VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

Finnish Journal of Social Research
Advance access (2024), pp. 1–18
https://doi.org/10.51815/fjsr.144495

Cybercrime target exposure, suitability, personality and victimization: A longitudinal approach

Marko Mikkola, Markus Kaakinen, Nina Savela, Reetta Oksa, Iina Savolainen and Atte Oksanen

Abstract

This study utilizes the routine activity theory as a framework to examine if workplace social media usage, compulsive internet use, online aggression and personality traits are related to an elevated risk of cybervictimization. We leveraged 7-wave longitudinal survey data from the Finnish working population (N = 650) and employed multilevel, mixed-effects logistic regression to analyze fixed effects of in-between variables. Our findings reveal that target exposure, suitability and the personality trait of openness had a positive relationship with cybervictimization. We observed fluctuations in cybervictimization across the observation points, although the temporal pattern did not follow a linear trajectory. The results underscore the importance of longitudinal studies on victimization and advocate additional research on cybervictimization within the working population. This study also emphasizes the need for the integration of established theories to augment our comprehension of the fundamental factors influencing cybervictimization.

Keywords: cybercrime victimization, internet, social media, compulsive internet use, online aggression, personality

Introduction

Over the past few years, rapid and unforeseen societal changes have altered individuals' daily routines, ultimately affecting both protective and risky behaviours that can expose them to crime in the digital realm. These changes have created new opportunities for offenders to engage in illicit activities, whether offline or in online realms (Buil-Gil, 2021; Cohen & Felson, 1979). We have witnessed a rapid acceleration in digitalization in the past decades that has been further intensified by the COVID-19 pandemic since 2020. Together, these events have swiftly transformed societal structures and people's routines related to work locations, the execution of private tasks, maintaining contact with existing friends or forging new online friendships. Such drastic changes in our routines are increasingly exposing us to online criminals (Awan et al., 2021; Ojala & Pyöriä, 2017; Ozimek, 2020; Soto-Acosta, 2020; Teubner & Stockhinger, 2020). The current study scrutinizes this transformation and its impact on cybercrime victimization by

Mikkola (Tampere University), Kaakinen (Tampere University), Savela (LUT University), Oksa (Tampere University), Savolainen (Tampere University) and Oksanen (Tampere University) . Corresponding author's e-mail: marko.mikkola@tuni.fi. © Author(s) 2024. This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). ISSN 2736-9749 (print), 2814-5038 (online)

employing an integrative approach and longitudinal survey data.

Due to digitalization, corporations, governmental entities and enterprises have induced individuals with contemporary technologies to maintain and enhance communication with friends, colleagues and clients (Brynjolfsson et al., 2020; Buil-Gil et al., 2021; Calderon-Monge & Ribeiro-Soriano, 2024; Monteith et al., 2021; Ozimek, 2020). In numerous nations during the COVID-19 pandemic, citizens were mandated to remain indoors during curfew hours to circumvent physical interactions with others, thereby enforcing social isolation (Oksanen et al., 2020a; Subudhi & Palai, 2020). To mitigate the negative impact of such isolation and feelings of loneliness, individuals amplified their utilization of social media tools (Awan et al., 2021; Nimrod, 2020; Subudhi & Palai, 2020). Furthermore, the pandemic led to a situation in which employees were introduced to an array of novel enterprise communication tools to sustain contact with personal acquaintances, colleagues, customers and business associates, either on their personal or employer-provided devices (Buil-Gil et al*.,* 2021; Oksa et al., 2020).

Unfortunately, these changes, some of which were unforeseen due to the sudden virus outbreak and quick actions taken to mitigate it, drew the attention of cybercriminals and other online malefactors (Buil-Gil et al., 2021; Lallie et al., 2021; Nivette et al., 2021; Oksanen et al., 2020b). Cybercriminals, individuals committing criminal acts online, both in the past and present, have leveraged evolving technologies and methods to perpetrate novel forms of cyberattacks, regardless of whether they are targeting technological systems or individuals utilizing internet services (Europol, 2020; Lallie et al*.,* 2021). For instance, cyberattacks may involve the impersonation of public authorities in deceptive emails and text messages disseminated to millions of individuals (Europol, 2020; Lallie et al*.,* 2021). Moreover, cybercriminals target vulnerable systems of critical national infrastructure by gaining unauthorized access using stolen identities and passwords from employees (Buil-Gil et al., 2021; Knapp, 2011; Lallie, 2021; Nurse, 2019).

Cybercrime is a multifaceted phenomenon, as cybercriminals can attack individuals directly or indirectly using different types of tactics to achieve their goals (Hawdon, 2021). Cybercrime encompasses criminal activities facilitated by technology, which can be classified as either cyber-enabled or cyber-dependent (see Choi et al., 2020). Cyber-enabled and cyber-dependent crimes use information and communication technology (ICT) as a tool for committing offences, such as technology-facilitated sexual violence, but unlike cyber-dependent crimes, cyber-enabled can be committed without the use of ICT. In contrast, cyber-dependent crimes, such as hacking, rely entirely on technology and do not exist without it. Cybercrime is a broad term that includes a variety of offences, ranging from cyber-dependent hacking to cyber-enabled fraud, online harassment and sexual abuse (Bossler & Berenblum, 2019). A common factor in various types of cybercrimes is the significance of ICT in victimization, which necessitates identifying risk factors in technology-mediated environments.

Existing academic research and law enforcement agency studies indicate an increase in the number of deceptive emails or malware attacks since the onset of the pandemic (Buil-Gil et al., 2021; Europol, 2020; Gallagher & Brandt, 2020; Lallie et al., 2021; Shi, 2020). Academic research into cybercrime victimization has also seen a substantial increase over the past few decades. Most of the studies on cybercrime victimization focus on specific types of cybercrime, while others combine different types of cybercrime into one category (Ho & Luong, 2022). However, their bibliometric analysis revealed that longitudinal studies on cybercrime victimization are less prevalent than cross-sectional approaches. Additionally, the application of the Big Five personality traits is notably limited in extant academic studies related to cybercrime (van de Weijer & Leukfeldt, 2017), even though one's personality features can influence one's likelihood of becoming exposed to crime. The Big Five framework is a widely recognized model for characterizing an individual's personality traits, consisting of five main traits: extraversion, agreeableness, conscientiousness, openness to experience and neuroticism (Digman, 1990; John, Naumann & Soto, 2008).

Our study sought to address these research gaps by applying routine activity theory (RAT) and examining the personality traits of openness and conscientiousness within the framework of the Big Five personality theory, as previous research has indicated a positive association between openness and victimization, while conscientiousness does not exhibit such a relationship (van de Weijer & Leukfeldt, 2017). We are also applying social media use at work, compulsive internet use, and online aggression to study whether they are related to the increased risk of cybercrime victimization among the Finnish adult population. In our study, we address the phenomenon of cybercrime victimization using a 7-wave longitudinal survey data set among the Finnish working-age population, integrating personality traits with online behaviour. The longitudinal findings enrich the body of research and theories on cybercrime victimization and bear practical implications for the development of victimization prevention programs.

