based on how seriously you feel afraid of the situations below.

Contents		Never Afraid	Not Afraid	Afraid	Strongly Afraid
Q21-1	I am afraid that my privacy may be exposed through my SNS.	(1)	(2)	(3)	(4)
Q21-2	I am afraid of losing my money and property because of someone deceiving me through SNS.	(1)	(2)	(3)	(4)
Q21-3	I am afraid of someone sexually harassing me through SNS.	(1)	(2)	(3)	(4)
Q21-4	I am afraid of someone, I already know through SNS, sexually harassing and assaulting me.	(1)	(2)	(3)	(4)
Q21-5	I am afraid of someone insulting me and trying to damage my reputation through SNS.	(1)	(2)	(3)	(4)
Q21-6	I am afraid of someone spreading rumors or untruthful facts about me through SNS.	(1)	(2)	(3)	(4)

Q21-7	I am afraid of my personal information being leaked online.	(1)	(2)	(3)	(4)
Q21-8	I am afraid of someone impersonating me through SNS.	(1)	(2)	(3)	(4)
Q21-9	I am afraid of someone deceiving me through SNS in order to infect my computer and mobile phone with a virus.	(1)	(2)	(3)	(4)
Q21-10	I am afraid of someone repeatedly sending unwanted messages to me through SNS.	(1)	(2)	(3)	(4)
Q21-11	I am afraid of someone stealing my money and possessions by using my personal information that was collected through my SNS.	(1)	(2)	(3)	(4)
Q21-12	I am afraid of someone breaking into my house by using my information that was collected through my SNS.	(1)	(2)	(3)	(4)

Q22. The following questions focus on the likelihood of victimization on Social Networking sites. Please pick one in each question.

Contents		Strongly Disagree	Disagree	Agree	Strongly Agree
Q22-1	I am more likely to be victimized than others on SNS.	(1)	(2)	(3)	(4)
Q22-2	I cannot protect myself from someone committing a cybercrime against me on SNS.	(1)	(2)	(3)	(4)
Q22-3	I will be more seriously damaged in the long term than others if I am victimized on SNS.	(1)	(2)	(3)	(4)

Q23. The following questions focus on online behavior. Please pick one in each question.

Contents		Strongly Disagree	Disagree	Agree	Strongly Agree
Q23-1	I usually install security programs for using SNS.	(1)	(2)	(3)	(4)
Q23-2	I usually reject strangers' requests for friendships and messages.	(1)	(2)	(3)	(4)
Q23-3	I regularly change my account password of SNS.	(1)	(2)	(3)	(4)
Q23-4	I don't access SNS without my own	(1)	(2)	(3)	(4)

	mobile phone and Notebook.				

Q24. The following questions focus on relationships and culture on SNS. Please pick one in each question.

Contents		Never Afraid	Not Afraid	Afraid	Strongly Afraid
Q24-1	I can trust cyber friendships among online users.	(1)	(2)	(3)	(4)
Q24-2	Cyber friends on SNS share similar ideas.	(1)	(2)	(3)	(4)
Q24-3	Individuals in cyber friendships are very close.	(1)	(2)	(3)	(4)
Q24-4	Individuals in cyber friendships tend to help each other.	(1)	(2)	(3)	(4)
Q24-5	If someone slanders an individual and uses swearwords at them on SNS, other online users will punish these violent acts.	(1)	(2)	(3)	(4)
Q24-6	If someone posts unhealthy content on SNS, other online users will punish these violent acts.	(1)	(2)	(3)	(4)
Q24-7	Cyber friends on SNS have disciplines and regulations to keep their healthy culture.	(1)	(2)	(3)	(4)
Q24-8	Cyber friends try to create a healthy culture in the SNS environment among each other.	(1)	(2)	(3)	(4)

Part G: Behavior on the SNS

Q25. The following questions are only for <u>middle and high school students</u>. Please pick one based on the statements below regarding your Social Networking site use in the past 12 months.

Content		Yes	No
Q25-1	I have bullied my schoolmates by using their unpleasant nicknames on Social Networking sites.	(1)	(2)
Q25-2	I have uploaded my schoolmates' unwanted postings, pictures and video clips.	(1)	(2)
Q25-3	I have released my schoolmates' secrets without permission.	(1)	(2)
Q25-4	I have shared my schoolmates' interesting information with other schoolmates through Social Networking sites.	(1)	(2)
Q25-5	I have spread rumors or untruthful facts about my schoolmates on Social Networking sites.	(1)	(2)

Q26. The following questions focus on asking your experiences on Social Networking sites in the past 12 months. Please pick one in each question.

Content		Yes	No
Q26-1	I have consistently rejected someone's requests for friendship and membership on Social Networking sites.	(1)	(2)
Q26-2	I have deceived someone through a fake promotion with a great prize and coupons on Social Networking sites.	(1)	(2)
Q26-3	I have stolen someone's personal information by making a fake link on Social Networking sites.	(1)	(2)
Q26-4	I have impersonated another person on Social Networking sites.	(1)	(2)
Q26-5	I have used someone's pictures and videos or personal information without their permission on Social networking sites.	(1)	(2)
Q26-6	I have spread rumors or untruthful facts about someone on SNS.	(1)	(2)
Q26-7	I have damaged someone's reputation through slander (without using swearwords) him or her on SNS.	(1)	(2)
Q26-8	I have used swearwords at someone or threatened someone on SNS.	(1)	(2)
Q26-9	Despite someone rejecting my messages, I have repeatedly sent messages to someone.	(1)	(2)
Q26-10	I have threatened someone by sending fearful messages, pictures and videos.	(1)	(2)
Q26-11	I have sent sexual messages, pictures and videos on SNS.	(1)	(2)
Q26-12	I have suggested that someone get into prostitution on SNS.	(1)	(2)

Q27. How many friends or acquaintances relate with Question 26?
(1) None (2) Few (3) Many (4) A lot

Q28. How often do you interact with cyber friends who relate with Question 26?
(1) None (2) Almost none (3) Sometimes (4) Frequent

Q29. The following questions focus on the seriousness of issues on SNS. Please pick one in each question.

