ASIAN COMMUNICATION RESEARCH

e-ISSN 2765-3390, p-ISSN 1738-2084
https://doi.org/10.20879/acr.2024.21.007

Original Research

Mapping the Influences of Social Network Site Use on Cybercrime Victimization: Trends and Recommendations

Huong Thi Ngoc Ho[1], Hai Thanh Luong[2], and Quang Anh Phan[3]

[1] School of Journalism and Information Communication, Huazhong University of Science and Technology

[2] School of Social Science, The University of Queensland

[3] VNU School of Interdisciplinary Sciences and Arts

Corresponding to
Quang Anh Phan
VNU School of Interdisciplinary Sciences and Arts, Block G7, 144 Xuan Thuy Road, Cau Giay District, Hanoi, Vietnam.
Email: phanquanganh@vnu.edu.vn

Disclosure Statement
No potential conflict of interest was reported by the author.

Received
29 Jan 2024
Revised
23 Feb 2024
Accepted
29 Feb 2024

ABSTRACT

Many online criminals are now targeting those who use social networking sites (SNSs). However, there is a lack of studies that provide a broad overview of the relationship between SNS use and cybercrime victimization. We undertake a comprehensive literature assessment of an articles series found in various databases to address this information gap. This work aims to assess the current state of scholarship reflecting how SNS use affects cybercrime victimization regarding the theories used, the forms of cybercrime studied, the variables investigated, and the key findings. The results indicated that the Routine Activities Theory was the most frequently employed theory; nevertheless, its effectiveness in explaining cybercrime victimization was controversial. In addition, most research has focused on cyberbullying, but numerous types of cybercrime have received less attention. The main predictors of cybercrime victimization were examined based on the dimension of basic use of SNS, and the psychological, social, and demographic attributes of users. Several recommendations are also provided for future research.

KEYWORDS

social networking sites, social networks, cybercrime victimization, online victimization, review.

SNSs are networked communication platforms that allow users to create a public or semi-public profile. Accordingly, SNSs contain user-provided content and display the interaction with user-generated content on the sites; these platforms also articulate connection lists viewed and traversed by others (Boyd & Ellison, 2008). Historically, SixDegress, established in 1997, marked the beginning of SNSs. Since then, the world has witnessed the explosion of a multitude of SNSs, such as Cyworld (2001), Friendster (2002), LinkedIn (2003), Myspace (2003), Facebook (2004), and Twitter (2006). Although SNSs are forms of social media, not all forms of social media can

be classified as SNSs (Carr & Hayes, 2015). Social media contains many communication forms, including blogs, photo and video-sharing platforms, social games, and SNSs (Carr & Hayes, 2015; Rus & Tiemensma, 2017).

Currently, these SNSs have become part of the daily life of many people (Jun & Firdaus, 2023; Pyun & Kim, 2023) and have attracted the growing concern of the academic community (Boyd & Ellison, 2008). Users join SNSs for many purposes, ranging from building and maintaining relationships, socializing, and time-killing (Brandtzæg & Heim, 2009) to entertaining, searching for information in various formats such as text, audio, or visual messages (Cappella & Li, 2023; Roslan et al., 2022)(Roslan et al., 2022), creating an ideal image (Dunne et al., 2010), or obtaining self-enhancement (Lin & Lu, 2011). Despite obvious and enormous advantages, SNSs have exposed undeniable negative influences and drawbacks (Baccarella et al., 2018; Fox & Moreland, 2015), such as physical and mental health problems (Das & Sahoo, 2011; Rajkarnikar & Shrestha, 2017), users' deviant behavior of users (Moreno et al., 2013; Vannucci et al., 2020), the spread of cyberhate messages (Lee-Won et al., 2021; Lee, 2021) and especially risks of cybercrime victimization (Kirwan et al., 2018; Lee et al., 2019; Leukfeldt, 2014). SNSs are assumed to provide a wide range of suitable conditions for perpetrators to commit cybercrimes (Benson et al., 2015; Reyns et al., 2011).

Cybercrime refers to any illegal activity or harm performed using network technology (Wall, 2008). According to popular belief, cybercrime is a new criminal activity that can only be carried out using computers and the Internet (Drew, 2020). Furthermore, it encompasses the more conventional forms of criminal activity that use information and communication technology (ICT) to commit crimes (Luong et al., 2019; Nguyen & Luong, 2021). Those who end up being the primary targets of this type of criminal activity also have a specific profile. The term 'cybercrime victimization' refers to "the practice of victimizing others through the use of information and communication technology" (Roberts, 2009, p. 591). Cybercrime victims can be people and institutions (Näsi et al., 2015). The victim is an essential component in determining the level of success that a cybercrime will have. In cyberspace, information includes "intellectual property, intelligence, information systems, and services of various kinds" (Newman & Clarke, 2003, p. 18); users can share it voluntarily on SNSs, making it one of the criminogenic elements and targets of cybercrimes (Newman & Clarke, 2003). The availability of personal information on SNSs increases the chances of being victimized by cybercrime. For example, cybercriminals can illegally use someone's personal information (i.e. name, birthday, photos) to commit impersonation and cyberscams. In particular, there is an increase of cyberscams relating to deepfake AI based on images, videos, and audios which were published via SNSs. It raised questions about safety within SNSs and the directions for managing SNS development in the future. Therefore, it is worth evaluating the relationships between SNS use and cybercrime victimization.

However, a holistic review that provides a more detailed description of the research status of this topic is scarcely documented. There have been several review articles focusing on SNS (Nef et al., 2013; Rus & Tiemensma, 2017; Saiphoo et al., 2020; Williams, 2019) or cybercrime victimization (Abdullah & Jahan, 2020; Gardella et al., 2017) separately, while few of the research articles have reviewed a specific type of cybercrime on social media (Kumar & Sachdeva, 2019), revealing that the lack of review work that connects SNSs and cybercrime victimization is a noticeable research gap. By conducting a systematic review of studies related to the connection between SNS use and cybercrime victimization, current research aims to (1)

synthesize applied theories, types of cybercrime, main variables, and findings; (2) identify the influence of SNS use on cybercrime victimization; and (3) identify research gaps and directions for the future. Specifically, the current paper proposes to answer three research questions (RQs), which are

RQ1: Which theories and types of cybercrime were applied to investigate the connection between SNS use and cybercrime victimization?
RQ2: What are the main constructs/variables used to investigate the relationship between SNS use and cybercrime victimization?
RQ3: How does SNS use affect cybercrime victimization?

After the method, the answers to these three questions will be presented in the Results and Discussion section, with further suggested directions for future research made available in the Recommendation section. In addition, the Concluding remarks will generalize the contributions and limitations of the article.

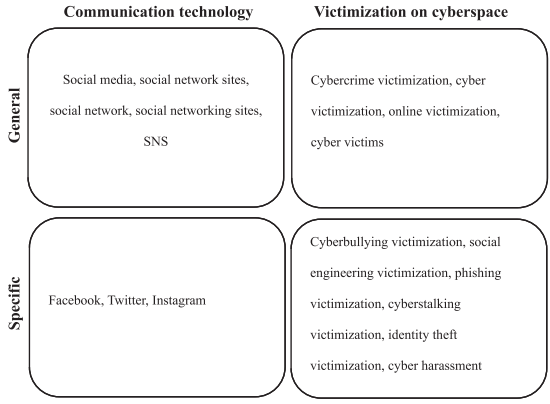
METHODS

Search Strategy

A systematic review of the literature collects and categorizes various studies (Williams, 2019) and answers specific questions by addressing connections between these studies (Baumeister & Leary, 1997). The studies included in this article reflect the influences of SNS use on cybercrime victimization. Therefore, search terms were actual words of the given topic, divided into two dimensions: (1) search terms for communication technology and victimization in cyberspace and (2) general terms and specific terms. Based on search terms from other review articles on SNS (Chen et al., 2023; Newman et al., 2021; Rus & Tiemensma, 2017; Saiphoo et al., 2020) and cybercrime victimization (Ho & Luong, 2022) as well as the synthesis of keywords in the research on cybercrime victimization from 2010 to 2020 (Ho & Luong, 2022), the current article selected several of the most used keywords. More details are provided in Figure 1.

Keywords were combined to search using the appropriate Boolean terms. Search terms were applied to databases of Scopus, Web of Science – Social Science Citation Index (WoS-SSCI),

Figure 1. *Groups of Search Terms*



and Web of Science – Science Citation Index-Expanded (WoS-SCIE). These databases are the central search system for conducting a systematic literature review (Gusenbauer & Haddaway, 2020; Zyoud et al., 2018).

Four main inclusion criteria were applied according to the topic, objectives, and scope of this investigation. First, all journal articles were in English since most of the research indexed in selected databases is compiled in this language. Second, the studies must be empirical and quantitative; variables of SNS use and cybercrime victimization were measured by the respondents' self-report because the current research plans to observe the relations between these variables. Third, the construct of SNS use can include various elements concerning SNS, such as frequency of use, behaviors on SNS, and characteristics of SNS or SNS users; the construct of cybercrime victimization could be related to experience, susceptibility, or risks of cybercrime victimization. Fourth, the selected studies must address how SNS use, as the independent variable, impacts cybercrime victimization as the dependent variable.

Furthermore, excluded papers are identified according to several criteria: (1) not journal articles and not written in English; (2) not empirical research, qualitative research, no inferential statistics; (3) investigate the perspective of ICT, the Internet, social media or SNS use but have no the variable of cybercrime victimization; (4) focus on the perspective of cybercrime victimization but lack elements of SNS use (the general Internet or social media use were not accepted) or SNS use is not examined as an affecting factor; (5) other perspectives of cybercrimes beyond victimization (i.e. legal issues, offenders, or policies); and (6) other cases which are irrelevant to studied topic.