Cybercrime and cybercrime victimization

Cybercrime refers to a crime committed using network-enabled devices such as computers or smartphones and targeting national or international institutions or individuals around the globe (Arshey & Angel Viji, 2021; Burton et al., 2022; Marcum & Higgins, 2019). On an individual level, cybercrime takes many distinctive forms, such as sending computer viruses and phishing attempts via email, leaving threatening messages on social media platforms, online defamation, identity theft and cyber romance scams (Arshey & Angel Viji, 2021; Ho & Luong, 2022; Näsi et al., 2015; Reyns, 2013).

Unlike crime in the physical world, crime occurring in the digital world does not have physical or geographical boundaries. This means that a criminal act can be conducted regardless of the physical location of the criminal or crime target (Buil-Gil et al., 2021). As our daily routines shift from the physical world to the digital world, criminals seem to follow their targets similarly. Thus, according to Miró-Llinares and Moneva (2019), increased use of the internet and its services may be associated with a shift of crime from the physical to the digital world. In addition, fast-paced societal and individual routine changes seem to have created new illicit opportunities for cybercriminals (Buil-Gil et al., 2020; Hawdon et al., 2020; Lallie et al., 2021).

It is difficult to define the actual number of cybercrime victims, but the figures of cybercrime victimization seem to be on the rise (Hawdon, 2021; Ho & Luong, 2022; Näsi et al., 2015). In general, individuals of a younger demographic, particularly males, are at a heightened risk compared to females, with notable exceptions, such as cyberromance scams or instances of sexual harassment, where females are more susceptible to victimization than their male counterparts (Ho & Luong, 2022; Whitty & Buchanan, 2012). Academic research has already noted how traditional crime shifted to cybercrime prior to and during the pandemic (e.g., Meško, 2018; Miró-Llinares & Moneva, 2019; Plachkinova, 2021). Thus, cybercrime is not just a prevalent issue occurring now but also an emerging problem of tomorrow (Buil-Gil et al., 2021; Europol, 2022).

Past studies on cybercrime victimization

There are a significant number of cross-sectional studies on cybercrime victimization using national or cross-national data focusing on adolescents, young adults and adults (e.g., Herrero et al., 2021; Kaakinen et al., 2018; Kokkinos & Antoniadou, 2019; Kranenbarg et al., 2019; Marcum, 2008; Marcum et al., 2010; Moneva et al., 2020; Ngo & Paternoster, 2011; Näsi et al., 2017; Näsi et al., 2021; Ren et al., 2017), while longitudinal cybercrime victimization studies are less common (Marttila et al., 2021; Robers et al., 2013; van de Weijer, 2019; van Wilsem, 2013; Wilcox et al., 2014; Wright & Li, 2012; Zhang et al., 2021).

Existing research indicates that young individuals are more frequently victims of cybercrime, primarily because they tend to be more active online users than other age groups (Kokkinos & Antoniadou, 2019; Näsi et al., 2015; McLaughlin et al., 2012; Oksanen & Keipi, 2013). However, as adults age, they become more susceptible to specific cyber threats, such as computer viruses and defamation (Ngo & Paternoster, 2011). Gender also plays a role in cybercrime victimization, with males being more prone to cybercrime in general, while females are likelier to experience online harassment (Marcum et al., 2010; Moneva et al., 2020; Näsi et al., 2015).

Factors such as high exposure to online criminals, close proximity to them, and the attractiveness of the target significantly contribute to online victimization (Herrero et al., 2021; Marcum et al., 2010; Näsi et al., 2017; Vakhitova et al., 2019; van Wilsem, 2013). It has also been noted that it is riskier to interact with strangers online than with friends and family (Vakhitova, 2016). Furthermore, compulsive internet use is linked to a higher risk of falling victim to online crimes. This is primarily because individuals with compulsive online behaviour are likelier to encounter strangers on the internet, thus exposing themselves to online criminals (Gámez-Guadix et al., 2016; Marttila et al., 2021).

An individual's personality traits have been found to decrease or increase the risk of cybercrime victimization. For instance, individuals with high impulsivity scores have been found to be at greater risk of victimization than others (e.g., Gottfredson & Hirschi, 1990; Tagney et al., 2018). The Big Five is a popular framework for describing individuals' personalities (John & Srivastava, 1999), and it has been used in previous victimization studies (e.g., Liu & Campbell, 2017; van de Weijer & Leukfeldt, 2017; Zhou, Zheng & Gao, 2019).

Existing studies suggest that individuals who are open to online experience, as per the Big Five personality traits, are likelier to become victims of cybercrime. Conversely, those who score high on conscientiousness are less likely to be victimized (van de Weijer & Leukfeldt, 2017). The finding can be seen challenging an earlier study from Wilcox et al. (2014), who argued that neither agreeableness nor conscientiousness have significant direct effects on victimization. A prior cross-sectional study found an association between professional social media use and cyberbullying victimization (Oksanen et al., 2020b). However, to the best of our knowledge, there are no prior studies investigating the association between cybercrime victimization and social media use at work.

Explaining cybercrime victimization

Routine Activity Theory

Academic research into cybercrime victimization has drawn upon a diverse array of established theories from the fields of criminology, psychology and social psychology. These include but are not limited to, RAT (Cohen & Felson, 1979) and the general theory of crime. Even though some of these theories were formulated prior to the advent of the internet, they have demonstrated their efficacy in elucidating cybercrime victimization and the apprehension associated with cybercrime (e.g., Cook et al., 2023; Felson, 2016; Herrero et al., 2021; Kaakinen et al., 2018; Kokkinos & Antoniadou, 2019; Kranenbarg et al., 2019; Moneva et al., 2020; Ren et al., 2017).

RAT is a situational theory, according to which the likelihood of crime in the digital world can be determined by the theory's three key elements: the target's suitability, exposure to offenders and lack of guardianship (Cohen & Felson, 1979; Felson, 2016; Wachs et al., 2021). According to RAT, a situation where crime is likeliest to occur is created by the daily routines of a suitable target. Crime also requires an opportunity, as the motivated offender cannot commit a crime unless an opportunity presents itself to the offender. These opportunities are socially structured and vary across individual's daily routines (Madero-Hernandez & Fisher, 2012). The routines of an individual can be seen as a set of repetitive practices or behavioural patterns in their everyday lives that help individuals navigate and control their social environment (Reckwitz, 2002). One pitfall of these practices is that they can create opportunities for malicious actors to commit their criminal deeds (Cohen & Felson, 1979). Thus, according to RAT, crime does not occur randomly but rather follows the routine patterns and practices of individuals in social life (Cohen & Felson, 1979; Marcum, 2008).

Even though RAT was originally developed before the time of the internet, online criminal activities can be seen to follow the same principles as crimes committed in the physical world, regardless of time and the distance between the offenders and the targets, as they are immaterial in the online environment (Felson, 2016; Leukfeldt & Yar, 2016; Meško, 2018). Thus, RAT has retained its popularity among scientists and is widely used to explain cybercrime victimization (Bossler & Holt, 2009; Choi, 2008; Holt et al., 2020; Marcum et al., 2010; Marttila et al., 2021; Näsi et al., 2017; Reyns, 2013; Vakhitova et al., 2019). Closely associated with RAT (Cohen & Felson, 1979) is the lifestyle-exposure theory of victimization (LET; Hindelang et al., 1978). Both theories emphasize an individual's lifestyle and everyday routines. We recognize that both theories could have been applied to our research, but because our approach focuses on overall changes in routines at the societal level and because we also apply variables other than exposure to risky routines, we used RAT because it is more general and applicable to our approach to cybercrime victimization.