Contents		Strongly Disagree	Disagree	Agree	Strongly Agree
Q29-1	Consistently rejecting someone's requests for friendship and membership on Social Networking sites is a serious issue for me.	(1)	(2)	(3)	(4)

Q29-2	Fake promotions with great prizes and coupons on Social Networking sites are serious issues for me.	(1)	(2)	(3)	(4)
Q29-3	Stealing another's personal information through making a fake link on Social Networking sites is a serious issue for me.	(1)	(2)	(3)	(4)
Q29-4	Being impersonated by another person on Social Networking sites is a serious issue for me.	(1)	(2)	(3)	(4)
Q29-5	Using another's pictures and videos or personal information without their permission on Social Networking sites is a serious issue for me.	(1)	(2)	(3)	(4)
Q29-6	Spreading rumors or untruthful facts about someone on SNS is a serious issue for me.	(1)	(2)	(3)	(4)
Q29-7	Damaging someone's reputation through slandering (without using swearwords) him or her on SNS is a serious issue for me.	(1)	(2)	(3)	(4)
Q29-8	Using swearwords at someone or threatening someone on SNS is a serious issue for me.	(1)	(2)	(3)	(4)
Q29-9	Someone consistently rejecting my messages is a serious issue for me.	(1)	(2)	(3)	(4)
Q29-10	Threatening someone by sending fearful messages, pictures and videos is a serious issue for me.	(1)	(2)	(3)	(4)
Q29-11	Sending sexual messages, pictures and videos on SNS is a serious issue for me.	(1)	(2)	(3)	(4)
Q29-12	Suggesting, through SNS, that someone get into prostitution is a serious issue for me.	(1)	(2)	(3)	(4)

Q33. The following questions focus on stress. Please pick one in each question.

Contents		Strongly Disagree	Disagree	Agree	Strongly Agree
Q33-1	I have some stress because I don't have a good relationship with my family.	(1)	(2)	(3)	(4)
Q33-2	I have some stress because I don't have a good relationship with my friends.	(1)	(2)	(3)	(4)
Q33-3	I have some stress because someone unfairly treats me.	(1)	(2)	(3)	(4)
Q33-4	I have some stress because my financial status is poor.	(1)	(2)	(3)	(4)
Q33-5	I have some stress because of school grades (Question only for middle and high school students).	(1)	(2)	(3)	(4)
Q33-6	I have some stress because of my appearance (Question only for middle and high school students).	(1)	(2)	(3)	(4)

Q34. The following questions focus on mood and behavior. Please pick one in each question.

Contents		Strongly Disagree	Disagree	Agree	Strongly Agree
Q34-1	I usually feel blue.	(1)	(2)	(3)	(4)
Q34-2	I frequently think my life is unfortunate and gloomy.	(1)	(2)	(3)	(4)
Q34-3	I have much worry.	(1)	(2)	(3)	(4)
Q34-4	Sometimes I feel like I want to commit suicide.	(1)	(2)	(3)	(4)
Q34-5	I cry often.	(1)	(2)	(3)	(4)
Q34-6	When something wrong happens, I feel as if it is my fault.	(1)	(2)	(3)	(4)
Q34-7	I feel lonely.	(1)	(2)	(3)	(4)
Q34-8	I don't have any interest in the rest of my life.	(1)	(2)	(3)	(4)
Q34-9	I don't feel that my future is hopeful.	(1)	(2)	(3)	(4)
Q34-10	I feel very bad about everything.	(1)	(2)	(3)	(4)

Part I: Experience of Online

Q35. The following questions focus on experience of online. Please pick one in each question.

Contents		Strongly Disagree	Disagree	Agree	Strongly Agree
Q35-1	I have used someone else's social security number (including a family member), without their permission, online.	(1)	(2)	(3)	(4)
Q35-2	I have illegally downloaded subscription-based software online.	(1)	(2)	(3)	(4)
Q35-3	I have watched or downloaded porn videos/movies online.	(1)	(2)	(3)	(4)
Q35-4	I have slandered someone online.	(1)	(2)	(3)	(4)

Q36. How often do you recognize that online users slander and use swearwords each other?
(1) None (2) Sometimes (3) Often (4) Very often

Q37. How frequently do you think that personal information is leaked from online web sites, other than on social networking sites?
(1) None (2) Sometimes (3) Often (4) Very often

Part J: Policy Implication

Q38. The following questions focus on use of SNS. Please pick one in each question.

Contents		Strongly Disagree	Disagree	Agree	Strongly Agree
Q38-1	Law enforcement agents can use the function of location chase on SNS to prevent crime.	(1)	(2)	(3)	(4)
Q38-2	Law enforcement agents can use personal history on SNS to prevent crime.	(1)	(2)	(3)	(4)
Q38-3	Freedom of expression online can be prohibited on SNS to prevent crime.	(1)	(2)	(3)	(4)

Q39. How strong of an ethical level do you think that our society has on SNS?

(1) Very low-level (2) Low level (3) Strong level (4) Very strong level

Q40. In your opinion, which suggestion is the best way to enforce the ethical level on SNS?
(1) Do not do anything, then the level of ethic will be enforced itself.
(2) Under the criminal justice system, law enforcement authorities must punish the criminals.
(3) Online users enforce the ethics on SNS themselves.
(4) The SNS provider needs to have some campaign or to impose sanctions on criminals.
(5) Others ( )

Part K: Other

DQ1. What kinds of transportation do you use?
(1) Walk (2) Train (3) Bus (4) Taxi (5) Car (6) Bicycle

DQ2. Where do you mostly spend your time during the week?
(1) Home (2) School (3) Library (4) Office (5) Others

DQ3. Where do you mostly spend your time during the weekend?
(1) Home (2) Gym (3) Library (4) Multiplex mall for entertainment (5) Bar (6) Others

DQ4. What is your profession?
(1) Manager/specialist (2) Office worker (3) Sales person
(4) Agricultural and fisher expert (5) Basic level worker (6) Basic level Office worker (7) Military officer (8) Housewife (9) Student (10) Other

DQ5. What is your highest level of education?
(1) Elementary school (2) Middle school (3) High school (4) College (5) University (6) Graduate school (7) None