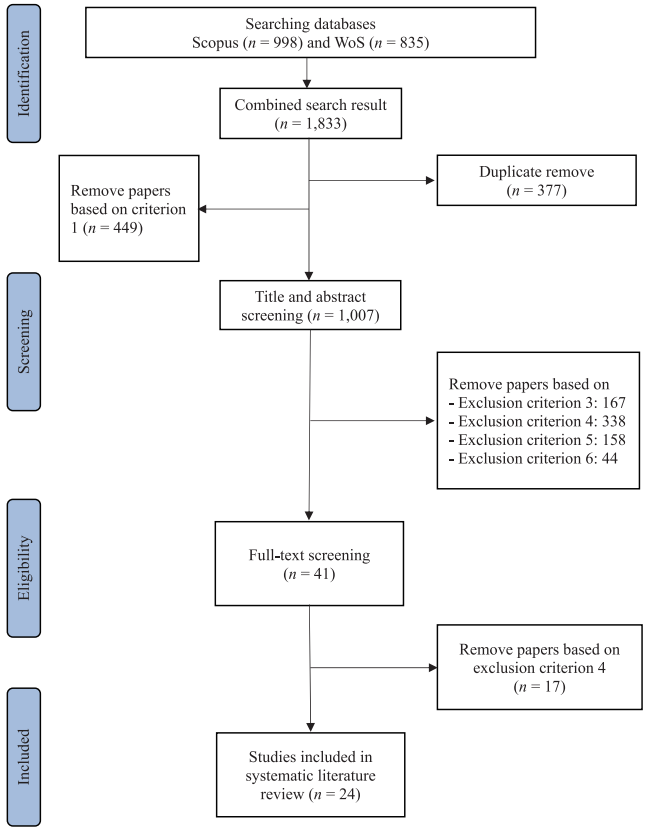
Data Collection Procedure

PRISMA - Preferred Reporting Items for Systematic Reviews and Meta-Analyses (Moher et al., 2009) were used for collecting data because it provides a straightforward and suitable procedure for review research, with more details presented in Figure 2. The selected keywords were retrieved from Scopus and WoS in January 2023. The data files were exported automatically; the initial result included 1833 documents (998 Scopus papers and 835 WoS-SSCI and WoS-SCIE papers). This study used R Studio to merge data files from two databases and remove 377 duplicates. In the Excel file, by filtering in the column of language and document types, 449 documents were released due to the exclusion of criterion one (not in English, review articles, book chapters, notes, letter, conference review, conference paper, proceeding paper, corrections, and editorial materials).

Then, 1007 papers were selected by title and abstract. First, an author wrote a draft classifying the screened articles, including three groups: 1) eligible articles were highlighted in yellow, 2) excluded articles were highlighted in red, and 3) papers that needed more consideration were highlighted in gray. The excluded articles were divided into subgroups according to the exclusion criteria. Then, based on the draft, the authors worked together to discuss and make the final decision for each article.

As a result, 966 studies were excluded. Specifically, 259 articles were removed due to the second exclusion of criterion 2. Numerous articles were qualitative research, systematic review, comparative study, measurement development, applied case study, discourse analysis, content analysis, deep learning, or machine learning. One hundred and sixty-seven articles were removed due to the third exclusion criterion (examined the use of social networks, the Internet, online dating sites, and gaming sites without variables of cybercrime victimization). A plethora of studies focused on the consequences of cybercrime victimization or factors that affect other factors, except SNS use (358 articles) were removed

Figure 2. *The PRISMA Diagram Depicts Data Collections*



based on the fourth exclusion criterion. Some studies addressed the relationship between the general use of the Internet or social networks and victimization by cybercrimes, but they were also removed. The current research targeted SNSs due to the different attributes of SNSs compared to other types of ICT. Furthermore, according to the fifth exclusion criterion, 138 articles related to the prevalence of cybercrime, offenders, intervention, prevention, or detection of cybercrimes were removed. Due to exclusion criterion six, 44 cases aimed at exploring traditional crime, issues of law and policies, or psychological issues were unsuitable for the current study.

41 articles were reviewed in full text, and 17 were removed after review and discussion among the authors. Although these studies covered both elements of SNS use and cybercrime victimization, they did not indicate the influence of the former on the latter or applied descriptive analysis only. The final eligible articles were 24.

Analytical Approach

The current study uses content analysis to explore the given topic because this analytical approach is suitable for text data and supporting interpretation from systematic data synthesis

(Krippendorff, 1989). Quantitative and qualitative analysis is combined to describe the status of applied theories and types of cybercrime and interpret the influences of SNS use on cybercrime victimization.

To provide answers to the research questions and in the hope that we would be able to move beyond the basic details of the studies that were examined, such as titles, authors, years of publication, and overall objectives, we designed this study to synthesize the data into four distinct categories, including 1) employed theories, 2) examined cybercrimes, 3) main independent variables, and 4) key findings. Data from categories one and two are for the first research question; the others were used for the second and third questions.

RESULTS AND DISCUSSION

There were 24 studies on the given topic. Table 1 summarizes the reviewed studies, including authors, titles, years, aims, theories, types of cybercrime, independent variables, and critical findings.

Research Question 1

Applied Theories. Half of the reviewed research was theory-driven (12 out of 24 studies); the others did not apply a specific theory but were based on the relevant literature for theoretical frameworks. The most frequently employed theory was Routine Activity Theory (RAT, seven out of 12 theory-driven studies)

RAT (Cohen & Felson, 1979) was originally used to explain traditional crime victimization and then widely applied to cybercrime

Table 1. *Summary of the Research Included*

Study	Objective	Theory, Sample & Types of cybercrime	Independent Variable	Key Finding
Social networking and online self-disclosure as predictors of cyberbullying victimization among children and youth (Aizenkot, 2020)	Test SNS activity, online self-disclosure, and education phrases as predictors of CV	N/A; *n* = 5,581; 3rd to 12th grades; 52.4% females; Israel; Cyberbullying	SNS activity; online self-disclosure; education phrase; gender	(1) Internet and SNS activities positively affect cyberbullying victimization; (2) The more amount of personal details on an SNS profile, the more cyberbullying victimization; (3) Females were more active online than males but cyberbullying victimization was more prevalent in male students compared to female students; (4) Secondary school students spent more time online than primary school students but cyberbullying victimization was more prevalent in primary school students than the other group.
A LRAT approach to cybercrime victimization: An empirical assessment of SNS lifestyle exposure activities (Suh et al., 2020)	Examine the relationship between lifestyle exposure via SNS activities and CV	LRAT; *n* = 147; age 10–59; 59% females; Cyber harassment, cyber impersonation, cyber hacking	Lifestyle exposure via SNS activities; SNS privacy settings	(1) Less strict privacy settings increased the likelihood of cyber harassment and cyber impersonation victimization; (2) Expressing opinions or feelings increased cyber hacking victimization; (3) Disclosing SNS profile on SNS made the individual more vulnerable for CV; (4) Frequency of use and preferences disclosure on SNS did not predict CV.

Table 1. *Summary of the Research Included(Continued)*

Study	Objective	Theory, Sample & Types of cybercrime	Independent Variable	Key Finding
Online victimization, social media utilization, and cybercrime prevention measures (Miguel et al., 2020)	Test relationship between FB utilization and CV	LRAT; n = 209; M_{age}=23.30; 74% females; USA; Hacking, cyber impersonation, cyberbullying, identity theft, online romance scam, online fraud	FB utilization (intensity and extensity); demographics; prevention (mutuality, recognition, and control setting)	(1) FB utilization including intensity and extensity of use increased the frequency of victimization; (2) Individuals who did not value mutuality in accepting an online friend request are more likely to be victims of cybercrimes than ones who did the opposite; (3) Recognizing friend requesters did not affect online victimization; (4) The users who had privacy settings set to public were more likely to experience online victimization than ones had privacy settings set to private. (5) Males were less likely to be victims of cybercrime.
Cyber victimization among secondary students: Social networking time, personality traits, and parental education (Rodríguez-Enríquez et al., 2019)	Identify the association between CV and SNS use, personality, and parental education	N/A; n = 765; 56.5% girls; M_{age}=15.99; Spain; Cyberbullying	Personality traits; use of SNS and screen time; parental education	(1) Girls were victims of cybercrimes more than boys; (2) Individuals who spent more time on SNS, had a high level of emotional instability and extraversion, but a low level of conscientiousness, were more likely to be cyber victims; (3) Parental education was not significantly associated with cyber victimization.
Risk factors for SNS scam victimization among Malaysian students (Kirwan et al., 2018)	Identify risk factors associated with falling victim to malicious techniques (SNS scams)	RAT; n = 295; students; M_{age}=21.29; 73.9% female; Malaysia; Online scam	SNS use; personality; impulsiveness	(1) Using fewer devices for SNSs, being on an SNS for a longer duration, extraversion, and openness to experience increased CV; (2) Most impulsivity factors had a weak effect on SNS scam victimization.
Parent-child connections on SNS and Cyberbullying (Mesch, 2018)	Investigate the role of a parent-child connection on SNS in reducing risky online activities among youth and negative online experiences	RAT; 800 pairs of children-parents; Parents: 56.4% female, M_{age}= 45.06; Adolescent: M_{age}=14.51, 49% girls; USA; Cyberbullying	Parental control; Exposure to online risks	(1) Lying about age, having a public profile on SNS, and frequency of SNS use increased the exposure to cyberbullying and predicted negative experience on SNS; (2) Parent control on SNS had a negative association with the odds of cyberbullying victimization on SNS; (3) Being friend with parents on SNS reduced the likelihood of cyberbullying victimization; (4) Girls were more likely than boys to fall victimization. of cyberbullying.

