European Journal on Criminal Policy and Research (2023) 29:283–301
https://doi.org/10.1007/s10610-021-09497-0

Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors

Matti Näsi[1] · **Petri Danielsson**[1] · **Markus Kaakinen**[1]

Accepted: 22 August 2021 / Published online: 6 September 2021

Abstract
This study examines the prevalence of different types of cybercrime victimisation and their shared risk factors among the population of Finland. We examine how respondents' socio-economic background variables, past offline victimisation experiences, online activity, user skills, and protective measures impact the risk of the most common forms of online victimisation and online polyvictimisation. Our nationally representative survey data were collected from 5455 Finns aged 15 to 74 years (response rate 39%) as part of the Finnish National Crime Survey in 2018. According to our findings, the five most common forms of victimisation were malware, harassment, sexual harassment, hacking, and fraud. Online routines and exposure to potential offenders, along with past offline victimisation experiences, served as notable risk factors for a range of different victimisation experiences online. Our findings show slightly different SES risk factors for victimisation of different online offences, thereby indicating the diverse nature of different types of online victimisation. Our findings also show that young age, better financial situation, high internet use, and user skills, along with past offline victimisation of property crime and violence, associate with increased risk of online polyvictimisation. High user protection decreased the risk of online polyvictimisation.

Keywords Cybercrime · Offline victimisation · SES · Online use · User protection · Population sample · Online polyvictimisation

Introduction

Over the last few decades, new information and communication technologies have become an integral part of modern societies. From the premise of crime, this "technologisation" of societies has expanded both the toolset for many traditional forms of crime, as well as the environment where crime can occur, thereby enabling a new playground and new forms of criminal behaviour to ensue. In order to better understand the relationship between crime

✉ Matti Näsi
matti.j.nasi@helsinki.fi

[1] Institute of Criminology and Legal Policy, University of Helsinki, PO Box 24 (Unioninkatu 40), 00014 Helsinki, Finland

and technology, it is important to try to establish a comprehensive, population-level, basic understanding of the role of cybercrime in today's society.

Cybercrime, which in a broad sense serves as a collective term for all crime that either occurs in the online space or is aided by the use of technology (Näsi et al., 2015; Yar & Steinmetz, 2019), is as an umbrella term for a wide range of different offences. Although cybercrime is not a particularly new phenomenon, research that relies on nationally representative data sets remain relatively scarce (see, e.g. Oksanen & Keipi, 2013; van Wilsem, 2013; Reyns & Henson, 2016; Holt et al., 2018; Reep-van den Bergh and Junger 2018; see also, Virtanen, 2017), and the range of victimisation prevalence tends to vary notably between the surveys (see Reep-van den Bergh and Junger 2018 for an overview of victim prevalence in the existing population-level cybercrime victim surveys in Europe).

Further challenges in existing research on cybercrime are that many of the more notable and cited studies rely on college sample data, or data that is not representative at a wider age range of the general population (e.g. Holt & Bossler, 2008; Ngo & Paternoster, 2011; Bossler & Holt, 2010; Reyns et al., 2011; Bossler et al., 2012; Holt et al., 2016; Marcum et al., 2014; Reyns et al., 2016; see also e.g., Kigerl, 2012; Räsänen et al., 2016; Reyns et al., 2019). This means that information on the prevalence of different types of cybercrime victimisation and their risk factors on the level of the whole population is still lacking.

Much of the existing research has focused on specific online offence types. Only few studies have examined polyvictimisation in the online context, often combining both online and offline victimisation experiences in the context of interpersonal violence. Our research therefore provides a new approach and information concerning cybercrime victimisation. Cénat and colleagues (Cénat et al., 2019), for example, found an association between offline polyvictimisation and cybervictimisation, as offline polyvictimisation increased the risk of online victimisation. Sargent and colleagues (Sargent et al., 2016) found that experiences of cybervictimisation and psychological intimate partner violence are associated with problematic mental health outcomes. A study by Hamby and colleagues (Hamby et al., 2018) found that digital polyvictimisation is associated with an increased risk for anxiety and post-traumatic stress symptoms.