Big Five framework

According to psychological and social psychological theories, an element of the risk of victimization is attributed to the human connections we establish and foster, both in the digital realm and in the physical world (Kendrick et al., 2012; Turanovic et al., 2014; Turanovic et al., 2016). The desire for interpersonal attachment and the cultivation of friendships, as posited by Baumeister and Leary (1995), are integral components of human sociality and motivation. Thus, to avoid loneliness, we tend to keep the company we have or to seek new, meaningful relationships. Being in contact with known friends might act as a form of shield against the threats of the online world, whereas being in contact with unknown people constitutes a higher risk of cybervictimization (Cohen & Felson, 1979; Wachs et al., 2021).

The personality dimensions of the Big Five, derived from natural-language descriptions people use to describe themselves and others, provide a general taxonomy of personality traits. The framework integrates various systems of personality description without implying that personality can be reduced to just five traits. Each of these dimensions encapsulates numerous specific personality characteristics (John & Srivastava, 1999). These dimensions are agreeableness (trust, straightforwardness, altruism, compliance, modesty and tendermindedness), conscientiousness (competence, order, dutifulness, achievement-striving, self-discipline and deliberation), extraversion (gregariousness, assertiveness, activity, excitement-seeking, positive emotions and warmth), neuroticism (anxiety, anger, hostility, depression and self-consciousness), and openness (ideas, fantasy, aesthetics, actions, feelings and values; John & Srivastava, 1999).

In recent decades, because of the development of digital technology and online services, people have turned their attention to maintaining existing relationships and forging new ones online to ease the burden of loneliness or alleviate feelings of isolation. Of the Big Five personality traits, openness has been found to be a strong predictor of social media activities, especially interactions with others. In contrast, the trait of conscientiousness has shown less correlation with social media activities, potentially reducing the risk of victimization (Liu & Campbell, 2017; van de Weijer & Leukfeldt, 2017). Staying connected with family, relatives and known close friends might reduce the risk of online victimization. Conversely, seeking new online friends among previously unknown people or living a long way from one's friends could potentially increase the risk of victimization (Kendrick et al., 2012; Turanovic et al., 2014; Turanovic et al., 2016). One of the study's aims was to examine the correlation between social media usage and cybervictimisation. Consequently, we opted to integrate only conscientiousness and openness from the Big Five personality framework into our study because, in a previous study, openness was found to be positively associated with cybercrime victimization, while conscientiousness was found not to have a similar association (van de Weijer & Leukfeldt, 2017).

This study

This study uses longitudinal national data gathered prior to and during the pandemic era when the Finnish workforce went through a rapid change in how individuals carry out their daily lives. We examine how online crime targets' exposure to motivated offenders and targets' suitability for online offenders affect individuals' cybercrime victimization risk. Existing studies have found openness to be related to having a large network of friends, but these friendships lack closeness. Conscientious individuals have fewer friends, but the friendship quality is better, and they have less conflict with their friends (Harris & Vazirem, 2016). In accordance with RAT, close friends can decrease, and unknown new friends can increase the risk of online crime victimization (Cohen & Felson, 1979; Wachs et al., 2021).

Some previous studies using cross-sectional and longitudinal data have shown that a target's exposure and suitability can increase the risk of online victimization (Herrero et al., 2021; Marcum, 2008; Marcum et al., 2010; Näsi et al., 2017; Vakhitova et al., 2019), while others have shown that exposure to offenders does not increase the odds of cybervictimization (Wick et al., 2017). Therefore, we will assess whether exposure and suitability are positively related to victimization.

Hypothesis 1 (H1): *Social media use at work, compulsive internet use and aggressive internet communication are related to an increased risk of cybercrime victimization.*

The personality trait of openness from the Big Five framework has been found to be a strong predictor of social media activities; thus, it has been found to increase the risk of cybercrime victimization (Liu & Campbell, 2017). Conversely, conscientiousness from the same framework has been found to correlate less with social media activities and, therefore, lower the risk of victimization (Liu & Campbell, 2017).

Hypothesis 2 (H2a and H2b): *Personality factors are associated with cybercrime victimization. We expect that conscientious individuals have a lower risk of victimization (H2a), and individuals with a higher openness score (H2b) are likelier victims.*

Age and gender have been found to be related to the risk of cybercrime victimization, depending on the type of cybercrime. We expect, based on existing studies, that younger people, especially males, are likelier to be victimized online than older people and females (e.g. Meško, 2018; Ngo & Paternoster, 2011).

Hypothesis 3 (H3): *Younger people are more prone to be victimized online than older people.*

Hypothesis 4 (H4): *Men are more prone to be victimized online than women.*

Method

Participants and procedure

The study participants took part in the longitudinal Social Media at Work in Finland Survey, which targeted the Finnish working population living in mainland Finland. The baseline survey was collected in March–April 2019 in collaboration with Norstat Finland. Respondents were drawn from Norstat's participant panel, which is the largest in Finland. The response rate was 28.31% (Latikka et al., 2022; Oksa et al., 2021). Follow-up surveys of the same respondents were collected in September–October 2019 (second time point, T2: *N* = 1,318). T2 is the starting point of this study, as a cybercrime victimization measure was added to the second wave of the study. Data collection continued in March–April 2020 (T3: *N* = 1,081), September–October 2020 (T4: *N* = 1,152), March–April 2021 (T5: *N* = 1,018), September–October 2021

(T6: *N* = 982), March–April 2022 (T7: *N* = 932) and September–October 2022 (T8: *N* = 921). In T4, all the original respondents from T1 were invited to participate again. Our analysis focused on those participants who responded to all follow-up surveys (T2–T8) without any additional exclusion criteria. The data from T2 to T8 thus included 4,550 observations from 650 participants.

The study participants were 42.46% female and aged between 18 and 64 years (M = 44.70, SD = 10.82). Out of the participants, 18.46% worked in the service sector; 16.31% in health and welfare; 14.31% in business, communication and technology; 14.00% in raw materials and manufacturing; 10.92% in retail and transportation; 10.15% in education; 6.92% in public administration; 5.38% in construction and 3.54% in other sectors. Geographically, participants came from all the regions of mainland Finland: 36.46% from the Helsinki–Uusimaa area, 21.23% from Southern Finland, 23.08% from Western Finland and 19.23% from Eastern and Northern Finland. Based on the representativeness analysis (e.g. Latikka et al., 2022), the sample characteristics generally matched the working population in Finland, and no major biases were found during the longitudinal study. Dropout analysis showed that participants who responded to all survey waves were more often highly educated, male and older compared to the official statistics of Finland's average working population (Latikka et al., 2022). We used analytical weights to fix the sample biases. The data and code used will be available upon a reasonable request from the authors of this research paper.