Table 1. *Summary of the Research Included(Continued)*

Study	Objective	Theory, Sample & Types of cybercrime	Independent Variable	Key Finding
An empirical study on the susceptibility to social engineering in SNS: The case of FB (Algarni et al., 2017)	Investigate the influence of FB-based source features on users' vulnerability to SE victimization	SCT; n = 377; 60% females; Age: 18+; Social engineering/ phishing	Characteristics of FB sources; Credibility of sources	(1) Dimensions of source credibility that included perceived sincerity, perceived competence, perceived attraction, and perceived worthiness had positive relationships with susceptibility to SE victimization; (2) FB source characteristics had positive relationships with source credibility; (3) Women were more vulnerable to SE than men; (4) Young adults were more susceptible to SE.
Social tie strength and online victimization: An analysis of young people aged 15–30 years in four nations (Keipi et al., 2017)	Examine the association between the characteristics of the SNS user, the strength of social bonds, and the experience of hate victimization and harassment.	SNT; 555 Finnish, American 1,033, 978 German, 999 British; Age: 15-30; Online hate, online harassment	Demographic factors; SNS use; online and offline identification; the number of online and offline friends; quality of online and offline users' bonds	(1) SNS activity was positively associated with risks of hate victimization; (2) The number of online and offline friends had no association with negative experiences online; (3) Strong identification with online communities positively associated with the experience of hate victimization and harassment. (4) The quality of the interactions between users on the Internet was negatively associated with experiences of victimization hate and harassment.
One step forward, two steps back: Cyberbullying within SNS (Navarro et al., 2017)	Examine the relationship between SNS use and the risk of victimization.	RAT; n = 4,257; M_{age} = 15; USA; Cyberbullying	Proximity to potential offenders; target suitability; guardianship	(1) The high amount of time spent on SNS per day increased the risk of cyberbullying victimization; (2) Specific activities within SNS such as bullying others, posting status updates and utilizing private messages increased the suitability of targets to potential offenders; (3) Increased guardianship (parental control) did not mitigate the risk of cyberbullying victimization on SNS; (4) Females were more likely to be victims of cyberbullying
Factors associated with online victimization among Malaysian adolescents who use SNS: A cross-sectional study (Marret & Choo, 2017)	Determine the association between online interpersonal victimization and patterns of SNS use, offline victimization, offline perpetration, and parental conflict	N/A; n = 1,478; students; age: 15-16; Malaysia; Online harass-ment, online sexual solicitation	Demographic characteristics; the prevalence of specific risky online behavior; online victimization; online perpetration; parent conflict; offline victimization; offline perpetration	(1) Boys had higher odds of victimization of online harassment victimization; (2) Participation in multiple types of online behavior increased the risk of online victimization; (3) Online and offline perpetrations had an association with an increased risk of victimization; (4) Offline victimization or parental conflict increased online victimization.

Table 1. *Summary of the Research Included(Continued)*

Study	Objective	Theory, Sample & Types of cybercrime	Independent Variable	Key Finding
Differences in friendship networks and experiences of cyberbullying among Korean and Australian adolescents (Lee et al., 2017)	Investigate connections between friendship networks in an online setting and experiences of cyberbullying victimization.	N/A; Korean (n = 520); Australian (n = 401); adolescents, age 12-15; Australia and Korea; Cyberbullying	The quantity of online and offline friends; demographics	The numbers of online and offline friends were positively associated with victimization by cyberbullying.
A lifestyle exposure perspective of victimization through FB among university students. Do individual differences matter? (Kokkinos & Saripanidis, 2017)	Examine the association between individual differences, risk factors, and risky FB lifestyles and FB victimization	LET; n = 240; students; M_{age} = 21.54; FB users; Greece; Cyberbullying	Personality; self-esteem; depression; loneliness; FB account; time spent on FB; number of FB friends; knowledge of FB privacy settings; use of FB privacy settings; self-disclosure; indiscreet FB content.	(1) Depression, loneliness, positive attitudes towards indiscreet FB content, high self-disclosure, high spent time on FB, large number of FB friends, no use of FB privacy settings had a positive effect on FB victimization; (2) Low self-esteem and high extraversion were not significantly associated with FB victimization; (3) Low agreeableness and low conscientiousness increased victimization; (4) Knowledge of FB privacy settings had no significant correlation with online victimization; (5) No significant association between gender and age and FB victimization.
Individual information security, user behavior, and cyber victimization: An empirical study of social networking users (Saridakis et al., 2016)	Test relationship between online victimization and user activity and perceptions of personal information security on SNS	RAT; TRA; TPB; n = 514; social network users; Spam, online fraud, offensive content, harassment	SNS usage; perceived control over information; computer efficacy; perceived risk; risk propensity	(1) High-risk propensity increased CV; (2) Perceived information control decreased the risk of becoming victims; (3) Multipurpose dominant use of SNS had a negative and significant association with online victimization; (4) SNS activities for knowledge exchange were positively correlated with online victimization; (5) computer efficacy had no effect on the risk of victimization.
Targets of online hate: Examining determinants of victimization among young Finnish FB users (Räsänen et al., 2016)	Evaluate the correlation between the risk of online hate victimization and online activities, and being offline victims.	RAT; n = 723; FB user; M_{age} = 16.6; 65.1% female; Finland; Online hate	online hate victimization; demographic factors; offending and victimization; online activities	(1) Actively searching for online hate material, producing online hate material, accessing online sites with risky content, concerning future online victimization, and offline victimization were positively associated with the risk of online hate victimization; (2) The number of Facebook friends, gender, and age did not predict victimization.

Table 1. *Summary of the Research Included(Continued)*

Study	Objective	Theory, Sample & Types of cybercrime	Independent Variable	Key Finding
Use of Social Networking Sites and the Risk of Cyberbullying Victimization: A population-level study of adolescents (Sampasa-Kanyinga & Hamilton, 2015)	Test association between SNS use and victimization of cyberbullying	N/A; *n* = 5,329, middle and high school students, age: 11-20; Canada; Cyberbullying	SNS use; demographics	(1) Time spent using SNS was positively associated with cyberbullying victimization; (2) There were no gender differences in the relationship between the use of SNSs and cyberbullying victimization.
Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem? (Peluchette et al., 2015)	Examine the impact of risky SNS practices, Self-disclosure and personality on the likelihood of cyberbullying victimization	N/A; *n* = 572; young adult FB users; 52.9% male; M_{age} = 22.1; USA and Australia; Cyberbullying	Demographic factors; SNS use; personality; self-disclosure; indiscreet content of FB profile	(1) Posting indiscreet content, having FB friends posting indiscreet content, the number of FB friends and the frequency of SNS use were positively associated with CV; (2) Extroversion and openness had a positive association with victimization by cyberbullying.
The strong, the weak, and the unbalanced: The link between tie strength and cyberaggression on a SNS (Wegge et al., 2015)	Examine the relationship between bond strength on FB and cyberaggression.	N/A; *n* = 1,229; Secondary school students; FB users; Belgium; Cyber harassment, cyberbullying	Social relationships; FB friendships	(1) The number of FB connections was positively associated with cyber aggression victimization; (2) Exposure to and interaction with FB-only friends (not friends at school) increased the risk of cyber harassment victimization.
Cyberbullying victimization prevalence and associations with internalizing and externalizing problems among adolescents in six European countries (Tsitsika et al., 2015)	Investigate the prevalence of cyber victimization and the factors associated with CV	N/A; *n* = 10,930; age: 14-17; Female/Male: 5,719/5,211; Spain, Poland, Netherland, Romania, Iceland, Greece; Cyberbullying	Demographics; SNS and internet use; emotional, behavioral, and academic problems	(1) The high frequency of using the internet and SNS increased cyber victimization; (2) There was a significant gender difference in cyber victimization; (3) Age was not significantly correlated with cyber victimization.
Habitual FB use and its impact on getting deceived on social media (Vishwanath, 2015)	Examine the link between FB habits and susceptibility to phishing attacks on FB	N/A; *n* = 150; senior graduate communication students; USA; Online scam, phishing	Frequency of FB use; FB habit strength; deficient self-regulation; number of FB friends; concern for privacy; attitudinal commitment	(1) The frequency of FB use, the number of friends on SNS, and lack of self-regulation were positively associated with phishing attacks on SNS. (2) Users with high privacy concerns were less likely to be victims of cybercrimes.

Table 1. *Summary of the Research Included(Continued)*

Study	Objective	Theory, Sample & Types of cybercrime	Independent Variable	Key Finding
Exposure to online hate among young social media users (Oksanen et al., 2014)	Investigate online hate material victimization among FB users	N/A; n = 723; M_{age}=16.6; 471 females; Finland; Online hate material	Online activity; attachment; happiness; offline victimization; sociographic characteristics	The high intensity of activity on the SNSs, poor attachment to the family, and physical offline victimization increased online hate victimization.
Online social networking and the experience of cyberbullying (O'Dea & Campbell, 2012)	Examine the relationship between online social networks and the experience of cyberbullying	N/A; n = 400; M_{age} = 14.31; 54.8% females; Australia; Cyberbullying	Internet and SNS use; perception of cyberbullying	Having SNS accounts was a stronger predictor of cyberbullying victimization compared to the time spent on SNS.
Predicting online harassment victimization among a juvenile population (Bossler et al., 2012)	Find out the risk factors of online harassment victimization	RAT; n = 434; middle and high school students; 51.2% female; USA; Online harassment	Proximity to motivated offenders; guardianship; suitable target	(1) Maintaining SNS, having peers harassing online, and posting sensitive information online increased online harassment victimization; (2) Protective software which was used by parents increased the risk of harassment victimization; (3) Females were more vulnerable to be victims of online victimization.
Risky eBusiness: An examination of risk-taking, online disclosiveness, and cyberstalking victimization (Welsh & Lavoie, 2012)	Investigate the application of RAT to explain cyberstalking victimization in SNS	RAT; n = 321, female students; M_{age}=20.03 Canada; Cyberstalking	Online exposure; online self-disclosure; risk-taking	(1) Online exposure and risk-taking were positively associated with cyberstalking victimization; (2) Levels of online self-disclosure had a direct positive impact on cyberstalking victimization.
Security in the 21st century: Examining the link between online social network activity, privacy, and interpersonal victimization (Henson et al., 2011)	Explore the association between SNS activity and SNS security and interpersonal online victimization	N/A; 974 young people; M_{age}=21; USA; online harassment, online sexual solicitation	Demographic; basic social network information	Engaging in risky online behaviors, such as opening numerous SNS accounts and adding strangers as friends, were more likely to be victims of interpersonal cybercrime.