The aim of this study, however, is to extend our understanding of cybercrime victimisation by examining the risk factors for not only a variety of different types of online victimisation, but also the risk factors for online polyvictimisation in a population-level context. Our aim is to contribute to the existing research by relying on nationally representative survey data from Finland. In this study, we will provide information on population-level victim prevalence of a wide range of different online offences. We will then focus on the most common forms of online victimisation to try answer the following questions:

> How do respondents' (1) socio-economic background variables, (2) online behaviour, and (3) past victimisation experiences of traditional crime associate with the risk of victimisation of different types of cybercrime as well as online polyvictimisation?

By doing so, we aim to facilitate a better understanding of how these aspects reflect on the risk of victimisation regarding different types of cybercrime, as well accumulation of different victimisation experiences. Furthermore, it will also provide information on whether victims of cybercrime are a separate group of crime victims compared to victims of traditional crime. As the majority of existing cybercrime research has focused on adolescents and young adults (see, e.g. Notten & Nikken, 2016), we expand on the current field by studying victims of all ages. Although Finland is a small country, it has a history of

being a very tech-savvy nation, having been dubbed as a forerunner country in technology adoption as early as the turn of the millennium (Castells & Himanen, 2002). Finland continues to not only have one of the highest Internet penetration rates in the world (Eurostat, 2021), while also being among the most ICT-skilled nations in the world (ITU, 2021). It is therefore interesting to examine how this premise reflects on the rate and risk factors of cybercrime victimisation and polyvictimisation.

In the next section, we highlight past research on cybercrime victimisation and related theoretical perspective and follow up with a description of data and methodology. We then describe our main results, before moving on to a final discussion of our key findings.

Cybercrime Victimisation and Risk Factors

Existing research regarding different forms of online victimisation and their risk factors is multifaceted. Not only is there variance in risk factors, such as victims' SES, when comparing different types of online victimisation (see, e.g. Ngo & Paternoster, 2011), but research on specific types of online victimisation has resulted in somewhat inconsistent findings. For example, although young age has been found to be a common risk factor for various forms of online victimisation (e.g. Näsi et al., 2015; Reyns et al., 2019; van Wilsem, 2013), the challenge is that a majority of the existing research focuses on adolescents and young adults; thus, the picture concerning older age groups remains incomplete.

In terms of gender, females are commonly found to be more likely victims of sexual harassment (Eckert, 2018; Henry and Powell, 2018; Holt & Bossler, 2008), but the results concerning more general forms of online harassment are mixed (e.g. Näsi et al., 2015, 2017; van Wilsem, 2013), and that males have commonly been found to be more likely victims of other types of online offences (e.g. Bergmann et al., 2018; Milani et al., 2020; Näsi et al., 2015). Education and financial status do not appear to be more notable factors regarding online victimisation than they do in relation to offline crime. There is some evidence suggesting that financial challenges serve as a risk factor for online victimisation in general (e.g. Näsi et al. 2015; Oksanen & Keipi, 2013), whereas a recent study by Milani and colleagues (Milani et al., 2020), for example, found that higher education served as a risk factor for malware, fraud, and hacking victimisation.

Existing research has also examined the relationship between offline and online victimisation. A common finding is that those who have been victims online were more likely to report offline victimisation experiences as well. However, again, majority of these studies examine adolescents and young adults, with a strong focus on different forms of harassment victimisation (e.g. Choi et al., 2019; Ioannou et al., 2018; Mitchell et al., 2011; Räsänen et al., 2016; Reyns & Fisher, 2018; Sumter et al., 2012; Zetterström Dahlqvist & Gillander Gådin, 2018). Therefore, there is a need for more information concerning overlapping offline-online victimisation experiences with regard to a wider range of online offences and among a wider range of age categories (see also Oksanen & Keipi, 2013).

Cybercrime and Theory

From a theoretical perspective, the existing research on cybercrime victimisation is relatively one-dimensional as much of the prior research on cybercrime relies on routine activity theory (RAT). Like the vast majority of previous research, this study relies on routine activity theory in examining cybercrime victimisation. Although RAT was developed to explain why traditional crime occurs, it has also been widely adopted in the online context.