DQ6. What is your average monthly income?
(1) 0 ~ $1000 (2) $1000 ~ $2000 (3) $2000 ~ $3000 (4) $3000 ~ $4000
(5) $4000 ~ $5000 (6) $5000 ~ $6000 (7) $6000 ~ $7000 (8) Over $7000

DQ7. How many family members reside in your home? Write down the number of family members.
Include yourself ( )

Appendix II: Descriptive Statistics

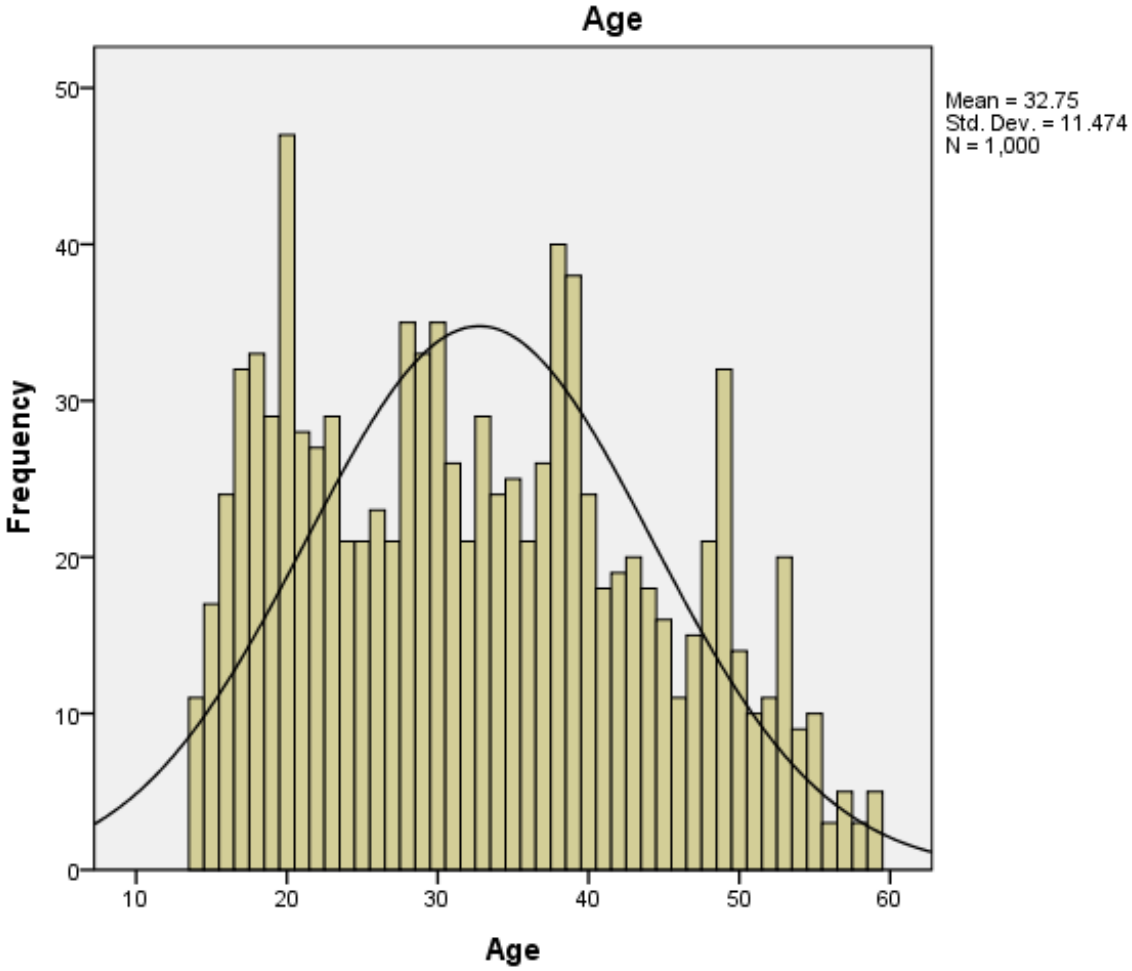
Statistics

		Age	Gender
N	Valid	1000	1000
	Missing	0	0
Mean		32.75	.5100
Std. Error of Mean		.363	.01582
Median		31.89[a]	.5100[a]
Mode		20	1.00
Std. Deviation		11.474	.50015
Variance		131.650	.250
Skewness		.265	-.040
Std. Error of Skewness		.077	.077
Kurtosis		-.947	-2.002
Std. Error of Kurtosis		.155	.155
Range		45	1.00
Minimum		14	.00
Maximum		59	1.00
Sum		32753	510.00

a. Calculated from grouped data.

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	490	49.0	49.0	49.0
	Male	510	51.0	51.0	100.0
	Total	1000	100.0	100.0	


Age
Mean = 32.75
Std. Dev. = 11.474
N = 1,000
Frequency
0
10
20
30
40
50
10
20
30
40
50
60
Age

Appendix III: Independent Measures

A. Digital Guardianship

Statistics

Lack_Digital_G

N	Valid	1000
	Missing	0
Mean		2.3500
Std. Error of Mean		.03732
Median		2.0000
Mode		2.00
Std. Deviation		1.18021
Variance		1.393
Skewness		-.224
Std. Error of Skewness		.077
Kurtosis		-.346
Std. Error of Kurtosis		.155
Range		6.00
Minimum		.00
Maximum		6.00
Sum		2350.00