Note. CV = Cybercrime victimization; FB = Facebook; SNS = Social network sites; LRAT = Lifestyle-Routine Activity Theory; RAT = Routine Activity Theory; LET = Lifestyle Exposure Theory, SCT = Source Credibility Theory, SNT = Social Network Theory, TRA = Theory of Reasoned Action, TPB = Theory of Planned Behavior.

victimization (Kirwan et al., 2018). Three core components of RAT are (1) motivated offenders, (2) suitable targets, and (3) the absence of capable guardianship. According to RAT, the victimization event was the result of the spatiotemporal convergence of motivated

offenders and suitable targets without capable guardianship. A motivated offender refers to a person who has the capacity and motivation to commit a crime and is seeking prey (i.e. scammers, hackers, stalkers; Nguyen, 2020). This component is often examined as 'exposure to motivated offender', which is the accessibility of victims to potential offenders. Suitable targets are various from a person or an organization to confidential data, online payment, online services, or computer systems that may be opportunistic or targeted selection due to certain attributes and circumstances. Unlike traditional crime, spatiotemporal convergence is not necessary for cybercrimes to occur because the offenders and victims may be online at different times and a long physical distance. Capable guardianship includes factors that protect potential victims from victimization. Given the context of cybercrime, guardianships can be in numerous forms ranging from human factors (i.e. online administrators, online peers, parents) to non-human factors (i.e. anti-virus software, firewalls, passwords, two-step verification; Leukfeldt & Yar, 2016).

Several studies comprehensively examined all three components (Bossler et al., 2012; Navarro et al., 2017; Räsänen et al., 2016; Saridakis et al., 2016; Welsh & Lavoie, 2012) while the others investigated one or two components (Kirwan et al., 2018; Mesch, 2018).

It is believed that the greater the exposure to potential offenders, the greater the victimization of cybercrime (Bossler et al., 2012; Navarro et al., 2017; Räsänen et al., 2016; Saridakis et al., 2016; Welsh & Lavoie, 2012). Some constructs used to measure the first component included the frequency of SNS use (Bossler et al., 2012; Kirwan et al., 2018; Mesch, 2018; Navarro et al., 2017; Saridakis et al., 2016; Welsh & Lavoie, 2012), years of SNS use (Kirwan et al., 2018), number of devices for SNS use (Kirwan et al., 2018), number of SNS accounts (Bossler et al., 2012), number of friends on SNSs (Räsänen et al., 2016), public profile on SNSs (Mesch, 2018), lying about age (Mesch, 2018), sharing a password (Mesch, 2018), activities on SNSs (i.e. commenting on friends' posts, sending private messages, tagging people in posts, updating statuses, posting video or photo, playing games on SNS; Mesch, 2018), online peer harassment (Bossler et al., 2012), and engaging in online deviance or offending (Bossler et al., 2012; Räsänen et al., 2016). Factors such as spent time, number of devices, number of friends, or online activities were supposed to increase the presence of users in cyberspace; hence, they also increased the exposure to offenders. Even though some constructs of the first component may cause confusion and should be better examined as measures of the second component (i.e. lying about age, sharing a password, or some specific online activities). The last two factors were included in the first component because participation in online deviance or connections with peers harassing others on SNSs put users into a larger community of offenders and deviants.

Relating to the suitable target component, previous research often examined personal factors such as risk-taking behaviors on SNSs (Saridakis et al., 2016; Welsh & Lavoie, 2012), low-risk perception (Saridakis et al., 2016), concerns about potential cybercrime victimization (Räsänen et al., 2016), prior negative offline experience (Räsänen et al., 2016), and demographic attributes of users (Bossler et al., 2012). Furthermore, the factor of activities on SNS (Navarro et al., 2017; Räsänen et al., 2016) and participation in online offending (Navarro et al., 2017) were also examined given the second component in several research works. These factors not only increased the online presence of users, leading to exposure to potential cybercriminals but could also be considered the characteristics of individuals that made them suitable targets for cybercrimes.

Regarding the last component, guardianships were supposed to decrease cybercrime victimization. Measures of guardianship can

be categorized as (1) physical guardianship, hardening a target from victimization; (2) social guardianship, the presence of individuals with the capacity to deter attacks or offer safeguard from crimes; and (3) personal guardianship, individuals' characteristics that protect them from crimes (Bossler et al., 2012). In previous research, physical guardianship included protective software programs (Bossler et al., 2012) and the location of using (Bossler et al., 2012). It was supposed that it was easier to control someone's online activities in the common area than in the private area to limit risky activities. Social guardianship focused on parental control (Mesch, 2018; Navarro et al., 2017; Räsänen et al., 2016), the connection of parent and child on SNSs (Mesch, 2018), and less peer computer deviance (Bossler et al., 2012). Personal guardianship consisted of information control (Saridakis et al., 2016), computer skills (Bossler et al., 2012; Saridakis et al., 2016), and less risky information sharing (Bossler et al., 2012; Welsh & Lavoie, 2012). Two variables 'peer computer deviance' and 'risky information sharing' were employed to measure the guardianship because Bossler et al. believed that the less peer computer deviance and sensitive information sharing, the more guardianship. However, these two variables were also used for the first and second components, respectively, in some different research, so it might create confusion somehow.

Several variables were used flexibly for more than one component of RAT in the different studies. For example, SNS activities and online offending were examined as the component of exposure to potential offenders (Mesch, 2018) and the component of target suitability (Navarro et al., 2017). It depended on the decisions of the researchers to categorize a construct into which component because each construct can be interpreted in several different directions. The phenomenon of overlap exists mainly in different research. Furthermore, it is noted that it often appeared when one work covered three components and the other examined one or two components only. In a special case, peer deviance was used to measure both the component of exposure to offenders and guardianships in the same research (Bossler et al., 2012). Bossler et al. recognized the complexity of the overlap, but they still categorized peer harassment as a variable of the first component and peer computer deviance as a measure of the third component. Furthermore, some components of RAT were more likely to be significant than others (Leukfeldt & Yar, 2016). Specifically, variables classified as exposure to offenders and suitable targets were more significantly correlated with cybercrime victimization than guardianships (i.e. locations of using SNSs, protective software, and computer skills had no effect on the risk of cybercrime victimization).

Similarly to RAT, Lifestyle Exposure Theory (LET, Hindelang et al., 1978) and Lifestyle-Routine Activity Theory (LRAT, Cohen et al., 1981) are in a group of criminal opportunity theories which were employed in the context of cybercrime victimization (LRAT was applied in two studies, and LET was applied in one study). These theories have close ties (Vakhitova et al., 2016). RAT was supposed to expand LET; LRAT integrated LET and RAT. While RAT describes the event of victimization itself (the convergence of three core components results in crime victimization), LET emphasizes the risk of victimization from the probabilistic perspective (Pratt & Turanovic, 2016). LET indicated that several people are at higher risk of crime victimization than others due to their lifestyle (Vakhitova et al., 2016). The lifestyle here is a set of daily activities (Madero-Hernandez, 2019) that contain vocational and leisure activities (Hindelang et al., 1978). Meanwhile, LRAT consisted of five elements: exposure, proximity, target attractiveness, guardianship, and properties of crimes (Cohen et al., 1981). Exposure to offenders refers to the visibility or accessibility of individuals to potential offenders.

Proximity to offenders refers to the physical distance between potential victims and offenders. Target attractiveness refers to "the material or symbolic desirability of persons or property target" (Cohen et al., 1981, p. 508), and levels of resistance to attack (McNeeley, 2015). In terms of guardianship, potential victims who are less well-guarded are more likely to be attacked. Last, properties of specific crimes are suggested to have close connections with possibilities for crimes and influence on four factors above. To explain victimization in cyberspace, LET and LRAT mainly asserted that online victimization was closely related to the victim's online lifestyle (Suh et al., 2020), for example, frequency of SNS use, disclosure of preference on SNSs, expression of opinions or feelings on SNSs, extensity and intensity of SNS use and risky lifestyle on SNSs.

LET, RAT and LRAT originally were applicable for traditional crimes (with direct contact between offenders and targets). LET just examines the risky factors increasing the probability of victimization while RAT and LRAT investigate the convergence of factors leading to the event of cybercrime victimization. It seems that LRAT comprehensively examines crime victimization through more elements than the others. However, given an online environment, the physical distance is blurred, and then the construct of proximity to offenders did not maintain the original meaning and was used interchangeably with exposure to offenders in some research (Bossler et al., 2012). Furthermore, it is difficult to examine the role of properties of a specific cybercrime in cybercrime victimization from the victim survey research. Previous research using LRAT often examined only three factors similar to RAT. Then, RAT was the most applied theory.