The basic premise of routine activity theory is that in order for crime to occur, a motivated offender, a suitable target, and the absence of a capable guardian must converge in space and time (Cohen & Felson, 1979). The presence of a motivated offender tends to be a given whether it is an offline or online space. Target suitability and the role and presence of capable guardians in the online context, however, require a slightly modified approach compared to traditional crime. There have also been attempts to further develop the core premises of RAT to be more applicable in the online context. Holt and Bossler (2008), for example, brought forward a slightly updated theoretical approach dubbed as lifestyle-routine activities theory (see also, e.g. Reyns et al., 2011, 2019). However, most studies on cybercrime continue to rely on the "traditional" version of RAT.

As noted, the role of online routines is at core of much the existing cybervictimisation research, which covers a wide range of different offences, such as identity theft (e.g. Burnes et al., 2020; Reyns, 2013; Reyns & Henson, 2016); malware, ransomware, and misuse of personal data (e.g. Bergmann et al., 2018; Holt & Bossler, 2008; Holt et al., 2020; Kigerl, 2021); spam and phishing (e.g. Kigerl, 2012, 2021), online hate (e.g., Kaakinen et al., 2018; Räsänen et al., 2016; Wachs et al., 2021); online harassment (e.g., Näsi et al., 2017; Reyns et al., 2011; van Wilsem, 2011); and online bullying (e.g. Aboujaoude et al., 2015; Li et al., 2020; Tokunaga, 2010), grooming (Wachs et al., 2020), fraud (Whitty, 2019), business crime (e.g. Williams et al., 2019), and with personality traits of the victims (e.g. van de Weijer et al., 2017). This has resulted in one of the most systematic, and not altogether surprising finding that the more time spent online contributes to greater exposure to potential offenders and for victimisation (see also, Milani et al., 2020; Leukfeldt & Yar, 2016).

Some studies suggest that it is not merely excessive time spent online, but what users actually do while online that counts (Kaakinen et al., 2021). Therefore, noting that both online target suitability and the role of guardianship are influenced by how visible one is online, what types of activities they undertake, as well as what kind of protective measures they have in place, both in relation to hardware and the services they use (e.g., Álvarez-García et al., 2019; Miró-Llinares et al., 2020; Branley & Covey, 2017; Notten & Nikken, 2016; see also, Macaulay et al., 2020; White et al., 2017; Reyns et al., 2019; Reyns & Henson, 2016; Reyns et al., 2011; Holt & Bossler, 2008). Furthermore, elements such as user skills can function as a protective or target-hardening factor that makes users less suitable victims for potential offenders. However, earlier research has also reported user skills to be positively associated with the risk of cybercrime victimisation (see, e.g. van Wilsem, 2013). This may reflect the qualitative differences between the least and most fluent internet users as the most skilled users tend to show more diverse use of online services (Hargittai, 2010; Hargittai & Hinnant, 2008, see also Cheng et al., 2020), suggesting that the most skilled internet users would also be more exposed to a wider variety of online offenders. However, a recent study by Milani and colleagues (Milani et al., 2020) found IT skills to have little impact with regard to cybervictimisation; thus, the role of user skills is somewhat mixed (see also Hawdon et al., 2020). We are therefore also keen to examine in our analysis how the level of online activity and thus visibility, level of user skills, along with level of user protection, associate with the risk of different forms of cybervictimisation as well as polyvictimisation. This makes for an interesting analysis, particularly since Finns have been found to be among the most active and skilled users of Information and Communication Technologies (ICT) in the world, (Eurostat, 2021; ITU, 2021).

Beyond online activity and routines, few studies have examined the association between self-control and cybervictimisation. A study by Whitty (2019) found that in addition to online routines, people who score high on the scale of impulsivity, as well as sensation

seeking and addictive behaviour (along with being older in age), had a higher risk of fraud victimisation. Studies by Bossler and Holt (2010) and Reyns and Fisher (2018) found weak connections with low self-control and cybervictimisation, whereas a study by Holt and colleagues (Holt et al., 2020) found a connection between low self-control and malware victimisation, and van Wilsem (2011) found a similar connection with regard to online hacking and harassment victimisation (see also Louderback & Antonaccio, 2020). These aspects of self-control, however, are not examined in this study.