Measures

The dependent variable, cybercrime victimization, was measured using the question, "Has someone committed a crime against you online during the past six months?" with a yes or no response at data collection points T2–T8. If the participants answered yes, they were then asked to choose the type of online crime committed from a list. Options on the list were as follows: (1) slander or defamation of your character, (2) coercion or a threat of violence, (3) identity theft, (4) fraud, (5) sexual harassment and (6) other. Seven independent variables from our data were selected. Participants were given the option to select multiple choices. All independent variables showed acceptable inter-item reliability (McDonald's omega).

Exposure to a motivated offender. According to previous studies, an increased risk of online victimization is associated with the time individuals spend on the internet or the provision of private information on social media (Marcum, 2008; Marcum et al., 2010; Ngo & Paternoster, 2011; Näsi et al., 2021). We measured targets' exposure to a motivated offender by looking at respondents' reported use of work-related social media platforms and tools with the question, "How often do you use social media to keep in touch with your colleagues or work community?" The answer options for work-related social media use were: (0) I don't use it, (1) less than weekly, (2) weekly, (3) daily and (4) many times a day. The omega reliability coefficients showed good internal consistency for social media use at work (0.79–0.89 for T2–T8).

Target suitability. The chosen personality traits of openness and conscientiousness were measured with items included in the 15-item Big Five Inventory (Hahn et al., 2012). Personality was only measured at the third time point (T3), as personality is regarded as quite stable for working-age adults over shorter periods of time (Cobb-Clark & Schurer, 2012). Moreover, personality trait profiles have been found to be quite stable across mid-adulthood (Kinnunen et al., 2012). For both traits, we created a 3-item sum variable ranging from 3 to 21. Higher scores in conscientiousness and openness indicate higher levels of that personality trait. The omega reliability coefficients showed acceptable internal consistency for conscientiousness (0.69) and openness (0.72).

Compulsive internet use was measured using the Compulsive Internet Use Scale (CIUS; Meerkerk et al., 2009). The CIUS does not consider the internet itself to be addictive to its users, but rather the services the internet offers, such as social media or other types of online activities. The higher the CIUS score, the higher the risk of online victimization (Dihr et al., 2015; Griffiths, 2000). In existing studies, a high CIUS score has been associated with a higher risk of cybercrime victimization and risks associated with online gambling (Kokkinos & Antoniadou, 2019; Oksanen et al., 2019). In our study, compulsive internet use was measured using an instrument that consists of 14 measurable items ranging from 0 (*Never*) to 4 (*Very*

Table 1 Descriptive Statistics of the Study Variables

		T2		T3		T4		T5		T6		T7		T8		Within-person
Continuous variables	Range	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*M*	*SD*	*SD*
Social media use at work	0–80	4.53	5.30	5.49	6.46	5.19	5.34	5.27	5.91	5.21	5.40	5.13	5.49	5.53	6.92	3.37
Compulsive internet use	3–21	6.87	4.20	6.75	4.08	6.83	4.14	6.81	4.23	6.71	4.11	6.70	4.19	6.75	4.34	2.05
Conscientiousness	3–21			15.70	3.04											
Openness	3–21			14.68	3.40											
Age[1]	18–64	44.94	10.75													
Categorical variables	Coding	*n*	%	*n*	%	*n*	%	*n*	%	*n*	%	*n*	%	*n*	%	
Cybercrime victimization	0/1	60	9.23	61	9.38	56	8.62	63	9.69	71	10.92	63	9.69	63	9.69	
Aggressive internet communication	0/1	26	4.00	29	4.46	25	3.85	18	2.77	24	3.69	18	2.77	18	2.77	
Female[1]	0/1	275	42.31													
n		650		650		650		650		650		650		650		4,550

Note. Categorical variables are presented as frequencies (*n*) and relational proportions (*%*). Continuous variables are presented as means (*M*) and standard deviations (*SD*). [1]Age and gender information measured in the original survey timepoint before follow-up surveys (T2–T8) *often*). A higher CIUS score indicates a high level of compulsive internet use. The omega reliability coefficients showed good internal consistency for compulsive internet use (.86–.88 for T2–T8).

Offensive or threatening messaging against others online was assessed with the question, "How often during the past six months have you sent messages on social media that offend or threaten other users?" The answer options for the use of threatening messages were (0) never, (1) every now and then, (2) monthly, (3) weekly and (4) daily. A dichotomous variable (0 = never, 1 = sometimes) was created based on the answers.

Age and gender. Age was measured by asking about the participant's ages. Only respondents aged between 18 and 65 years were accepted into the study. Age was treated as a continuous variable. The gender variable was measured by asking the participant's gender, with the options (1) male, (2) female and (3) other. None of the respondents chose option (3) other.

Statistical techniques

Descriptive statistics and correlations of the study variables are detailed in Tables 1 and 2. We performed the statistical analyses in two different stages using Stata/IC 16.1 software. First, we used multilevel mixed-effects logistic regression to analyze associations between RAT-related variables and cybercrime victimization (Table 3). In the mixed-effects logistic regression models, variables at Level One (Within-Subjects Level) and Level Two (Between-Subjects Level) were included. Level One variables consisted of time-varying risk factors, such as social media use at work, compulsive internet use and aggressive internet communication. Level Two variables included more static individual characteristics such as age, gender, personality traits, openness and conscientiousness. Then, we analyzed the fixed effects of within-level variables (social media use at work, compulsive internet use and sending offending messages). These results are presented in Table 4. Fixed-effects regression controls for static between-individual differences allowed the analysis to focus on within-individual temporal variability in the studied risk factors and cybercrime outcomes.

For our models, we report odds ratios (OR), statistical significance (p) and robust standard errors adjusted for the clustering of observations within individuals. Our models included random intercepts and random slopes for time, with an independent covariance structure. For the random parts of our models, we reported standard deviations and 95% confidence intervals. Additional robustness checks were conducted with multilevel, fixed-effect logistic regression, including all time-varying predictors to adjust for potential between-person selectivity.

Table 2 Zero-order correlation matrix

Variables	1.	2.	3.	4.	5.	6.	7.	8.
1. Cybercrime victimization								
2. Social media use at work	0.13**							
3. Compulsive internet use	0.20**	0.26**						
4. Aggressive internet communication	0.21**	0.14**	0.21**					
5. Openness	0.05	0.08*	0.01	-0.02				
6. Conscientiousness	-0.02	-0.06	-0.18**	-0.06	0.19**			
7. Age	-0.10*	-0.10**	-0.31**	-0.11**	0.12**	0.15**		
8. Gender	-0.02	-0.08*	-0.10*	-0.08*	-0.05	0.10*	0.39	

*p < 0.05 ** p < 0.01

Results

The observed cybercrime victimization varied between 8.62% (T3: March–April 2020) and 10.92% (T5: March–April 2021). The variation in cybercrime victimization was not linear over time. At T2 (the starting point of this study), 9.23% of participants reported victimization, at T3 9.38%, at T4 8.62%, at T5 9.69%, at T6 10.92%, at T7 9.69%, and at T8 9.69%. The changes in victimizations between the time points were relatively small, and no linear trend was detected.