However, not all components of these theories had significant associations with cybercrime victimization. Some findings did not completely support the effectiveness of these theories (Navarro et al., 2017). Therefore, evaluating their value appeared challenging (Leukfeldt & Yar, 2016), leading to an argument about the usability of these theories in explaining cybercrimes. Furthermore, RAT, LET, and LRAT seemed suitable for "single entities" (van der Wagen & Pieters, 2020, p. 7) but not for "a chain or network of various human, technical, and/or virtual elements" (van der Wagen & Pieters, 2020, p. 7).

Despite the controversies, LET, RAT and LRAT are still critical theories for investigating victimization in both physical and virtual worlds. There is a lack of sufficient evidence to reject RAT, LET, and LRAT (Räsänen et al., 2016). These theories also demonstrated their benefits in explaining specific types of cybercrime victimization. The nature of each cybercrime and the characteristics of sample populations are different, so the usability of these theories can vary (Leukfeldt & Yar, 2016). Cybercrime was divided into two main categories, including cyber-enabled crimes (i.e. cyberfraud) and cyber-dependent crimes (i.e. hacking). The former usually involves more victim-related factors than the latter; meanwhile, the latter more involves technology than the former. It was obvious that RAT, LET and LRAT were likely to examine cybercrime from the perspective of human beings. As a result, their applications for cyber-enabled offenses, such as cyberbullying, were given preference. Furthermore, the result may be different in the alternative samples. For example, the frequency of SNS use was indicated to increase online victimization in the sample of adolescents or young people (Kokkinos & Saripanidis, 2017; Mesch, 2018; Miguel et al., 2020; Navarro et al., 2017; Peluchette et al., 2015) but no significant effect within the sample at the age of 10 to 59 (Suh et al., 2020). Another reason might be due to the restrictions of methods such as small non-representative samples in several research (Leukfeldt & Yar, 2016).

Beyond RAT, LET, and LRAT, other theories employed were the Theory of Reasoned Action

(TRA, Fishbein & Ajzen, 1975), the Theory of Planned Behaviors (TPB, Ajzen, 1985, 1991), the Social Tie Theory (STT) or Social Network Theory (SNT, Granovetter, 1973), and the Source Credibility Theory (SCT, Hovland & Weiss, 1951; Hovland et al., 1953). TPB was considered an advanced version of TRA. TRA indicated the relationships between attitudes, subjective norms, behavioral intention, and behavior. Beyond these factors, TPB included another factor, namely perceived behavioral control. In the literature, TRA and TPB were applied to account for SNS behaviors, and how SNS users decided to respond to an online request and became victims of cybercrimes on SNS (Saridakis et al., 2016). STT or SNT focuses on the construct of social ties or social networks that are a set of relationships between two or more individuals. Social ties may be categorized as strong or weak social ties. The strengths of social bonds were believed to play a protective role in both physical and virtual environments. Therefore, previous research evaluated the impact of social connection strength on cybercrime victimization (Keipi et al., 2017). Lastly, source credibility is a term that covers the positive characteristics of information or communication sources that impact the acceptance of information receivers of information (Ohanian, 1990). Source credibility theory asserted that receivers had the likelihood to believe and accept a message from a source that seemed to be credible (Hovland & Weiss, 1951). Therefore, this theory was used to investigate the effect of the credibility of the source on user behaviors and their risks of victimization online (Algarni et al., 2017).

While several different theories were examined, the quantity was modest because these theories did not aim to directly explain victimization as RAT, LET, or LRAT did. Instead, these theories cover some constructs that can affect victimization or explain victim behavior.

Types of Cybercrime. The reviewed studies concern a variety of cybercrimes, as shown in Table 1. Consistent with previous results, reviewed research focused mainly on cyber-enabled crimes, and cyberbullying was the most common cybercrime (50% of the total published articles), followed by cyberstalking and online harassment (33.3%), cyberscams such as phishing or romance scam (20.8%), online hate or offensive content (16.7%), and cyber impersonation and identity theft (12.5%). Some other cybercrimes, such as hacking (8.33%), online sexual solicitation on SNS (8.33%), or spam (4.16%) were scarcely documented. Except for cyberbullying, other cybercrimes were investigated less separately. Instead, they were measured as items for cybercrime victimization. For example, Saridakis et al. (2016) measured cybercrime victimization through several items including victimization of spam, online fraud, offensive content and online harassment; Suh et al. (2020) included some items relating to cyber harassment, cyber impersonation and cyber hacking in the variable of cybercrime victimization.

Table 2. *Frequency of Cybercrimes Examined*

Cybercrime	Frequency (%)
Cyberbullying	12 (50%)
Cyber harassment, cyberstalking	8 (33.3%)
Online scam (i.e., romance scam, phishing)	5 (20.8%)
Online hate, offensive content	4 (16.7%)
Cyber impersonation, identity theft	3 (12.5%)
Online sexual solicitation	2 (8.33%)
Hacking	2 (8.33%)
Spam	1 (4.16%)

Given that RAT and LRAT, the most common theories in previous studies, are suitable for cyber-enabled crimes and individual cases, it is understandable why cyberbullying was the most frequently examined. Furthermore, the rise of the Internet and SNS increases the risks of rapidly distributing toxic messages and

images (Choi & Lee, 2017). There are numerous opportunities for cyberbullying or harassment to become prevalent, appealing to the concerns of scholars. These types of cybercrime seem to be a decidedly special issue among children and youth (Aizenkot, 2020; Navarro et al., 2017), the most frequent population in research.

Research Question 2

The retrieved studies examined various variables which were categorized into two main groups: The first group was related to SNS experience (i.e. general use and activities on SNS), and the second group was related to the characteristics of users (psychological, social, and demographic attributes).

Variables of the SNS Experience. A wide range of research concerned factors regarding general SNS use such as the number of SNS accounts, frequency of use (years of SNS use or time spent on SNS), devices for SNS access, locations of use, mutual friends, recognition of friend requesters, SNS habit strength, deficient self-regulation, and privacy setting or self-disclosure (i.e. keep personal information including real name, facial photo, address, gender, age, phone number, email address in public or private setting). Of these variables, several were the most used in the studies, containing time spent, number of friends on SNS, number of SNS accounts and privacy settings.

Except for the variables of general use of SNS, the previous research also investigated variables of SNS activities. Numerous measured items were related to the most elementary features of SNS, such as updating profiles, posting photos or videos, adding friends, sending messages, leaving comments, tagging, posting status updates, sharing feelings, and playing games on SNSs. Besides, some risky online activities (i.e. bullying others, online offending, searching and accessing harmful content, interacting with strangers, and adding strangers as friends) were also important variables given the lens of LET, RAT, and LRAT.

Variables of SNS Users' Characteristics. In addition to SNS experience, other factors related to SNS users were tested to understand their relationships with the likelihood of victimization by cybercrimes, including psychological, social, and demographic aspects. Psychological factors were frequently examined variables, related to perception perspectives (i.e. the perception of source credibility, including perceived sincerity, competence, attraction and worthiness of the source; Algarni et al., 2017), personality (i.e. extraversion, agreeableness, conscientiousness, neuroticism, and openness; Kirwan et al., 2018; Peluchette et al., 2015), self-esteem (Kokkinos & Saripanidis, 2017), or emotion (i.e. depression, loneliness and fear; Kokkinos & Saripanidis, 2017; Räsänen et al., 2016). Social aspects of SNS users contained previous cybercrime experience (Räsänen et al., 2016), parental control (Bossler et al., 2012; Mesch, 2018), parent-child connection (Mesch, 2018; Navarro et al., 2017), social ties (Keipi et al., 2017; Wegge et al., 2015), offline victimization (Marret & Choo, 2017; Räsänen et al., 2016), offline perpetration (Marret & Choo, 2017), online peer deviance (Bossler et al., 2012), or parent conflict (Marret & Choo, 2017). Lastly, previous research mentioned demographic attributes of SNS users, such as gender, age, or education phrase.

Generally, previous research covered numerous basic factors of SNS experiences (general use and SNS activities) and explored them from the angle of risk factors rather than safety factors (Ngo et al., 2020). Most variables were selected under the lens of the RAT components as analyzed above. In addition to factors of general use of SNS and online activities, psychological factors were crucial to understanding how online victimization occurred. Numerous cybercrimes require certain levels of involvement; then, users' decision-making may open up more chances for cybercrime success (Ho & Luong,

2022). Furthermore, social and demographic factors provided cyber offenders with detailed descriptions of suitable targets.

There were very few variables regarding non-human factors (i.e. technological perspectives or features of social network platforms) to understand how suitable each platform is for properties of cybercrimes. The reasons may be partly due to the research method of the self-report survey and the theories applied.

Research Question 3

The use of SNSs positively influences cybercrime victimization in several aspects. The more SNS accounts, the higher the risk of interpersonal victimization (Henson et al., 2011) because a great number of SNS accounts gave potential offenders more avenues to access potential victims (Reyns, 2010). Numerous research indicated that the number of online friends positively affected cybercrime victimization (Choi & Lee, 2017; Kokkinos & Saripanidis, 2017; Peluchette et al., 2015; Wegge et al., 2015). Besides, individuals with longer duration of SNS use (Kirwan et al., 2018) and a high amount of daily time spent on SNS were likely to be victims of cybercrimes (Kokkinos & Saripanidis, 2017; Mesch, 2018; Miguel et al., 2020; Navarro et al., 2017; Peluchette et al., 2015).