Data and Methods

Our data were collected as part of the Finnish National Crime Survey (FNCS-2018), a nationally representative victim survey conducted in the fall of 2018. The FNCS has been conducted annually since 2012 and consists of standard sections on victimisation and fear of crime as well as a thematic module. In 2018, the thematic module focused on cybercrime victimisation, internet use, and behaviour in the online environment. A gross sample of 14,000 persons aged 15 to 74 years and with permanent residence in Finland was sampled from the Population Information System using a stratified random sampling with gender, age-group, and region as the strata. Younger age groups were oversampled relative to the older age groups. All respondents were sent a paper questionnaire with an option to participate online. The paper questionnaire was available in Finnish or Swedish, the main official languages in Finland, while the online questionnaire was additionally available in English and Russian. The availability of multiple languages in the online survey was indicated in a multi-language cover letter that was sent along with the Finnish-language paper questionnaire to persons whose registered native language was neither Finnish nor Swedish. Altogether, 5455 persons participated in the survey, making for a 39.0% response rate. For the analysis, the data were weighted to account for varying inclusion probabilities and unit non-response in each stratum.

Dependent Variables and Independent Variables

The survey included a list of 10 different cybervictimisation items (see appendix for a more detailed description of the items). In short, these items included *phishing*, *fraud*, *identity theft*, *malware*, *hacking*, *sexual harassment*, *other harassment*, *violation of personal privacy*, *defamation*, and *threat of violence*. The items were measured both as lifetime experience and in the preceding 12 months. In the following, we provide descriptive statistics for both measures, but focus on victimisation in the preceding 12 months in the models. For the multivariate analyses, as well as Poisson regression analysis of polyvictimisation, we restrict the analysis to the five most common forms of victimisation: *malware*, *other/general harassment*, *sexual harassment*, *hacking*, and *fraud* (see also Table 2). In short, in the survey, these five items were described as follows: "*Your computer or smart device has been infected by malware*" (malware), "*You have received sexually harassing messages on the internet*" (sexual harassment), "*You have received other harassing messages on the internet*" (general harassment), "*Your email or social media account has been hacked*" (hacking), "*Your debit or credit card has been used on the internet without your permission*" (fraud). Therefore, we included in our more detailed analysis only the five most common forms of cybervictimisation. This was done so that both analyses would focus on the same forms of victimisation. The prevalence rates for the other forms of victimisation were

too low for a more nuanced analysis and were thus excluded from further exploration. All the outcomes are binary, with 0 indicating no victimisation and 1 indicating being victimised at least once in the prior 12 months. In terms of polyvictimisation, the dependent variable was constructed as counts with values ranging from 0 to 5 types of victimisation during the previous 12 months. Six percent of the respondents reported at least some type of online victimisation experience in the prior 12 months.

As for independent variables (see Table 1 for descriptive statistics of the independent variables), we included both SES background variables, namely *gender*, *age-group*, *educational level*, and *perceived financial situation*, along with items that measure activity and behaviour in an online environment. Furthermore, as we were also keen to examine

Table 1 Descriptive statistics of the independent variables

	N	%
Gender		
Male	2677	49.5
Female	2732	50.5
Age		
15–24	821	15.2
25–34	937	17.3
35–54	1747	32.3
55–74	1901	35.2
Education		
Tertiary	1930	35.4
Secondary	2773	50.8
Primary	752	13.8
Financial situation		
Good	1646	30.7
Challenging	3724	69.3
Internet use		
Lowest use	1816	33.7
Medium use	1773	32.9
Highest use	1804	33.5
User skills		
Lowest skills	1663	30.9
Medium skills	1801	33.4
Highest skills	1923	35.7
User protection		
Lowest protection	1585	29.4
Medium protection	1850	34.3
Highest protection	1952	36.2
Victim property crime		
No	4441	81.4
Yes	1014	16.6
Victim violent crime		
No	4630	84.9
Yes	825	15.1

whether there was and overlap with online and offline victimisation experiences, we included prior offline victimisation, both *property* and *violence*, as control variables.

The measures for gender and 10-year age-group were derived from the Population Information System, which is a computerised national register containing all the basic information about Finnish citizens and foreign citizens residing in Finland on a permanent or temporary basis, while the measures for educational level and the perceived financial situation of the household were obtained from the survey. Age was classified into four groups: 15 to 24, 25 to 34, 35 to 54, and 55 to 74-year olds. Educational level was classified into three groups: primary, secondary, and tertiary education (see the appendix for a more detailed description). The measure for perceived financial situation was constructed as a dichotomised variable, where the group with financial difficulties included respondents who indicated that, considering all of the combined income in their household, it was "very hard", "hard", or "somewhat hard" to manage financially with that income, whereas the group with no financial difficulties included respondents who reported that it was "somewhat easy", "easy", or "very easy" to manage financially with their combined income.