In line with our first hypothesis, we found that individuals who use social media more often than others at work were at higher risk of cybercrime victimization (OR = 1.34, *p* < 0.001). Also, individuals scoring high points for compulsive internet use (OR = 1.40, *p* = 0.002) were more often at risk of victimization than others. Sending aggressive messages over the internet had a significant impact on an increased risk of cybervictimization (OR = 9.64, *p* < 0.001).

In the second hypothesis (H2a), we assumed conscientious individuals to have a lower risk of victimization and individuals scoring higher points for openness (H2b) to have a higher risk of victimization. According to the results, participants who had a higher score for openness (OR = 1.62, *p* = 0.012) were likelier to be victimized. We found no statistically significant difference in conscientiousness (OR = 0.90, *p* = 0.494).

In line with the third hypothesis (H3), younger individuals were at a higher risk of cybercrime victimization than older individuals, as the risk decreased with age (OR = 0.97, *p* = .049). However, contrary to H4, gender was not related to victimization (OR = 1.16, *p* = 0.665).

Additional robustness checks were conducted with compulsive internet use, social media use at work and aggressive internet communication. According to the results of the fixed effects analysis, compulsive internet use was no longer significant (OR = 1.02, *p* = 0.879), whereas both social media use at work (OR = 1.26, *p* = 0.023) and aggressive internet communication (OR = 3.94, *p* < 0.001) remained significant.

Table 3 Multilevel mixed-effects logistic regression model predicting cybercrime victimization: RAT variables

	OR	*Robust SE*	95% CI	*p*
Social media use at work	1.34	0.08	[0.13, 0.46]	< 0.001
Compulsive internet use	1.40	0.11	[0.13, 0.54]	0.002
Aggressive internet communication	9.64	0.45	[1.38, 3.15]	< 0.001
Openness	1.62	0.19	[0.11, 0.86]	0.012
Conscientiousness	0.90	0.15	[-0.41, 0.20]	0.494
Age	0.97	0.02	[-0.07, 0.00]	0.049
Gender	1.16	0.33	[-0.51, 0.80]	0.665

Note. 650 observations

Table 4 Fixed effects regression model predicting cybercrime victimization: RAT and background variables

	OR	*SE*	95% CI	*p*
Social media use at work	1.26	0.13	[1.03, 1.54]	0.023
Compulsive internet use	1.02	0.13	[0.80, 1.30]	0.879
Aggressive internet communication	3.94	1.37	[1.99, 7.79]	< 0.001

Note. 650 observations

Discussion

This study utilized RAT to examine how social media use at work, compulsive internet use, online aggression and personality traits are related to an increased risk of cybercrime victimization. In our longitudinal study of the Finnish adult workforce, the focus was on how online crime targets' exposure to, and suitability for, online offenders' effects on individuals' victimization risk while the workforce was going through major changes in the concepts of work.

The findings of the study support our first hypothesis that exposure to online offenders is related to cybercrime victimization. The more individuals use social media services and the more aggressively they behave, the higher the risk of victimization. According to the results, compulsive internet use was not associated with an increased risk of victimization after accounting for interpersonal differences. It could be that mere extensive time spent on the internet does not increase the victimization risk, but the quality of activities remains the key factor.

Regarding Hypothesis 2, the results of our analyses revealed openness to be related to victimization (H2b), but no statistically significant difference was found for conscientiousness (H2b). Open individuals are likelier to be victimized online, similar to prior research (van de Weijer & Leukfeldt, 2017). Our results for conscientiousness are in line with other research, suggesting no direct connection (Wilcox et al., 2014). Even though openness is related to cybercrime victimization, we do not believe it to be deterministic, as there are other factors, such as situational factors, which play a role in determining whether one is victimized online.

Our third hypothesis, the result regarding age, is somewhat expected, as juveniles, adolescents, and young adults have been found to be at higher risk of victimization (Kokkinos & Antoniadou, 2019; Oksanen & Keipi, 2013). In our fourth hypothesis, we expected men to be more prone to being victimized online. Men and women face different types of threats online, but in our study, we looked at multiple types of threats with respect to victimization, which could be a reason why we did not find differences between genders.

Along with the rest of the world, Finnish society went through a rapid change during the COVID-19 pandemic in how we work from our homes and use a mix of general social media tools with enterprise social media platforms for work-related tasks and to stay in touch with our friends or seek new meaningful relationships with previously unknown people online (e.g., Buil-Gil et al., 2021; Oksa et al., 2020). Evidently, working from home has both positive and negative impacts on employees and employers, such as fewer interruptions while working at home, reduced social contacts, blurring boundaries between work and one's own private life and more work-related stress (Ayyagari et al., 2011; Hahne, 2021; Oksa et al., 2020). However, according to RAT, crime follows the routine patterns and practices of individuals in social life (Cohen & Felson, 1979). Thus, during major societal changes when routines change, criminals are likeliest to change their ways of searching for suitable targets and choosing when and how to launch their attack. According to the results of our study, it is plausible to assume that online perpetrators have changed their methods of conducting criminal activities, as the number of victims is on the rise.

This study provides new information on cybervictimization, which continues to be a critical issue as the prevalence and sophistication of cybercrimes increase. The practical implications that corporations, organizations and governments should rethink are their approaches to any future situation where the workforce must undergo rapid changes in how they work and where they work from because malicious actors on the internet will follow the change to their advantage. In addition, the protection of the workforce from cyberattacks cannot be entrusted only to technology, as it cannot stop or filter all possible cyberattacks.

We have adapted RAT, along with the traits of conscientiousness and openness from the Big Five personality traits, to our study to explain cybervictimization. Even though RAT is a situational theory, it is beneficial to combine situational theory with theories on personality traits because personality can increase or decrease individuals' risk of being victimized online. Like all other studies, this study also had limitations. First, as our study utilized observational data, no causal inferences could be made based on our findings. Issues related to potential between-person selectivity were addressed with additional fixed-effects analyses. The data of the study were also collected in Finland and targeted only working-age individuals. Thus, there might be some limitations in generalizing our findings to other national contexts. The response rate (28.31%) and sample size of participants who answered all our study questions (N = 650) might also raise questions on external validity and statistical power. However, the data sample generally matches the working population in Finland, and no major biases were found. Finally, the study was based on self-reported measures of cybercrime victimization. However, the measures used for this study comprehensively examined the topic. Although our study did not focus on the impact of the COVID-19 pandemic, we considered the pandemic in the interpretation of our results. Additionally, we did not examine different types of cybercrime separately, which warrant distinct hypotheses due to their unique characteristics. Future research should incorporate more specific hypotheses to address different types of cybercrime individually.

Conclusions

Situational criminological theories like RAT are useful when explaining cybercrime victimization. However, even if the situation is right, crime does not necessarily happen. This could be because of a potential target's personality or another crime-preventing factor. This study demonstrates how personality is associated with the risk of victimization. It also demonstrates the need to expand and continue testing established criminological theories during and after times of rapid societal change, as cybercrime and cybercrime victimization are evolving, complicated phenomena of the internet and networked societies. Clearly, online victimization cannot be totally prevented by using cybersecurity tools that remove or filter malicious content from email, instant messaging, social media applications or internet browsing, as criminals and other malefactors of the internet can always bypass some of the defensive tools (Ho & Luong, 2022). Therefore, individuals' personalities play a vital role as one of the factors associated with the risk of cybervictimization.