The low level of privacy setting, the public nature of personal information in SNS (real name, facial photo, address, gender, age, phone number, email address), or the disclosure of personal information in SNS increased cybercrime victimization (Aizenkot, 2020; Kokkinos and Saripanidis, 2017; Suh et al., 2020; Tsitsika et al., 2015; Welsh & Lavoie, 2012). Online self-disclosure and lower privacy settings might leak sensitive information against users and turn them into suitable targets for offenders. Personal information was easily used for impersonation, identity theft, and other online scams. Users may encounter a higher risk of cyber harassment or online hate because personal information provides harassers with various materials for their villainous behaviors (Bossler et al., 2012). Furthermore, due to the centralized nature, information exploitation, and poor privacy of numerous SNS, users need to be increasingly concerned about privacy issues on these platforms, especially after the privacy violation case of Facebook. Most of the SNSs available to date may provide opportunities to exploit user content (Poongodi et al., 2020), and user's personal information is collected and used without permission. Therefore, information control played a role in decreasing the risk of victimization (Saridakis et al., 2016); users with high privacy concerns were less likely to be victims of cybercrimes (Vishwanath, 2015).

Hazardous SNS activities including sharing feelings on SNS (Suh et al., 2020), updating status regularly (Navarro et al., 2017), adding strangers as friends (Henson et al., 2011), submitting intimate images (Marret & Choo, 2017), interacting with strangers (Marret & Choo, 2017), online offending or online bullying (Marret & Choo, 2017), sharing inappropriate information (Kokkinos & Saripanidis, 2017), searching and accessing harmful content (Räsänen et al., 2016) had positive associations with cybercrime victimization. These activities, especially risky online activities, were supposed to increase the probability for users to expose themselves to offenders and turn them into attractive targets of attackers on SNS.

In addition to the experience of SNS, a wide range of psychological, social, and demographic attributes of SNS users were also positively associated with cybercrime victimization. Users who perceive the high credibility of SNS sources (via several characteristics of sources such as a large number of friends, using a real name for the source, mutual friends, or owned by celebrities) were easier to fall into social engineering-based attacks on Facebook. Another point is that users with high extraversion and openness

were positively associated with cyberbullying victimization (Peluchette et al., 2015) and SNS scam victimization (Kirwan et al., 2018). They were more willing to adopt risky online behaviors, which positively influenced the victimization of cybercrimes. Similarly, users with low agreeability and conscientiousness increased the risk of being victimized (Kokkinos & Saripanidis, 2017). Previous studies also found that people with higher depression, loneliness, and fear of victimization were likely to fall into Facebook victimization (Kokkinos & Saripanidis, 2017; Räsänen et al., 2016). Other users' problems, such as online and offline perpetrations, online and offline victimization, parental conflict, or peer harassment online, led to an increased rate of cybercrime victimization (Bossler et al., 2012; Marret & Choo, 2017; Räsänen et al., 2016). Several factors related to online relationships had negative associations with cybercrime victimization, such as being friends with parents on SNSs (Mesch, 2018) and the strengths of online relationships (Keipi et al., 2017). The former was indicated to mitigate the likelihood of cyberbullying victimization, and the latter reduced online hate and harassment victimization.

However, it was observed that there were some inconsistent results between different studies. There were no significant correlations between cybercrime victimization and variables related to the number of friends on SNS (Keipi et al., 2017; Räsänen et al., 2016), frequency of use (Suh et al., 2020), and parental control (Navarro et al., 2017). The reason for the differences in the results of the first two factors might be due to the different measures and coding methods in the different research. The factor of parental control was expected to be guardianship of protecting young users from cybercrimes. However, it was observed that the strengths of the relationship between parents and children were not the same within the different social-cultural communities. Hence, the inconsistent results related to parental control are understandable.

Inconsistency was also found in results for gender and age. From the perspective of gender, some findings suggested that women were more likely to become victims of cybercrime (Algarni et al., 2017; Mesch, 2018; Navarro et al., 2017; Rodríguez-Enríquez et al., 2019; Tsitsika et al., 2015) but others showed the opposite; men had higher risks of falling into cybercrime victimization (Aizenkot, 2020; Marret & Choo, 2017; Miguel et al., 2020). Several studies even indicated that gender had no association with cybercrime victimization (Kokkinos & Saripanidis, 2017; Räsänen et al., 2016). With age, young adults were more susceptible to social engineering (Algarni et al., 2017). Young people represented the largest and most active group of users on SNS (Baker & White, 2010; Subrahmanyam et al., 2008) , then their frequent presence and activities in cyberspace might increase the exposure to potential offenders and the risks of victimization according to RAT. However, most of the reviewed studies found that age had no connection with cybercrime victimization on SNS (Kokkinos & Saripanidis, 2017; Räsänen et al., 2016; Tsitsika et al., 2015).

The advantages of SNS are undeniable, and so are the drawbacks of SNS. The presence of cyberspace users or their participation in SNS activities might put them in negative experiences in various ways, especially given the lack of capable guardianships. Therefore, users are expected to fully perceive the risks of cybercrime victimization in SNSs and effectively control their attendance in cyberspace.

Recommendations

In addition to summarizing previous studies, the current article also aims to recommend directions for future studies. Therefore, the following subsections will discuss more directions for future research.

Recommendation 1: For Theory-based Approaches

RAT, LET, or LRAT are typical theories for understanding cybercrime from the perspective of victims. However, the effectiveness of these theories seems to be limited in the context of a few types of cybercrime and sample population (i.e. young people). It recommends future studies to employ them to explore other cybercrimes (mentioned below) and in a variety of sample populations (i.e. older adults). In addition, the overlap among measures of distinct components of the theories in the previous literature exposed the confusion and unclear insights of each component. It would be better for future research to strictly follow the operational definitions to ensure the separated roles of every component. Furthermore, it encourages various theories studied. Beyond the risk factors for cybercrime victimization, which have been frequently investigated, the effects of protection factors on cybercrime victimization must also be explored more (Ngo et al., 2020). Hence, it calls for theories related to protection factors in future research. For example, the Protection Motivation Theory (Rogers, 1975, 1983) or the COM-B framework (Michie et al., 2011) is an alternative consideration, providing information on cybercrime victimization from different aspects concerning SNS users' protective behaviors.

Recommendation 2. Exploring More Types of Cybercrime

Cybercrimes are diversified, but research conducted only touched upon certain types of cybercrime, leaving behind a lacuna of under-researched topics. Therefore, future studies should shift their focus to other growing types of cybercrime rather than simply focusing on several well-documented traditional criminal forms. Sextortion, e-Whoring, investment scams, cryptocurrency scams or other financial scams, and even cyberterrorism or politics-related online offenses are all dangerous cybercrimes that SNS users may encounter. Remarkably, during the explosion of COVID-19 and lockdown initiatives or social distancing orders, social networks became the central channels of social interaction (Király et al., 2020), and people changed their habits and daily activities by participating more in the virtual world (Ma & McKinnon, 2022). Since COVID-19, the increase in online shopping scams, romance scams, cyber-dependent crime (Buil-Gil & Zeng, 2022) and cyber sexual crime is observable. The effect of COVID-19 opens up more opportunities for perpetrators to hunt for prey from various SNS. Therefore, it is worth exploring how SNS use has changed after COVID-19 and affects some cybercrimes above.

Another point is that future research may consider cases related to institutions because victims of cybercrimes are not only particular people. Many institutions maintain their SNS accounts to maintain contact with stakeholders and serve other purposes. Therefore, the risks of cybercrime, particularly cyber-dependent crimes for institutions, are not rare and need to be better understood.

Recommendation 3: For the Variables Suggested

SNSs are noticed to be used for a wide range of specific purposes, typically socializing, entertaining, or even working. Therefore, it is worthy of considering several variables scarcely documented, including activities concerning groups or communities on SNS (i.e. joining and interacting in public and private groups of hobbies, works, or investment), activities of entertainment (i.e. joining games, quizzes, or integrated applications on SNSs), or other kinds of financial involvement (i.e. borrowing money from sources advertised on SNS or selling products/services via SNSs). In addition, as mentioned above, the effect of protection factors, including safety behaviors (i.e. fact-checking or verifying information), and safety policies of governments and social network companies, on cybercrime victimization should be investigated more.

Rapid changes in social media and SNSs lead to numerous online activities and behaviors less investigated in the literature. Similarly, it lacks the investigation of the influence of several new technologies-based SNSs. It is necessary to update the new developments of SNS and their relations with cybercrime victimization. It is worth exploring how the characteristics of SNSs, especially new technology-based SNSs, affect cybercrime victimization. Technology development always surprises people, from Yahoo, Google, Facebook, Twitter, Instagram, and TikTok to the revolution of AI, web 3.0 and Blockchain (Kobayashi et al., 2019). Recently, blockchain technology has been assumed to be "reliable for the storage of sensitive information" (Niranjanamurthy et al., 2019, p. 14743) because the decentralized approach ensures privacy. Currently, we can witness a transition to blockchain-based SNS (Poongodi et al., 2020), and one question here is to what extent blockchain-based SNS are safe for users. According to a SWOT assessment of blockchain, security against cybercriminals is still one of its weaknesses (Niranjanamurthy et al., 2019). This topic is less explored and may attract those interested in the use of SNSs and the victimization of cybercrimes.

Concluding Remarks

This review paper retrieved 24 journal articles on the influences of SNS usage on cybercrime victimization from the Scopus database, WoS-SSCI and WoS-SCIE. It synthesized applied theories, types of cybercrime, main variables, and key findings reflecting the influence of SNS use on cybercrime victimization. In most previous studies, RAT and LRAT were utilized to explore cybercrime victimization on SNSs, the focus being cyberbullying rather than other forms of cybercrime. The findings demonstrated an apparent association between SNS usage and being a victim of cybercrime in terms of the following two primary aspects: SNS experience (general use and particular activities in SNS) and SNS users' characteristics (psychological, social, and demographic attributes). There is little doubt that using SNS increases the risk of being a victim of cybercrime, although different studies have produced contradictory findings.