Internet use was measured using 10 items (see the appendix for the full item list) asking "*How often do you use the internet for the following purposes*", such as, for example online banking, and reading news online, with a 5-point response scale ranging from "never" to "daily". We then summarised responses to all 10 items and formed three equal-sized (33/66 tertile) activity groups based on the item scores: high activity, medium activity, low activity.

Computer skills were measured using seven items (see appendix for a detailed description of the items) based on how often the respondent used certain types of programmes, or used a computer for certain purposes (use spreadsheets such as Microsoft Excel, use word processors such as Microsoft Word, use programming languages for programming or writing computer code, draw up diagrams, figures, or tables on a computer, write up reports on a computer, use a computer for basic mathematical calculations or formulae), with a 5-point response scale ranging from "never" to "daily". We then summarised responses to all seven items and formed three equal-sized (33/66 tertile) skills groups based on the item scores: high skills, medium skills, low skills.

The measure for *user protection* was constructed from six items (see appendix for a detailed description of the items) focusing on the protective measures respondents took in their online behaviour, where the respondents were asked, for example, how often they used protective measures such as long and complicated passwords, with a 5-point response scale ranging from "never" to "always". We then summarised responses to all six items and formed three equal-sized (33/66 percentiles) protection-level groups based on the item scores: high protection, medium protection, low protection.

Offline victimisation was measured both in terms of *property* and *violence*. Property crime victimisation in the survey was measured by asking respondents whether "in the past 12 months they had experienced theft of personal property, such as wallet, purse, credit card or mobile phone, taking place outside your home." with yes/no listed as the options for responses. Offline violence victimisation in the past 12 months was measured using a question set with 11 different types of violence victimisation (see appendix for full item list). The question set had a 4-point response scale which included the response options "Nobody", "Former or present spouse, cohabiting partner or dating partner", "Some other person you know closely", and "An unknown person or a person you know only remotely". We then summarised responses to all 11 items and formed combined binary item of victims of any violent crime in the past 12 months.

Analysis

For our analysis, firstly, we provide descriptive statistics of all the victimisation items, secondly, estimate logistic regression models, and thirdly Poisson regression models for the selected outcomes. The estimates from the logistic regression models are reported in average marginal effects (AME) (see also Bergmann et al., 2018). The reason for this is to give a more descriptive picture of the results. Compared to the more conventional odds ratios, average marginal effects give a more descriptive, and perhaps more straightforward interpretation of the results, as the risk is expressed as a percentage point change in probability. We chose to use dichotomous and polychotomous variables in order to present marginal effects more easily. Marginal effects for continuous variables tend to be less informative and difficult to interpret. Average marginal effects are reported in Table 3. We estimated Poisson regression models with the numbers of crimes as a dependent variable with regard to our analysis of polyvictimisation. The estimates from the Poisson regression models are reported in incidence rate ratio (IRR). These results are reported in Table 4. The data were analysed using Stata.

Results

Table 2 presents the estimated prevalence rates for 10 different forms of cybercrime victimisation, both over one's lifetime and in the 12 months preceding the survey. By far, the most common form of victimisation was malware, followed by other harassment, sexual harassment, hacking, and fraud. For the other five forms of victimisation, the lifetime prevalence rate was less than 5% and prevalence in the preceding 12 months was circa 1%. For further analysis, we focus on the five most common forms of cybervictimisation.

In Table 3, we show the results from the logistic regression models in terms of victimisation in the prior 12 months. We present the estimates for statistically significant coefficients in average marginal effects.