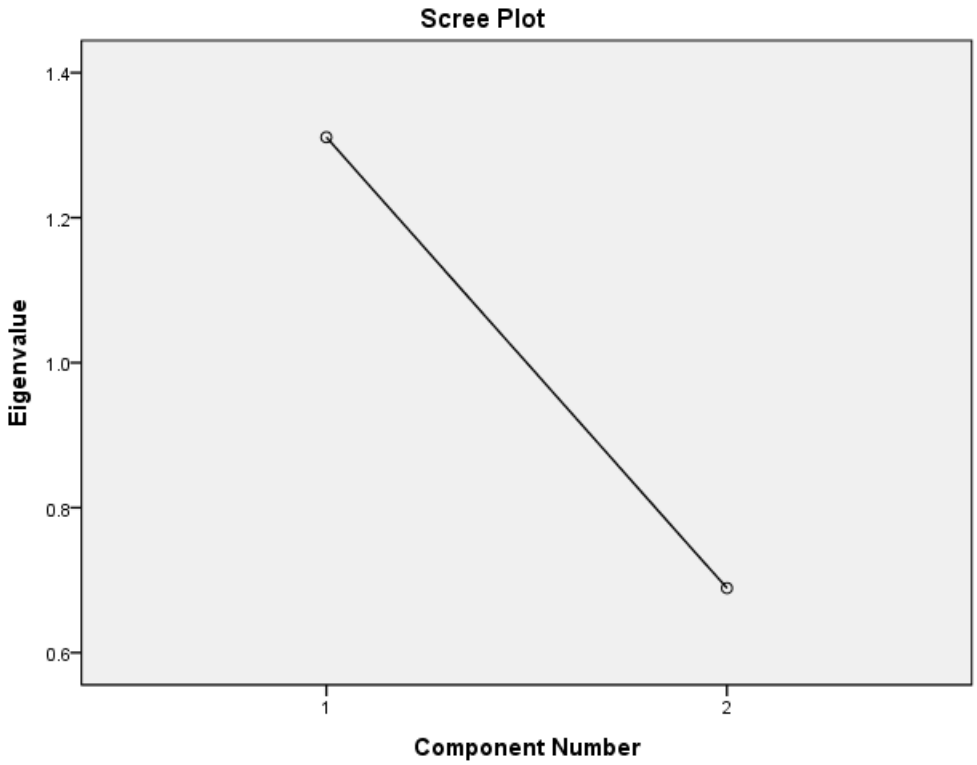
Lack_Digital_G

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	91	9.1	9.1	9.1
	1.00	102	10.2	10.2	19.3
	2.00	366	36.6	36.6	55.9
	3.00	261	26.1	26.1	82.0
	4.00	168	16.8	16.8	98.8
	5.00	11	1.1	1.1	99.9
	6.00	1	.1	.1	100.0
	Total	1000	100.0	100.0	

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.311	65.550	65.550	1.311	65.550	65.550
2	.689	34.450	100.000			

Extraction Method: Principal Component Analysis.



Component Matrix[a]

	Component
	1
8_1_Digital Guardianship (SNS Security)	.810
8_2_Application to make new friendships	.810

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Parameter Estimates

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test			Exp(B)	95% Wald Confidence Interval for Exp(B)	
			Lower	Upper	Wald Chi-Square	df	Sig.		Lower	Upper
(Intercept)	-.070	.0890	-.245	.104	.619	1	.431	.932	.783	1.110
[New_Gender=.00]	.182	.1238	-.061	.424	2.157	1	.142	1.199	.941	1.529
[New_Gender=1.00]	0[a]	.	.	.	.	.	.	1	.	.
Digital_Guardian	**.062**	**.0195**	**.023**	**.100**	**9.981**	**1**	**.002**	**1.064**	**1.024**	**1.105**
[New_Gender=.00] * Digital_Guardian	-.058	.0275	-.112	-.004	4.486	1	.034	.943	.894	.996
[New_Gender=1.00] * Digital_Guardian	0[a]	.	.	.	.	.	.	1	.	.
(Scale)	.262[b]	.0117	.240	.286						

Dependent Variable: Cyber_H_S=New_Q12_8 + New_Q12_9 + New_12_10 + New_Q12_11

Model: (Intercept), New_Gender, Digital_Guardian, New_Gender * Digital_Guardian

a. Set to zero because this parameter is redundant.

b. Maximum likelihood estimate.

B. Risky online lifestyle

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.766	.771	3

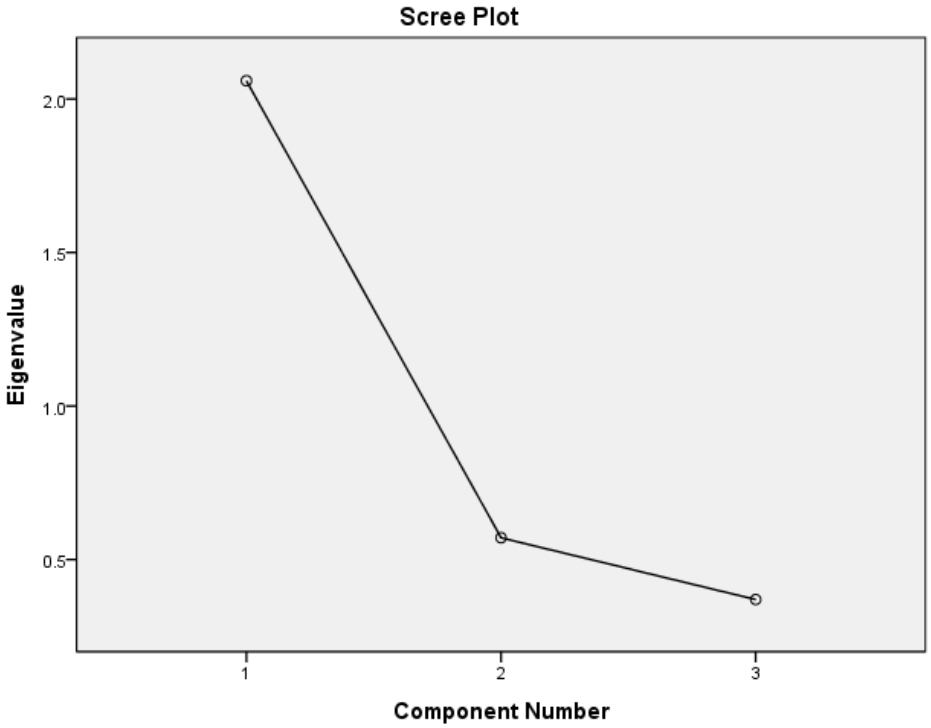
Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
35_2_Downloading illegally software online	2.66	1.053	.565	.336	.734
35_3_Watching or Downloading porn videos/movies	2.78	1.031	.680	.467	.590
35_4_Slandering someone online	2.97	1.298	.571	.358	.723

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.059	68.642	68.642	2.059	68.642	68.642
2	.571	19.032	87.673			
3	.370	12.327	100.000			

Extraction Method: Principal Component Analysis.