This research has been determined to have some shortcomings. Only major academic databases, including Scopus, WoS-SSCI, and WoS-SCIE, were used to retrieve the articles, and the articles examined had to be published in English and use quantitative research methodologies. Consequently, there was a possibility that not all articles related to the subject presented were investigated. The sample population and primary variables were summarized in the article; however, there was no in-depth analysis of the sample or the measurement scale of the variables. To learn more about various points of view, it is recommended that further research be conducted with eligible articles retrieved from other databases, such as the International Bibliography of the Social Sciences, PsychoINFO, or Communication and Mass Media Complete. Inclusion criteria must also be expanded to examine other types of methodology, including qualitative and mixed methods, and the papers selected can also be drafted in other languages. All these limitations should be called for further consideration in the future.

REFERENCES

Abdullah, A. T. M., & Jahan, I. (2020). Causes of cybercrime victimization: A systematic literature review. *International Journal of Research and Review, 7*(5), 89–98.

Aizenkot, D. (2020). Social networking and online self-disclosure as predictors of cyberbullying victimization among children and youth. *Children and Youth Services Review, 119*, 105695. https://doi.org/10.1016/j.childyouth.2020.

105695

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11–39). Springer. https://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T https://doi.org/10.1186/s42400-020-00047-5

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems, 26*(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y

Baccarella, C. V., Wagner, T. F., Kietzmann, J. H., & McCarthy, I. P. (2018). Social media? It's serious! Understanding the dark side of social media. *European Management Journal, 36*(4), 431–438. https://doi.org/10.1016/j.emj.2018.07.002

Baker, R. K., & White, K. M. (2010). Predicting adolescents' use of social networking sites from an extended theory of planned behaviour perspective. *Computers in Human Behavior 26*(6), 1591–1597. https://doi.org/10.1016/j.chb.2010.06.006

Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. *Review of General Psychology, 1*(3), 311–320. https://doi.org/10.1037/1089-2680.1.3.311

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Purpose of social networking use and victimisation: Are there any differences between university students and those not in HE? *Computers in Human Behavior, 51*(Part B), 867–872. https://doi.org/10.1016/j.chb.2014.11.034

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society, 44*(4), 500–523. https://doi.org/10.1177/0044118X11407525

Boyd, D. M., & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210–230.

Brandtzæg, P. B., & Heim, J. (2009). Why people use social networking sites. *OCSC 2009: Proceedings of the 3rd International Conference on Online Communities and Social Computing* (pp. 143–152). Springer. https://doi.org/10.1007/978-3-642-02774-1_16

Buil-Gil, D., & Zeng, Y. (2022). Meeting you was a fake: Investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime, 29*(2), 460–475. https://doi.org/10.1108/JFC-02-2021-0042

Cappella, J. N., & Li, Y. (2023). Principles of effective message design: A review and model of content and format features. *Asian Communication Research, 20*(3), 147–174. https://doi.org/10.20879/acr.2023.20.023

Carr, C. T., & Hayes, R. A. (2015). Social Media: Defining, developing, and divining. *Atlantic Journal of Communication, 23*(1), 46–65. https://doi.org/10.1080/15456870.2015.972282

Chen, Y., Sherren, K., Smit, M., & Lee, K. Y. (2023). Using social media images as data in social science research. *New Media & Society, 25*(4), 849–871. https://doi.org/10.1177/14614448211038761

Choi, K.-S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior, 73,* 394–402. https://doi.org/10.1016/j.chb.2017.03.061

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity

approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review, 46*(5), 505–524. https://doi.org/10.2307/2094935

Das, B., & Sahoo, J. S. (2011). Social networking sites - A critical analysis of its impact on personal and social life. *International Journal of Business and Social Science, 2*(14), 222–228.

Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice 6*(1), 17–33. https://doi.org/10.1108/JCRPP-12-2019-0070

Dunne, Á., Lawlor, M. A., & Rowley, J. (2010). Young people's use of online social networking sites - A uses and gratifications perspective. *Journal of Research in Interactive Marketing, 4*(1), 46–58. https://doi.org/10.1108/17505931011033551

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research.* Addison-Wesley.

Fox, J., & Moreland, J. J. (2015). The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances. *Computers in Human Behavior, 45,* 168–176. https://doi.org/10.1016/j.chb.2014.11.083

Gardella, J. H., Fisher, B. W., & Teurbe-Tolon, A. R. (2017). A systematic review and meta-analysis of cyber-victimization and educational outcomes for adolescents. *Review of Educational Research, 87*(2), 283–308. https://doi.org/10.3102/0034654316689136

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360–1380.

Gusenbauer, M., & Haddaway, N. R. (2020). Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. *Research Synthesis Methods, 11*(2), 181–217. https://doi.org/10.1002/jrsm.1378

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. https://doi.org/10.1177/0734016811399421

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

Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010-2020: A bibliometric analysis. *SN Social Science, 2,* 4. https://doi.org/10.1007/s43545-021-00305-4

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). *Communication and persuasion: Psychological studies of opinion change.* Yale University Press.

Hovland, C. I., & Weiss, W. (1951). The influence of source credibility on communication effectiveness. *The Public Opinion Quarterly, 15*(4), 635–650.

Jun, T. J., & Firdaus, A. (2023). Social media political information dependency (SMPID): Theorising news seeking in an age of sharing and posting. *SEARCH Journal of Media and Communication Research, 15*(1), 1–21.

Keipi, T., Kaakinen, M., Oksanen, A., & Räsänen, P. (2017). Social tie strength and online victimization: An analysis of young people aged 15-30 years in four nations. *Social Media + Society, 3*(1). https://doi.org/10.1177/2056305117690013

Király, O., Potenza, M. N., Stein, D. J., King, D. L., Hodgins, D. C., Saunders, J. B., Griffiths, M. D., Gjoneska, B., Billieux, J., Brand, M.,

Abbott, M. W., Chamberlain, S. R., Corazza, O., Burkauskas, J., Sales, C. M. D., Montag, C., Lochner, C., Grünblatt, E., Wegmann, E., … Demetrovics, Z. (2020). Preventing problematic internet use during the COVID-19 pandemic: *Consensus guidance. Comprehensive Psychiatry, 100,* 152180. https://doi.org/10.1016/j.comppsych.2020.152180

Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk factors for social networking site scam victimization among Malaysian students. *Cyberpsychology, Behavior, and Social Networking, 21*(2), 123–128. https://doi.org/10.1089/cyber.2016.0714

Kobayashi, N., Onodera, K., & Fujio, M. (2019). *Bajji: New generation of SNS based on weighted directed graph using blockchain transaction for visualizing trust between users.* https://www.researchgate.net/profile/Noritaka-Kobayashi/publication/333942627_bajji_new_generation_of_SNS_based_on_weighted_directed_graph_using_blockchain_transaction_for_visualizing_trust_between_users/links/5d0d9cda299bf1547c73c4fc/bajji-new-generation

Kokkinos, C. M., & Saripanidis, I. (2017). A lifestyle exposure perspective of victimization through Facebook among university students. Do individual differences matter? *Computers in Human Behavior, 74,* 235–245. https://doi.org/10.1016/j.chb.2017.04.036

Krippendorff, K. (1989). Content Analysis. In E. Barnouw, G. Gerbner, W. Schramm, T. L. Worth, & L. Gross (Eds.), *International Encyclopedia of Communication* (Vol. 1, pp. 403–407). Oxford University Press.

Kumar, A., & Sachdeva, N. (2019). Cyberbullying detection on social multimedia using soft computing techniques: A meta-analysis. *Multimedia Tools and Applications, 78*(17), 23973–24010. https://doi.org/10.1007/s11042-019-7234-z

Lee-Won, R. J., Lee, J. Y., White, T., & Lee, J. (2021). The not-so-obvious harm of cyberhate: Source magnification of hate tweets, unhealthy food choice, and the moderating role of group identification. *Asian Communication Research, 18*(3), 151–167. https://doi.org/10.20879/acr.2021.18.3.151

Lee, J. (2021). The effects of racial hate tweets on perceived political polarization and the roles of negative emotions and individuation. *Asian Communication Research, 18*(2), 51–68. https://doi.org/10.20879/acr.2021.18.2.51

Lee, J. Y., Kwon, Y., Yang, S., Park, S., Kim, E.-M., & Na, E.-Y. (2017). Differences in friendship networks and experiences of cyberbullying among Korean and Australian adolescents. *The Journal of Genetic Psychology, 178*(1), 44–57. https://doi.org/10.1080/00221325.2016.1242475

Lee, S.-S., Choi, K., Choi, S., & Englander, E. (2019). A test of structural model for fear of crime in social networking sites. *International Journal of Cybersecurity Intelligence & Cybercrime, 2*(2), 5–22. https://doi.org/10.52306/02020219SVZL9707

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Lin, K.-Y., & Lu, H.-P. (2011). Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in Human Behavior, 27*(3), 1152–1161. https://doi.org/10.1016/j.chb.2010.12.009

Luong, H. T., Phan, H. D., Van Chu, D., Nguyen,

V. Q., Le, K. T., & Hoang, L. T. (2019). Understanding cybercrimes in Vietnam: From leading-point provisions to legislative system and law enforcement. *International Journal of Cyber Criminology, 13*(2), 290–308. https://doi.org/10.5281/zenodo.3700724

Ma, K. W. F., & McKinnon, T. (2022). COVID-19 and cyber fraud: Emerging threats during the pandemic. *Journal of Financial Crime, 29*(2), 433–446. https://doi.org/10.1108/JFC-01-2021-0016

Madero-Hernandez, A. (2019). Lifestyle Exposure Theory of Victimization. In F. P. Bernat & K. Frailing (Eds.), *The Encyclopedia of Women and Crime* (pp. 1–3). John Wiley & Sons. https://doi.org/10.1002/9781118929803.ewac0334