Malware Gender and age were associated with being a victim of malware. Women were 6.5 percentage points less likely to report being a victim of malware, while the probability for respondents in the oldest age group was 9.7 percentage points higher compared to the youngest age group. Respondents with secondary education were 2.4 percentage points

Table 2 Prevalence of cyber victimisation, over the lifetime and in the past 12 months (%)

	Lifetime	Past 12 months
Malware	42.3	12.4
(Other) Harassment	16.5	9.2
Sexual harassment	14.5	8.6
Hacking	8.8	3.1
Fraud	6.3	2.2
Defamation	4.3	1.2
Threat of violence	3.5	1.2
Phishing	2.2	0.7
Violation of personal privacy	1.6	0.5
Identity theft	1.3	0.4

Table 3 Logistic regression models for different forms of cybercrime victimisation, average marginal effects AME, and (CI 95%)

	Malware	Other harassment	Sexual harassment	Hacking	Fraud
Gender					
Male	Ref	Ref	Ref	Ref	Ref
Female	−6.5*** (−8.50–−4.54)	2.8** (1.03–−4.54)	Not sig	Not sig	Not sig
Age					
15–24	Ref	Ref	Ref	Ref	Ref
25–34	Not sig	−4.8** (−7.80–−1.80)	−4.8** (−8.08–−1.42)	Not sig	Not sig
35–54	4.9*** (2.02–7.79)	Not sig	−6.1*** (−9.05–−3.08)	Not sig	2.8*** (1.62–3.88)
55–74	9.7*** (6.45–12.99)	Not sig	−3.9* (−7.36–−0.53)	−2.7** (−4.69–−0.71)	1.8* (0.58–3.02)
Education					
Tertiary	Ref	Ref	Ref	Ref	Ref
Secondary	2.6* (0.32–4.78)	Not sig	Not sig	Not sig	−1.2* (−2.19–−0.11)
Primary	Not sig	Not sig	−3.4* (−6.51–−0.34)	Not sig	−2.1*** (−3.33–−0.95)
Financial situation					
Good	Ref	Ref	Ref	Ref	Ref
Challenging	−5.7*** (−8.08–−3.38)	−2.5* (−4.53–−0.53)	−2.3* (−4.32–−0.28)	Not sig	Not sig
Internet use					
Lowest use	Ref	Ref	Ref	Ref	Ref
Medium use	3.5** (0.98–5.93)	3.8*** (1.83–5.79)	3.6*** (1.49–5.64)	1.4* (0.09–2.67)	Not sig
Highest use	5.0*** (2.10–7.91)	6.9*** (4.50–9.26)	5.4*** (2.98–7.84)	1.9** (0.46–3.32)	1.3* (0.07–2.60)
User skills					
Lowest skills	Ref	Ref	Ref	Ref	Ref
Medium skills	5.8*** (3.30–8.25)	4.6*** (2.51–6.72)	3.6*** (1.40–5.71)	1.6* (0.20–2.95)	Not sig
Highest skills	6.4*** (3.40–9.40)	5.3*** (2.89–7.72)	3.8** (1.40–6.25)	Not sig	Not sig
User protection					
Lowest protection	Ref	Ref	Ref	Ref	Ref
Medium protection	−3.2* (−5.98–−0.38)	Not sig	Not sig	Not sig	Not sig
Highest protection	−4.8*** (−7.49–−2.08)	Not sig	Not sig	Not sig	Not sig

Table 3 (continued)

	Malware	Other harassment	Sexual harassment	Hacking	Fraud
Victim property crime					
No	ref	ref	ref	ref	ref
Yes	not sig	10.6** (2.69–18.42)	7.7* (0.06–15.31)	not sig	8.7** (2.23–15.29)
Victim violent crime					
No	ref	ref	ref	ref	ref
Yes	9.4*** (5.85–13.05)	7.0*** (4.17–9.83)	8.2*** (5.30–11.14)	3.6*** (1.74–5.49)	2.9*** (1.12–4.59)

Significance levels: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$

Table 4 Poisson regression models for polyvictimisation, incidence rate ratio (IRR), and CI 95%

	IRR	(CI 95%)
Gender		
Female	Not sig	
Age		
25–34	0.8*	0.64–0.96
35–54	Not sig	
55–74	Not sig	
Education		
Secundary education	Not sig	
Primary education	Not sig	
Finacial situation		
Challenging	0.7***	0.62–0.8
Internet use		
Medium	1.5***	1.23–1.74
High	1.8***	1.49–2.17
User skills		
Medium	1.6***	1.34–1.94
High	1.7***	1.40–2.11
User protection		
Medium	Not sig	
High	0.8**	0.72–0.97
Victim property crime		
Yes	1.9***	1.47–2.44
Victim violence		
Yes	2.0***	1.72–2.26