Component Matrix[a]

	Component
	1
35_2_Downloading illegally software online	.798
35_3_Watching or Downloading porn videos/movies	.876
35_4_Slandering someone online	.809

Extraction Method: Principal Component Analysis.

Component Matrix[a]

	Component
	1
35_2_Downloading illegally software online	.798
35_3_Watching or Downloading porn videos/movies	.876
35_4_Slandering someone online	.809

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

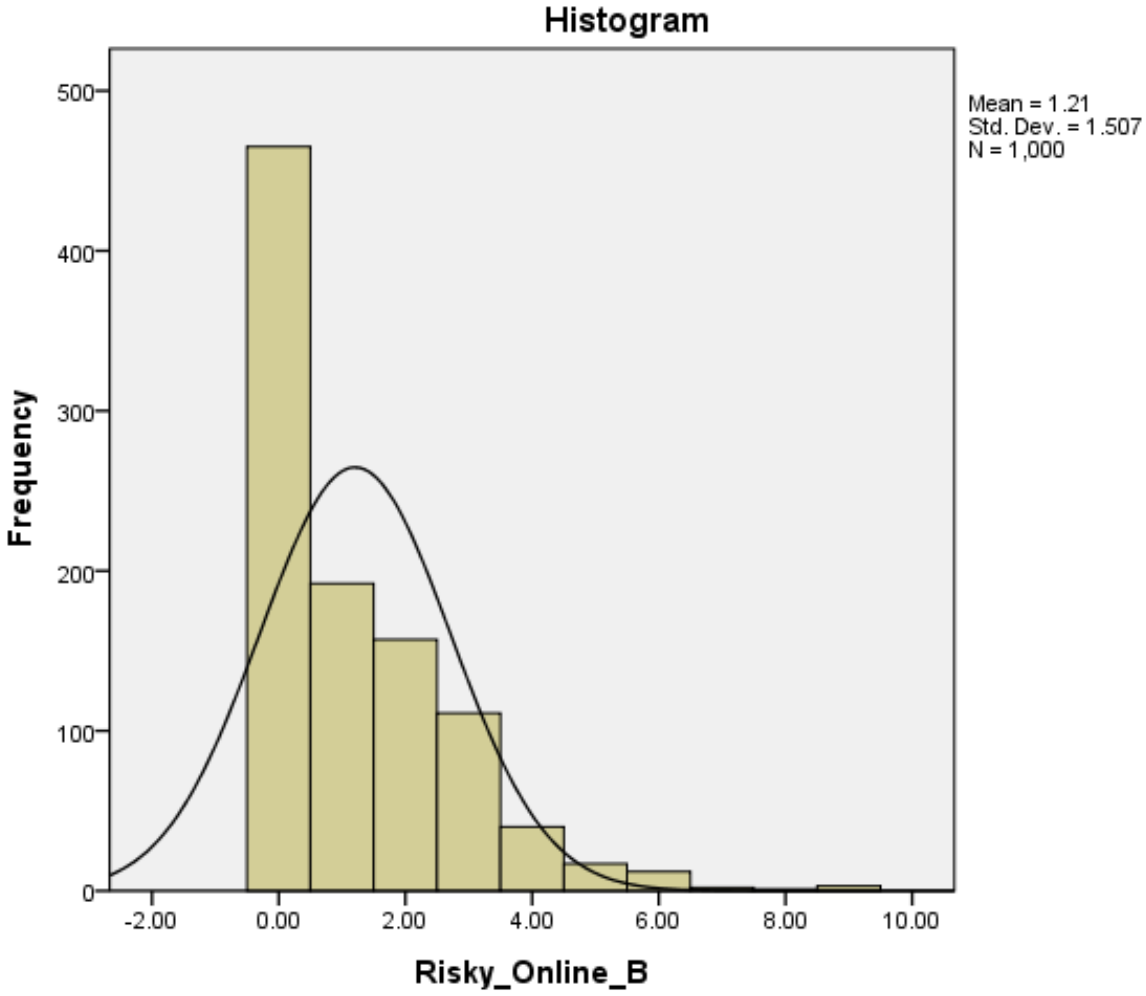
Risky_Online_Behavior: Q35_2 + Q35_3 + Q35_4

Statistics

Risky_Online_B

N	Valid	1000
	Missing	0
Mean		1.2050
Std. Error of Mean		.04766
Median		.8143[a]
Mode		.00
Std. Deviation		1.50707
Variance		2.271
Skewness		1.511
Std. Error of Skewness		.077
Kurtosis		2.842
Std. Error of Kurtosis		.155
Range		9.00
Minimum		.00
Maximum		9.00
Sum		1205.00

a. Calculated from grouped data.


Histogram
Mean = 1.21
Std. Dev. = 1.507
N = 1,000
Frequency
500
400
300
200
100
0
-2.00
0.00
2.00
4.00
6.00
8.00
10.00
Risky_Online_B

Parameter Estimates

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test			Exp(B)	95% Wald Confidence Interval for Exp(B)	
			Lower	Upper	Wald Chi-Square	df	Sig.		Lower	Upper
(Intercept)	-2.331	.3161	-2.950	-1.711	54.375	1	.000	.097	.052	.181
[New_Gender=.00]	-.899	.5147	-1.908	.110	3.051	1	.081	.407	.148	1.116
[New_Gender=1.00]	0[a]	.	.	.	.	.	.	1	.	.
Risky_Online_Behavior	**.153**	**.0603**	**.035**	**.271**	**6.429**	**1**	**.011**	**1.165**	**1.035**	**1.312**
[New_Gender=.00] * Risky_Online_Behavior	.131	.1079	-.080	.343	1.478	1	.224	1.140	.923	1.409
[New_Gender=1.00] * Risky_Online_Behavior	0[a]	.	.	.	.	.	.	1	.	.
(Scale)	1[b]									
(Negative binomial)	1									

Dependent Variable: Cyber_H_S=New_Q12_8 + New_Q12_9 + New_12_10 + New_Q12_11

Model: (Intercept), New_Gender, Risky_Online_Behavior, New_Gender * Risky_Online_Behavior

a. Set to zero because this parameter is redundant.

b. Fixed at the displayed value.