Marret, M. J., & Choo, W. Y. (2017). Factors associated with online victimisation among Malaysian adolescents who use social networking sites: A cross-sectional study. *BMJ Open, 7*(6), e014959. https://doi.org/10.1136/bmjopen-2016-014959

McNeeley, S. (2015). Lifestyle-Routine Activities and Crime Events. *Journal of Contemporary Criminal Justice, 31*(1), 30–52. https://doi.org/10.1177/1043986214552607

Mesch, G. S. (2018). Parent-child connections on social networking sites and cyberbullying. *Youth & Society, 50*(8), 1145–1162. https://doi.org/10.1177/0044118X16659685

Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science, 6,* 42. https://doi.org/10.1186/1748-5908-6-42

Miguel, C. S., Morales, K., & Ynalvez, M. A. (2020). Online victimization, social media utilization, and cyber crime prevention measures. *Asia-Pacific Social Science Review, 20*(4), 123–135.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Journal of Clinical Epidemiology, 62*(10), 1006–1012. https://doi.org/10.1016/j.jclinepi.2009.06.005

Moreno, M. A., Kota, R., Schoohs, S., & Whitehill, J. M. (2013). The Facebook influence model: A concept mapping approach. *Cyberpsychology, Behavior, and Social Networking, 16*(7), 504–511. https://doi.org/10.1089/cyber.2013.0025

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16*(2), 203–210. https://doi.org/10.1080/14043858.2015.1046640

Navarro, J. N., Clevenger, S., Beasley, M. E., & Jackson, L. K. (2017). One step forward, two steps back: Cyberbullying within social networking sites. *Security Journal, 30*(3), 844–858. https://doi.org/10.1057/sj.2015.19

Nef, T., Ganea, R. L., Müri, R. M., & Mosimann, U. P. (2013). Social networking sites and older users - A systematic review. *International Psychogeriatrics, 25*(7), 1041–1053. https://doi.org/10.1017/S1041610213000355

Newman, G. R., & Clarke, R. V. (2003). Situational crime prevention in the information society. *Superhighway robbery: Preventing E-commerce crime* (pp. 1–240). Willan Publishing. https://doi.org/10.4324/9781843924876

Newman, L., Stoner, C., & Spector, A. (2021). Social networking sites and the experience of older adult users: A systematic review. *Ageing & Society, 41*(2), 377–402. https://doi.org/10.1017/S0144686X19001144

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B.

(2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review, 45*(4), 430–451. https://doi.org/10.1177/0734016820934175

Nguyen, T., & Luong, H. T. (2021). The structure of cybercrime networks: Transnational computer fraud in Vietnam. *Journal of Crime and Justice, 44*(4), 419–440. https://doi.org/10.1080/0735648X.2020.1818605

Nguyen, V. T. (2020). Cybercrime in Vietnam: An analysis based on routine activity theory. *International Journal of Cyber Criminology, 14*(1), 156–173. https://doi.org/10.5281/zenodo.3747516

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: Pros, cons and SWOT. *Cluster Computing, 22*(Suppl 6), 14743–14757. https://doi.org/10.1007/s10586-018-2387-5

O'Dea, B., & Campbell, A. (2012). Online social networking and the experience of cyber-bullying. *Annual Review of CyberTherapy and Telemedicine, 10*, 212–217. https://doi.org/10.3233/978-1-61499-121-2-212

Ohanian, R. (1990). Construction and validation of a scale to measure celebrity endorsers' perceived expertise, trustworthiness, and attractiveness. *Journal of Advertising, 19*(3), 39–52. https://doi.org/10.1080/00913367.1990.10673191

Oksanen, A., Hawdon, J., Holkeri, E., Näsi, M., & Räsänen, P. (2014). Exposure to online hate among young social media users. *Sociological Studies of Children and Youth, 18,* 253–273. https://doi.org/10.1108/S1537-46612014000018021

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

Poongodi, T., Sujatha, R., Sumathi, D., Suresh, P., & Balamurugan, B. (2020). Blockchain in social networking. In G. Shrivastava, D.-N. Le, K. Sharma (Eds.), *Cryptocurrencies and blockchain technology applications* (pp. 55–76). Scrivener. https://doi.org/10.1002/9781119621201.ch4

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders, 11*(3), 335–354. https://doi.org/10.1080/15564886.2015.1057351

Pyun, M., & Kim, Y. C. (2023). Social media dependency and civic engagement among older urban adults in Korea. *Asian Communication Research, 20*(3), 175–193. https://doi.org/10.20879/acr.2023.20.018

Rajkarnikar, N., & Shrestha, D. (2017). The impact of social networking sites on undergraduate students: A case study of Pokhara university. *Proceedings of the Fifth International Academic Conference for Graduates,* Nanjing, China.

Räsänen, P., Hawdon, J., Holkeri, E., Keipi, T., Näsi, M., & Oksanen, A. (2016). Targets of online hate: Examining determinants of victimization among young Finnish Facebook users. *Violence and Victims, 31*(4), 708–725. https://doi.org/10.1891/0886-6708.VV-D-14-00079

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety, 12*(2), 99–118. https://doi.org/10.1057/cpcs.2009.22

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber lifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior,*

38(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Roberts, L. D. (2009). Cybercrime-victimization. In R. Luppicini & R. Adell (Eds.), *Handbook of Research on Technoethics* (pp. 575–592). IGI Global.

Rodríguez-Enríquez, M., Bennasar-Veny, M., Leiva, A., Garaigordobil, M., & Yañez, A. M. (2019). Cybervictimization among secondary students: Social networking time, personality traits and parental education. *BMC Public Health, 19,* 1499. https://doi.org/10.1186/s12889-019-7876-9

Rogers, R. W. (1975). A Protection Motivation Theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–177). Guilford.

Roslan, N. W., Rahim, N. A., Hamid, T. M. H. T. A., Roslan, N. M., & Roslan, S. N. A. (2022). Facebook vs. Twitter: Social media platform selection for news consumption among undergraduate students. *SEARCH Journal of Media and Communication Research, 14*(3), 117–129.

Rus, H. M., & Tiemensma, J. (2017). "It's complicated." A systematic review of associations between social network site use and romantic relationships. *Computers in Human Behavior, 75,* 684–703. https://doi.org/10.1016/j.chb.2017.06.004

Saiphoo, A. N., Halevi, L. D., & Vahedi, Z. (2020). Social networking site use and self-esteem: A meta-analytic review. *Personality and Individual Differences, 153,* 109639. https://doi.org/10.1016/j.paid.2019.109639

Sampasa-Kanyinga, H., & Hamilton, H. A. (2015). Use of social networking sites and risk of cyberbullying victimization: A population-level study of adolescents. *Cyberpsychology, Behavior, and Social Networking, 18*(12), 704–710. https://doi.org/10.1089/cyber.2015.0145

Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change, 102,* 320–330. https://doi.org/10.1016/j.techfore.2015.08.012

Subrahmanyam, K., Reich, S. M., Waechter, N., & Espinoza, G. (2008). Online and offline social networks: Use of social networking sites by emerging adults. *Journal of Applied Developmental Psychology 29*(6), 420–433. https://doi.org/10.1016/j.appdev.2008.07.003

Suh, J., Choe, J., & Park, J. (2020). A lifestyle-routine activity theory (LRAT) approach to cybercrime victimization: An empirical assessment of SNS lifestyle exposure activities. *Asia Pacific Journal of Information Systems, 30*(1), 53–71. https://doi.org/10.14329/apjis.2020.30.1.53

Tsitsika, A., Janikian, M., Wójcik, S., Makaruk, K., Tzavela, E., Tzavara, C., Greydanus, D., Merrick, J., & Richardson, C. (2015). Cyberbullying victimization prevalence and associations with internalizing and externalizing problems among adolescents in six European countries. *Computers in Human Behavior, 51*(Part A), 1–7. https://doi.org/10.1016/j.chb.2015.04.048

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice, 32*(2), 169–188. https://doi.org/10.1177/1043986215621562

1379

van der Wagen, W., & Pieters, W. (2020). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology, 17*(4), 480–497. https://doi.org/10.1177/1477370818812016

Vannucci, A., Simpson, E. G., Gagnon, S., & Ohannessian, C. M. C. (2020). Social media use and risky behaviors in adolescents: A meta-analysis. *Journal of Adolescence, 79*(1), 258–274. https://doi.org/10.1016/j.adolescence.2020.01.014

Vishwanath, A. (2015). Habitual facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication, 20*(1), 83–98. https://doi.org/10.1111/jcc4.12100

Wagen, W. van der, & Pieters, W. (2020). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology, 17*(4), 480–497. https://doi.org/10.1177/1477370818812016

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology, 22*(1–2), 45–63. https://doi.org/10.1080/13600860801924907

Wegge, D., Vandebosch, H., Eggermont, S., & Walrave, M. (2015). The strong, the weak, and the unbalanced: The link between tie strength and cyberaggression on a social network site. *Social Science Computer Review, 33*(3), 315–342.

Welsh, A., & Lavoie, J. A. A. (2012). Risky eBusiness: An examination of risk-taking, online disclosiveness, and cyberstalking victimization. *Cyberpsychology, 6*(1), 4. https://doi.org/10.5817/CP2012-1-4

Williams, J. R. (2019). The use of online social networking sites to nurture and cultivate bonding social capital: A systematic review of the literature from 1997 to 2018. *New Media & Society, 21*(11–12), 2710–2729. https://doi.org/10.1177/1461444819858749

Zyoud, S. H., Sweileh, W. M., Awang, R., & Al-Jabi, S. W. (2018). Global trends in research related to social media in psychology: Mapping and bibliometric analysis. *International Journal of Mental Health Systems, 12*, 4. https://doi.org/10.1186/s13033-018-0182-6