We found that open individuals do not avoid situations in which they are exposed to criminals. Although we found that the personality trait of openness is positively related to cybercrime victimization and conscientiousness is not, we cannot say that the traits are deterministic, as other factors, not only situational, can have a role in determining the individual's actual risk of cybervictimization. This is vital to realize when creating new cybercrime prevention education and awareness programs. We argue that experimental studies and more longitudinal research on openness and conscientiousness are required to understand how and in which situations these personality traits are associated with the odds of cybercrime victimization. Compulsive internet use should also be studied further, as it does not alone explain victimization when considering between-person differences.

References

Arshey, M., & Angel Viji, K. S. (2021). Thwarting cyber crime and phishing attacks with machine learning: A study. *7th International Conference on Advanced Computing and Communication Systems* (ICACCS), 353–357. https://doi.org/10.1109/ICACCS51430.2021.9441925

Awan, H. A., Aamir, A., Diwan, M. N., Ullah, I., Pereira-Sanchez, V., Ramalho, R., Orsolini, L., de Filippis, R., Ojeahere, M.I., Ransing, R., Vadsaria, A.K., & Virani, S. (2021). Internet and pornography use during the COVID-19 pandemic: Presumed impact and what can be done. *Frontiers in Psychiatry, 12*:623508. https://doi.org/10.3389/fpsyt.2021.623508

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological antecedents and implications. *MIS Quarterly, 35*(4), 831–858. https://doi.org/10.2307/41409963

Baumeister, R. F., & Leary, M. R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin, 117*(3), 497–529.

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice, 42*(5), 495–499.

Bossler, A., & Holt, T. (2009). Online activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420. Available at: https://www.cybercrimejournal.com/pdf/bosslerholtijcc2009.pdf (accessed 7 January 2023).

Brynjolfsson, E., Horton, J. J., Ozimek, A., Rock, D., Sharma, G., & TuYe, H.-Y. (2020). COVID-19 and remote work: An early look at US data. *National Bureau of Economic Research*. https://doi.org/10.3386/w27344

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. E*uropean Societies, 23*, 47–59, https://doi.org/10.1080/14616696.2020.1804973

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimization: A realist review. *Experimental Gerontology, 159*. https://doi.org/10.1016/j.exger.2021.111678

Calderon-Monge, E., & Ribeiro-Soriano, D. (2024). The role of digitalization in business and management: A systematic literature review. *Review of Managerial Science, 18*, 449–491. https://doi.org/10.1007/s11846-023-00647-8

Choi, K.S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308–33. Available at: https://www.cybercrimejournal.com/pdf/tinaijccjan2008.pdf (accessed 10 December 2022).

Choi, K.-S., Lee, C. S., & Louderback, E. R. (2020). Historical evolutions of cybercrime: From computer crime to cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 27–44). Springer Nature Switzerland.

Cobb-Clark, D. A., & Schurer, S. (2012). The stability of big-five personality traits. *Economics Letters, 115*(1), 11–15. https://doi.org/10.1016/J.ECONLET.2011.11.015

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

Cook, S., Giommoni, L., Pareja, N. T., Levi, M., & Williams, M. L. (2023). Fear of economic cybercrime across Europe: A multilevel application of routine activity theory. *The British Journal of Criminology, 63*(2), 384–406. https://doi.org/10.1093/bjc/azac021

Digman, J. M. (1990). Personality structure: Emergence of the five-factor model. *Annual Review of Psychology, 41*(1), 417–440. https://doi.org/10.1146/annurev.ps.41.020190.002221

Dihr, A., Chen, S., & Nieminen, M. (2015). A repeat cross-sectional analysis of the psychometric properties of the Compulsive Internet Use Scale (CIUS) with adolescents from public and private schools. *Computers & Education, 86*, 172–181. https://doi.org/10.1016/j.compedu.2015.03.011

Europol. (2020). Pandemic profiteering: How criminals exploit COVID-19 crisis, available at: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (accessed 23 October 2022).

Europol. (2022). Cybercrime. Available at: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (accessed 29 October 2022).

Felson, M. (2016). Routine activity approach. In R. Wortley & M. Townsley (Eds.), *Environmental criminology and crime analysis.* 87–97. Routledge.

Gallagher, S., & Brandt, A. (2020). Facing down the myriad threats tied to COVID-19. https://news.sophos.com/en-us/2020/04/14/covidmalware (accessed 23 October 2022).

Gámez-Guadix, M., Borrajo, E., & Almendros, C. (2016). Risky online behaviours among adolescents: Longitudinal relations among problematic internet use, cyberbullying perpetration, and meeting strangers online. *Journal of Behavioural Addictions, 5*(1), 100–107. https://doi.org/10.1556/2006.5.2016.013

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Griffiths, M. (2000). Excessive Internet use: Implications for sexual behavior. *Cyberpsychology & Behavior, 3*(4). https://doi.org/10.1089/109493100420151

Hahn, E., Gottschling, J., & Spinath, F. M. (2012). Short measurements of personality–validity and reliability of the GSOEP Big Five inventory (BFI-S). *Journal of Research in Personality, 46*(3), 355–359. https://doi.org/10.1016/j.jrp.2012.03.008

Hahne, A. S. (2021). The impact of teleworking and digital work on workers and society – Case study on Finland (Annex III). Publication for the Committee on Employment and Social Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662904/IPOL_STU(2021)662904(ANN01)_EN.pdf (accessed 19 February 2023).

Harris, K., & Vazirem, S. (2016). On friendship development and the Big Five personality traits. Social and Personality Psychology Compass, 10(11), 647–667.https://doi.org/10.1111/spc3.12287

Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice, 46*, 837–842. https://doi.org/10.1007/s12103-021-09652-7

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice, 45*, 546–562. https://doi.org/10.1007/s12103-020-09534-4

Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F.J., & Urueña, A. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International Journal of Environmental Research and Public Health, 18*(7). https://doi.org/10.3390/ijerph18073763

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

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

Holt, T. J., Leukfeldt, R., & van de Weijer, S. (2020). An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites. *Criminal Justice and Behavior*. https://doi.org/10.1177/0093854819900322

John, O.P., Naumann, L.P., & Soto, C. J. (2008). Paradigm shift to the integrative big five trait taxonomy: history, measurement and conceptual issues. In O. P. John, R. W. Robins & L.A. Pervin (Eds.), *Handbook of personality: Theory and research* (pp. 114–158). New York, NY: Guilford Press.

John, O. P., & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement and theoretical perspectives. *Handbook of Personality: Theory and Research, 2*, 102–138, available at: https://darkwing.uoregon.edu/~sanjay/pubs/bigfive.pdf (accessed 19 November 2022).