C. Online Lifestyle

SNSs Usage

1-4 Facebook

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	539	53.9	53.9	53.9
	1	2	.2	.2	54.1
	4	1	.1	.1	54.2
	5	7	.7	.7	54.9
	10	30	3.0	3.0	57.9
	15	5	.5	.5	58.4
	19	1	.1	.1	58.5
	20	21	2.1	2.1	60.6
	25	4	.4	.4	61.0
	30	32	3.2	3.2	64.2
	35	1	.1	.1	64.3
	40	28	2.8	2.8	67.1
	45	4	.4	.4	67.5
	50	26	2.6	2.6	70.1
	55	4	.4	.4	70.5
	60	43	4.3	4.3	74.8
	65	1	.1	.1	74.9
	70	44	4.4	4.4	79.3
	75	2	.2	.2	79.5
	80	42	4.2	4.2	83.7
	90	24	2.4	2.4	86.1
	95	6	.6	.6	86.7
	99	1	.1	.1	86.8
	100	132	13.2	13.2	100.0
	Total	1000	100.0	100.0	

1-4 KaKaostory

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	190	19.0	19.0	19.0
	1	1	.1	.1	19.1
	5	6	.6	.6	19.7
	9	2	.2	.2	19.9
	10	30	3.0	3.0	22.9
	15	6	.6	.6	23.5
	20	40	4.0	4.0	27.5
	25	7	.7	.7	28.2
	30	43	4.3	4.3	32.5
	35	4	.4	.4	32.9
	40	33	3.3	3.3	36.2
	45	4	.4	.4	36.6
	50	28	2.8	2.8	39.4
	55	4	.4	.4	39.8
	60	31	3.1	3.1	42.9
	70	47	4.7	4.7	47.6
	80	40	4.0	4.0	51.6
	85	2	.2	.2	51.8
	90	31	3.1	3.1	54.9
	95	2	.2	.2	55.1
	98	1	.1	.1	55.2
	99	3	.3	.3	55.5
	100	445	44.5	44.5	100.0
	Total	1000	100.0	100.0	

Parameter Estimates

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test			Exp(B)	95% Wald Confidence Interval for Exp(B)	
			Lower	Upper	Wald Chi-Square	df	Sig.		Lower	Upper
(Intercept)	-.604	.4300	-1.446	.239	1.971	1	.160	.547	.235	1.270
[New_Gender=.00]	**-1.689**	**.8306**	**-3.316**	**-.061**	**4.133**	**1**	**.042**	**.185**	**.036**	**.941**
[New_Gender=1.00]	0[a]	.	.	.	.	.	.	1	.	.
Q1_43	**-.013**	**.0048**	**-.022**	**-.004**	**7.314**	**1**	**.007**	**.987**	**.978**	**.996**
Q1_41	-.008	.0049	-.018	.001	2.852	1	.091	.992	.982	1.001
[New_Gender=.00] * Q1_43	.014	.0090	-.004	.031	2.339	1	.126	1.014	.996	1.032
[New_Gender=1.00] * Q1_43	0[a]	.	.	.	.	.	.	1	.	.
[New_Gender=.00] * Q1_41	.015	.0094	-.004	.033	2.479	1	.115	1.015	.996	1.034
[New_Gender=1.00] * Q1_41	0[a]	.	.	.	.	.	.	1	.	.
(Scale)	1[b]									
(Negative binomial)	1									

Dependent Variable: Cyber_H_S=New_Q12_8 + New_Q12_9 + New_12_10 + New_Q12_11

Model: (Intercept), New_Gender, Q1_43, Q1_41, New_Gender * Q1_43, New_Gender * Q1_41

a. Set to zero because this parameter is redundant.

b. Fixed at the displayed value.

Known SNS friends vs. Cyber H-S Victimization

Parameter Estimates

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test			Exp(B)	95% Wald Confidence Interval for Exp(B)	
			Lower	Upper	Wald Chi-Square	df	Sig.		Lower	Upper
(Intercept)	1.085	.4536	.196	1.974	5.717	1	.017	2.958	1.216	7.197
[New_Gender=.00]	-2.078	.7830	-3.613	-.543	7.043	1	.008	.125	.027	.581
[New_Gender=1.00]	0[a]	.	.	.	.	.	.	1	.	.
Q5_01	**-.033**	**.0056**	**-.044**	**-.022**	**34.135**	**1**	**.000**	**.968**	**.957**	**.979**
[New_Gender=.00] * Q5_01	.020	.0092	.002	.038	4.884	1	.027	1.021	1.002	1.039
[New_Gender=1.00] * Q5_01	0[a]	.	.	.	.	.	.	1	.	.
(Scale)	1[b]									
(Negative binomial)	1									

Dependent Variable: Cyber_H_S=New_Q12_8 + New_Q12_9 + New_12_10 + New_Q12_11

Model: (Intercept), New_Gender, Q5_01, New_Gender * Q5_01

a. Set to zero because this parameter is redundant.

b. Fixed at the displayed value.

General Info: New_Q7A1 + New_Q7A2

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.755	87.739	87.739	1.755	87.739	87.739
2	.245	12.261	100.000			

Extraction Method: Principal Component Analysis.

Age & Photo: New_Q7C12 + New_Q7C13

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.315	65.743	65.743	1.315	65.743	65.743
2	.685	34.257	100.000			

Extraction Method: Principal Component Analysis.

Occupation: New_Q7A4 + New_A7A5

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.606	80.302	80.302	1.606	80.302	80.302
2	.394	19.698	100.000			

Extraction Method: Principal Component Analysis.

Private Info: New_Q7A6 + New_Q7A7+ New_Q7A13

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	1.693	56.440	56.440	1.693	56.440	56.440
2	.716	23.875	80.315			
3	.591	19.685	100.000			

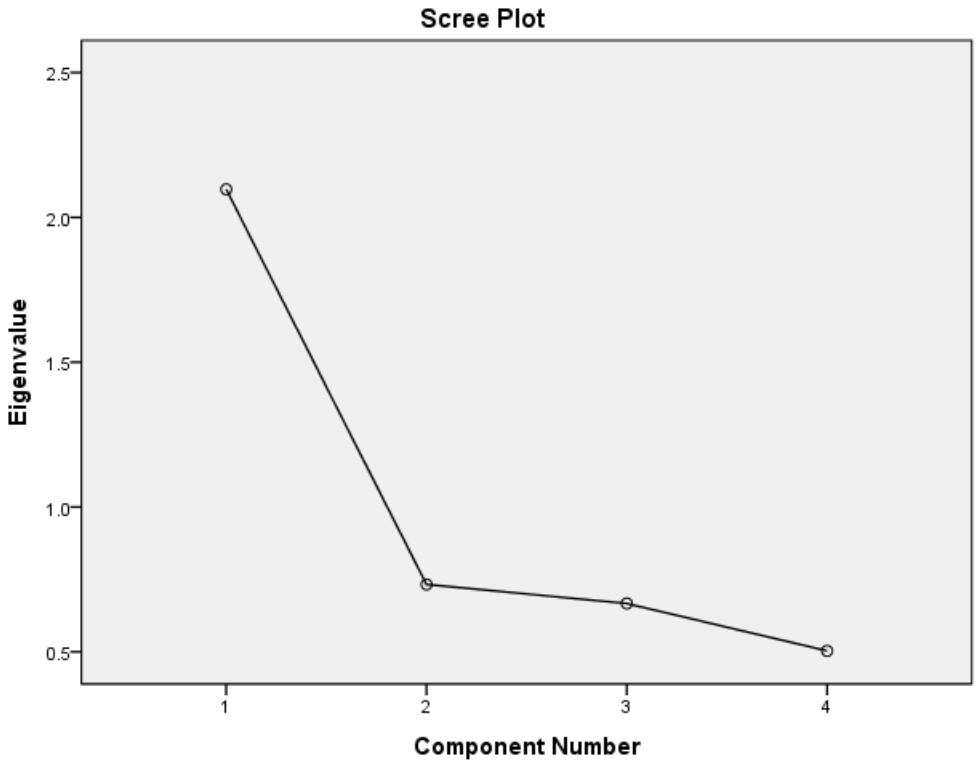
Extraction Method: Principal Component Analysis.

Personal Contact-Facebook: New_Q7A8 + New_Q7A9 + New_Q7A10 + New_Q7A11

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.097	52.424	52.424	2.097	52.424	52.424
2	.733	18.319	70.742			
3	.667	16.675	87.417			
4	.503	12.583	100.000			

Extraction Method: Principal Component Analysis.



Component Matrix[a]

	Component
	1
7_A8 Facebook	.732
7_A9 Facebook	.756
7_A10 Facebook	.713
7_A11 Facebook	.694

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

Appendix IV: Dependent Measure

Cyber-Harassment Victimization

Statistics

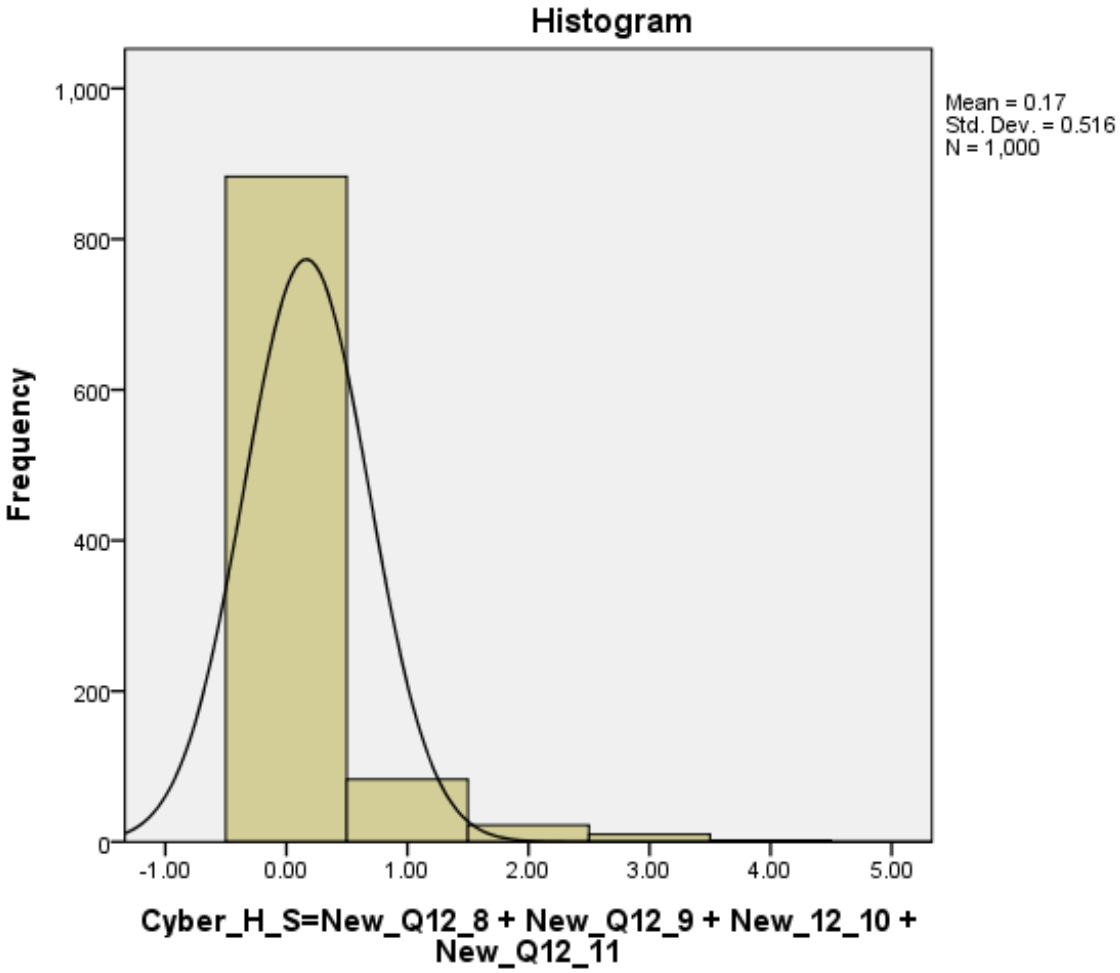
Cyber_H_S=New_Q12_8 + New_Q12_9 + New_12_10 + New_Q12_11

N	Valid	1000
	Missing	0
Mean		.1650
Std. Error of Mean		.01631
Median		.1211[a]
Mode		.00
Std. Deviation		.51579
Variance		.266
Skewness		3.808
Std. Error of Skewness		.077
Kurtosis		16.469
Std. Error of Kurtosis		.155
Range		4.00
Minimum		.00
Maximum		4.00
Sum		165.00

a. Calculated from grouped data.