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behavior and Social Networking, 21*(2), 129–137. https://doi.org/10.1089/cyber.2016.0728

Kendrick, K., Jutengren, G., & Stattin, H. (2012). The protective role of supportive friends against bullying perpetration and victimization. *Journal of Adolescence, 35*(4), 1069–80. https://doi.org/10.1016/j.adolescence.2012.02.014

Kinnunen, M. L., Metsäpelto, R. L., Feldt, T., Kokko, K., Tolvanen, A., Kinnunen, U., Leppänen, E., & Pulkkinen, L. (2012). Personality profiles and health: Longitudinal evidence among Finnish adults. *Scandinavian Journal of Psychology, 53*(6), 512–522. https://doi.org/10.1111/j.1467-9450.2012.00969.x.

Knapp, E. (2011). Chapter 2 – About industrial networks. In E. Knapp(Ed.), *Industrial network security, 7–29.* Syngress, https://doi.org/10.1016/B978-1-59749-645-2.00002-1

Kranenbarg, M. W., Holt, T. J., & van Gelder, J-L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization–offending overlap. *Deviant Behavior, 40*(1), 40–55. https://doi.org/10.1080/01639625.2017.1411030

Kokkinos, C. M., & Antoniadou, N. (2019). Cyber-bullying and cyber-victimization among undergraduate student teachers through the lens of the General Aggression Model. *Computers in Human Behavior, 98*, 59–68. https://doi.org/10.1016/j.chb.2019.04.007

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cybercrime and cyberattacks during the pandemic. *Computers & Security, 105*. https://doi.org/10.1016/j.cose.2021.102248

Latikka, R., Koivula, A., Oksa, R., Savela, N., & Oksanen, A. (2022). Loneliness and psychological distress before and during the COVID-19 pandemic: Relationships with social media identity bubbles. Social Science and Medicine, 114674. https://doi.org/10.1016/j.socscimed.2021.114674

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

Liu, D., & Campbell, W. K. (2017). The Big Five personality traits, Big Two metatraits and social media: A meta-analysis. *Journal of Research in Personality, 70,* 229–240. https://doi.org/10.1016/j.jrp.2017.08.004

McLaughlin. H., Uggen, C., & Blackstone, A. (2012). Sexual harassment, workplace authority, and the paradox of power. *American Sociological Review, 77*(4), 625–647. https://doi.org/10.1177/0003122412451728

Madero-Hernandez, A., & Fisher, B. S. (2012). Routine activity theory. In F. T. Cullen, and P. Wilcox (Eds.), T*he Oxford handbook of criminological theory*. Oxford Handbooks. Online edition, Oxford Academic. https://doi.org/10.1093/oxfordhb/9780199747238.013.0027

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization. I*nternational Journal of Cyber Criminology, 2*(2), 346–367, available at: https://www.cybercrimejournal.com/pdf/catherineijccdec2008.pdf (accessed 3 December 2022).

Marcum, C. D., & Higgins, G. E. (2019). Cybercrime. In M. Krohn, N. Hendrix, G. Penly Hall, & A. Lizotte, (Eds.), *Handbook on crime and deviance.* Handbooks of Sociology and Social Research. Springer, Cham. https://doi.org/10.1007/978-3-030-20779-3_23

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviours utilizing routine activity theory. *Deviant Behavior, 31*, 381–410. https://doi.org/10.1080/01639620903004903

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime victimization and problematic social media use: Findings from a nationally representative panel study. *American Journal of Criminal Justice, 46,* 862–881. https://doi.org/10.1007/s12103-021-09665-2

Meerkerk, G.-J., Van Den Eijnden, R. J. J. M., Vermulst, A. A., & Garretsen, H. F. L. (2009). The compulsive Internet use scale (CIUS): Some psychometric properties. *CyberPsychology & Behavior, 12(*1). https://doi.org/10.1089/cpb.2008.0181

Meško, G. (2018). On some aspects of cybercrime and cybervictimization. *European Journal of Crime, Criminal Law, and Criminal Justice, 26*(3). https://doi.org/10.1163/15718174-02603006

Miró-Llinares F. & Moneva A. (2019). What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks “Did cybercrime cause the crime drop?” *Crime Science, 8*(1), Article 12. https://doi.org/10.1186/s40163-019-0107-y

Moneva, A., Miró-Llinares, F., & Hart, T. C. (2020). Hunter or prey? Exploring the situational profiles that define repeated online harassment victims and offenders. *Deviant Behavior.* https://doi.org/10.1080/01639625.2020.1746135

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glen, T. (2021). Increasing cybercrime since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports, 23*(18). https://doi.org/10.1007/s11920-021-01228-w

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793. Available at: https://www.cybercrimejournal.com/pdf/ngo2011ijcc.pdf (accessed 14 January 2023).

Nimrod, G. (2020). Changes in Internet use when coping with stress: Older adults during the COVID-19 pandemic. *The American Journal of Geriatric Psychiatry, 28*(10), 1020–024. https://doi.org/10.1016/j.jagp.2020.07.010

Nivette, A. E., Zahnow, R., Aguilar, R., Ahven, A., Amram, S., Ariel, B., Arosemena Burbano, M. J., Astolfi, R., Baier, D., Bark, H., Beijers, J. E. H., Bergman, M., Breetzke, G., Concha-Eastman, I. A., Curtis-Ham, S., Davenport, R., Díaz, C., Fleitas, D., Gerell, M., Jang, K-H., Kääriäinen, J., Lappi-Seppälä, T., Lim, W-S., Loureiro, R., Mazerolle, L., Meško, G., Noemí, P., Peren, M. F. T., Poblete-Gazenave, R., Rose, S., Svensson, R., Trajtenberg, N., van der Lippe, T., Veldkamp, J., Predemo, V. C. J., & Eisner, M. P. (2021). A global analysis of the impact of COVID-19 stay-at-home restrictions on crime. *Nature Human Behaviour, 5*, 868–877. https://doi.org/10.1038/s41562-021-01139-z

Nurse, J. R. C. (2019). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. The Oxford Handbook of Cyberpsychology, 663–690. https://doi.org/10.1093/oxfordhb/9780198812746.013.35

Näsi, M., Danielsson, P., & Kaakinen, M. (2021). Cybercrime victimisation and polyvictimisation in Finland—Prevalence and risk factors. *European Journal on Criminal Policy and Research.* Online First. https://doi.org/10.1007/s10610-021-09497-0

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

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults' online harassment: A multi-nation study. *Criminology & Criminal Justice,* 1–15. https://doi.org/10.1177/1748895816679866

Ojala, S., & Pyöriä, P. (2017). Mobile knowledge workers and traditional mobile workers: Assessing the prevalence of multi-locational work in Europe. *Acta Sociologica, 61*(4), 402–418. https://doi.org/10.1177/0001699317722593

Oksa, R., Kaakinen, M., Savela, N., Ellonen, N., & Oksanen, A. (2020). Professional social media usage: Work engagement perspective. *New Media & Society, 1461444820921938*. https://doi.org/10.1177/1461444820921938

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the Internet: A Population-based study in Finland. *Vulnerable Children & Youth Studies, 8*(4), 298–309. https://doi.org/10.1080/17450128.2012.752119

Oksanen, A., Kaakinen, M., Latikka, R., Savolainen, I., Savela, N., & Koivula, A. (2020a). Regulation and trust: 3-month follow-up study on COVID-19 mortality in 25 European countries. *JMIR Public Health and Surveillance, 6*(2), Article e19218. https://doi.org/10.2196/19218

Oksanen, A., Oksa, R., Savela, N., Kaakinen, M., & Ellonen, N. (2020b). Cyberbullying victimization at work: Social media identity bubble approach. *Computers in Human Behavior, 109*(106363). https://doi.org/10.1016/j.chb.2020.106363

Oksanen, A., Sirola, A., Savolainen, I., & Kaakinen, M. (2019). Gambling patterns and associated risk and protective factors among Finnish young people. *Nordic Studies on Alcohol and Drugs, 36*(2), 161–176. https://doi.org/10.1177/1455072518779657

Ozimek, A. (2020). The future of remote work. *Social Science Research Network*. http://dx.doi.org/10.2139/ssrn.3638597

Plachkinova, M. (2021). Exploring the shift from physical to cybercrime at the onset of the COVID-19 pandemic. *International Journal of Cyber Forensics and Advanced Threat Investigations, 2*(1), 50–62. https://doi.org/10.46386/ijcfati.v2i1.29

Reckwitz, A. (2002). Toward a theory of social practices: A development in culturalist theorizing. *European Journal of Social Theory, 5*(2), 243–265. https://doi.org/10.1177/13684310222225432

Ren, L., He, N., Zhao, R., & Zhang, H. (2017). Self-control, risky lifestyles and victimization. A study with a sample of Chinese school youth. *Criminal justice and behaviour, 44*(5), 695–716. https://doi.org/10.1177/0093854816674758

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offences. *Journal of Research in Crime and Delinquency, 50*(2), 216–238. https://doi.org/10.1177/0022427811425539

Robers, S., Kemp, J., & Truman, J. (2013). Indicators of school crime and safety: 2012 (NCES 2013-036/ NCJ 241446). Washington, DC: National Center for Education Statistics, U.S. Department of Education, and Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, available at: https://eric.ed.gov/?id=ED543705 (accessed 27 November 2022).

Shi, F. (2020). Threat spotlight: Coronavirus-related phishing. Available at: https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing (accessed on 23 October 2022).

Soto-Acosta, P. (2020). COVID-19 Pandemic: Shifting digital transformation to a high-speed gear. *Information Systems Management, 37*(4), 260-266. https://doi.org/10.1080/10580530.2020.1814461

Subudhi, R. N., & Palai, D. (2020). Impact of Internet use during COVID lockdown. *Journal of Humanities and Social Sciences Research, 2*, 59–66. https://doi.org/10.37534/bp.jhssr.2020.v2.nS.id1072.p59

Tagney, J. P., Boone, A. L., & Baumeister, R. F. (2018). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. In R. F. Baumeister (Ed.), S*elf-regulation and self-control: Selected works of Roy F. Baumeister* (pp.173–212). Routledge.

Teubner, R. A., & Stockhinger, J. (2020). Literature review: Understanding information systems strategy in the digital age. *The Journal of Strategic Information Systems, 29*(4). https://doi.org/10.1016/j.jsis.2020.101642

Turanovic, J. J., & Pratt, T. C. (2014). "Can't stop, won't stop": Self-control, risky lifestyles and repeat victimization. *Journal of Quantitative Criminology, 30*(1), 29–56. https://doi.org/10.1007/s10940-012-9188-4

Turanovic, J. J., Pratt, T. C., & Piquero, A. R. (2016). Structural constraints, risky lifestyles, and repeat victimization. *Journal of Quantitative Criminology, 34,* 251–274. https://doi.org/10.1007/s10940-016-9334-5

Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M. K., & Webster, J. L. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior, 101,* 225–237. https://doi.org/10.1016/j.chb.2019.07.012

Wachs, S., Mazzone, A., Milosevic, T., Wright, M. F., Blaya, C., Gámez-Guadix, M., & O'Higgins Norman, J. (2021). Online correlates of cyberhate involvement among young people from ten European countries: An application of the Routine Activity and Problem Behaviour Theory. *Computers in Human Behavior, 123*. https://doi.org/10.1016/j.chb.2021.106872

Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M. K., & Webster, J. L. (2019). Lifestyles and routine activities: Do they enable different types of cyber abuse? *Computers in Human Behavior, 101*, 225–237. https://doi.org/10.1016/j.chb.2019.07.012

van de Weijer, S. G. A. (2019). Predictors of cybercrime victimization. Causal effects or biased associations? In R. Leukfeldt & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 83–111). Routledge. https://doi.org/10.4324/9780429460593

van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behaviour and Social Networking*. https://doi.org/10.1089/cyber.2017.0028

van Wilsem, J. (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. https://doi.org/10.1177/1043986213507402

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behaviour and Social Networking, 15*(3), 181–183. https://doi.org/10.1089/cyber.2011.0352

Wick, E. S., Nagoshi, C., Basham, R., & Jordan, C. (2017). Patterns of cyber harassment and perpetration among college students in the United States: A test of routine activities theory. *International Journal of Cyber Criminology, 11,* 24–38. https://doi.org/10.5281/zenodo.495770

Wilcox, P., Sullivan, C. J., Jones, S., & van Gelder, J.-L. (2014). Personality and opportunity: An integrated approach to offending and victimization. *Criminal Justice and Behavior, 41*(7), 880–901. https://doi.org/10.1177/0093854813520603

Wright, M. F., & Li, Y. (2021). Kicking the digital dog: A longitudinal investigation of young adults' victimization and cyber-displaced aggression. *Cyberpsychology, Behavior and Social Networking.* 448-454. http://doi.org/10.1089/cyber.2012.0061

Zhang, M.-C., Wang, L.-X., Dou, K., & Liang, Y. (2021). Why victimized by peer promotes cyberbullying in college students? Testing a moderated mediation model in a three-wave longitudinal study. *Current Psychology, 42.* https://doi.org/10.1007/s12144-021-02047-1.

Zhou, Y., Zheng, W., & Gao, X. (2019). The relationship between the Big Five and cyberbullying among college students: The mediating effect of moral disengagement. *Current Psychology, 38*, 1162–1173. https://doi.org/10.1007/s12144-018-0005-6.

Author biographies

Marko Mikkola (M. Soc. Sci) is Researcher in Faculty of Social Sciences of Tampere University, Finland. He conducts research related cybercrime and cyber harassment victimization.

Markus Kaakinen (PhD Soc.Sci) is a Postdoctoral researcher at the Institute of Criminology and Legal Policy at the University of Helsinki, Finland. His research focuses on criminology and social psychology of youth crime and aggressive behavior with a current emphasis on social media networks, cyberhate and hate crime.

Nina Savela (Dr. Soc. Sci.) is Postdoctoral researcher at Department of Social Sciences, LUT University, Lappeenranta, Finland.

Reetta Oksa (Dr. Soc. Sci) is Senior Researcher in Faculty of Information Technology and Communication Sciences. She conducts research related to human technology interaction, wellbeing and working life.

Iina Savolainen (PhD Soc.Sci) is Postdoctoral researcher at the Faculty of Social Sciences of Tampere University, Finland.

Atte Oksanen is Professor of Social Psychology and Vice Dean for Research at the Faculty of Social Sciences of Tampere University, Finland.