Cyber_H_S=New_Q12_8 + New_Q12_9 + New_12_10 + New_Q12_11

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	.00	883	88.3	88.3	88.3
	1.00	83	8.3	8.3	96.6
	2.00	22	2.2	2.2	98.8
	3.00	10	1.0	1.0	99.8
	4.00	2	.2	.2	100.0
	Total	1000	100.0	100.0	


Histogram
Mean = 0.17
Std. Dev. = 0.516
N = 1,000
Frequency
1,000
800
600
400
200
0
-1.00
0.00
1.00
2.00
3.00
4.00
5.00
Cyber_H_S=New_Q12_8 + New_Q12_9 + New_12_10 + New_Q12_11

Final Model:

Parameter Estimates

Parameter	B	Std. Error	95% Wald Confidence Interval		Hypothesis Test			Exp(B)	95% Wald Confidence Interval for Exp(B)	
			Lower	Upper	Wald Chi-Square	df	Sig.		Lower	Upper
(Intercept)	-3.601	.4976	-4.576	-2.625	52.356	1	.000	.027	.010	.072
[New_Gender=.00]	**1.496**	**.7082**	**.108**	**2.884**	**4.462**	**1**	**.035**	**4.464**	**1.114**	**17.889**
[New_Gender=1.00]	0[a]	.	.	.	.	.	.	1	.	.
Lack_Ditigal_G	**.238**	**.0994**	**.043**	**.433**	**5.717**	**1**	**.017**	**1.268**	**1.044**	**1.541**
Risky_Online_B	**.182**	**.0530**	**.078**	**.286**	**11.816**	**1**	**.001**	**1.200**	**1.081**	**1.331**
Unknown_Friends	**.032**	**.0057**	**.020**	**.043**	**30.433**	**1**	**.000**	**1.032**	**1.021**	**1.044**
[New_Gender=.00] * Lack_Ditigal_G	**-.309**	**.1528**	**-.608**	**-.009**	**4.077**	**1**	**.043**	**.734**	**.544**	**.991**
[New_Gender=1.00] * Lack_Ditigal_G	0[a]	.	.	.	.	.	.	1	.	.
[New_Gender=.00] * Unknown_Friends	**-.020**	**.0096**	**-.039**	**-.001**	**4.293**	**1**	**.038**	**.980**	**.962**	**.999**
[New_Gender=1.00] * Unknown_Friends	0[a]	.	.	.	.	.	.	1	.	.
(Scale)	1[b]									
(Negative binomial)	1									

Dependent Variable: Cyber_H_S=New_Q12_8 + New_Q12_9 + New_12_10 + New_Q12_11

Model: (Intercept), New_Gender, Lack_Ditigal_G, Risky_Online_B, Unknown_Friends, New_Gender * Lack_Ditigal_G, New_Gender * Unknown_Friends

a. Set to zero because this parameter is redundant.

b. Fixed at the displayed value.

Correlations and Covariances between Variables

	G	LDG	ORB	UN
Gender	1 - .250			
Lack Digital Guardianship	.055 .082 .033	1 - 1.393		
Online Risky Behavior	.238** .000 .180	.118** .000 .210	1 - 2.271	
Unknown Friends	.029 .366 .246	.183** .000 3.713	.045 .151 1.178	1 - 295.9

The top value in each cell is the correlation coefficient. The value below it is the variances or covariances

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Appendix V: Formal/Informal Capable Guardianship

Formal Capable Guardianship

14_Reporting to Police

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I have never reported it	180	18.0	97.3	97.3
	I have reported it	5	.5	2.7	100.0
	Total	185	18.5	100.0	
Missing	System	815	81.5		
Total		1000	100.0		

14_1_Reason for Not Reporting to Police

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I did not feel like taking the time to report it to the police	28	2.8	15.6	15.6
	I thought the evidence of the crime was not enough to catch the offender	14	1.4	7.8	23.3
	I thought it was not an issue to report to the police	3	.3	1.7	25.0
	My victimization was not serious	135	13.5	75.0	100.0
	Total	180	18.0	100.0	
Missing	System	820	82.0		
Total		1000	100.0		

14_2_Satisfaction with Solution of Police

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I was satisfied with the service of the police, but the offender was not captured	3	.3	60.0	60.0
	I was not satisfied with the service of the police and the offender was not captured	2	.2	40.0	100.0
	Total	5	.5	100.0	
Missing	System	995	99.5		
Total		1000	100.0		

Informal Capable Guardianship

15_Reporting to SNS Provider

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I did not	173	17.3	93.5	93.5
	I did	12	1.2	6.5	100.0
	Total	185	18.5	100.0	
Missing	System	815	81.5		
Total		1000	100.0		

15_1_ Reason for Not Reporting to SNS Provider

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	My victimization was not serious	105	10.5	60.7	60.7
	I did not feel like taking the time to report it to the provider	48	4.8	27.7	88.4
	I thought it was not an issue to report to the company	3	.3	1.7	90.2
	I thought even if I report it, it might not be changed	17	1.7	9.8	100.0
	Total	173	17.3	100.0	
Missing	System	827	82.7		
Total		1000	100.0		

15_2_Satisfaction with Solution of SNS Provider

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly not satisfied	2	.2	16.7	16.7
	Not satisfied	6	.6	50.0	66.7
	Satisfied	3	.3	25.0	91.7
	Strongly satisfied	1	.1	8.3	100.0
	Total	12	1.2	100.0	
Missing	System	988	98.8		
Total		1000	100.0		