Significance levels: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$

more likely to report being victims than respondents with tertiary education. Respondents in challenging financial situations were 5.7 percentage points less likely to report being victims compared to respondents with a good financial situation. Both higher internet use and user skills were associated with malware victimisation. Intermediate (AME 3.5) and high (AME 5.0) internet usage were associated with higher victimisation risk, while higher perceived skills (medium skills AME 5.8 and high skills AME 6.4) in computer use were likewise positively associated with a higher risk of malware victimisation. Personal protective measures were negatively associated with becoming a victim of malware (AME − 4.8 percentage points for highest protection). Notably, malware victimisation was the only outcome where the personal protective measures were statistically significant. In terms of offline victimisation, respondents who had been victims of violence were 9.4 percentage points more likely to report malware victimisation.

Other (Non-sexual) Harassment Women were 2.8 percentage points more likely to report victimisation than men. In terms of age, respondents in the age group 25 to 34 were 4.8 percentage points less likely to report victimisation compared to the youngest age group. Financial difficulties were negatively associated with harassment (AME − 2.5). Both higher internet use (medium use AME 3.8 and high use AME 6.9) and higher user skills were positively associated with harassment victimisation. Respondents belonging

to the intermediate skills group were 4.6 percentage points less likely to report victimisation, while the estimate for the high skills group was 5.3 percentage points. In terms of past offline victimisation, respondents who had been victims of property crime were 10.6 percentage points more likely to report online harassment victimisation. In addition, those who had been victims of violence were 7.0 percentage points more likely to report victimisation.

Sexual Harassment Unlike with non-sexual harassment, gender differences were not statistically significant. Respondents in the youngest age group were more likely to report being victims of sexual harassment, as the marginal effects in the older groups ranged from 3.9 to 6.1 percentage points less likely compared than the youngest age group. Respondents with self-reported financial difficulties were less likely to report sexual harassment (AME − 2.3). In line with the bulk of the other outcomes in the study, respondents with an intermediate (AME 3.6) or high (AME 5.4) level of internet activity were more likely to become victims compared to those with low internet activity. Again, as with other forms of cybercrime, higher computing skills were positively associated with sexual harassment victimisation as those with the highest skills were 3.8 percentage points more likely to report victimisation compared to respondents with the lowest skills. Respondents who had been victims of offline property crime were 7.7 percentage points more likely to report online sexual harassment victimisation. Respondents who had been victims of violence were 8.2 percentage points more likely to report victimisation.

Hacking In terms of hacking, respondents in the oldest age group were 2.7 percentage points less likely to report victimisation of hacking compared to the youngest age group. Similarly to malware victimisation, internet usage and high self-reported computer skills were positively associated with being a victim of hacking. AME for respondents in medium usage group was 1.4 and 1.9 for respondents in the high usage group. Respondents in both the intermediate and high user skills groups were 1.6 percentage points more likely to become victims compared to those with the lowest user skills. In addition, respondents who had been victims of offline violence were 3.6 percentage points more likely to report hacking victimisation.

Fraud The result regarding fraud shows that respondents in the age group 35 to 54 had a 2.8 percentage point higher probability to report being victims of fraud compared to respondents in the youngest age group. AME in the oldest age group was 1.8 percentage points. Respondents with secondary education had a 1.2 percentage points lower and respondents with primary education had a 2.1 percentage points lower probability to report being victimised compared to respondents with tertiary education. In addition, respondents who had been offline victims of property crime were 8.7 percentage points more likely to report victimisation and respondents who had been victims of violence were 2.9 percentage points more likely to report fraud victimisation.

In Table 4, we show the results from the Poisson regression models for polyvictimisation in the past 12 months. Here, we describe results that were statistically significant. Our findings show that compared to the youngest age group, those in the age group 25–34 years were less at risk of polyvictimisation (IRR 0.8). However, this risk was not significant in older age groups. In terms of financial situation, those who were in a challenging financial situation were less at risk of polyvictimisation (IRR 0.7) compared to those in a better financial situation. Respondents reporting medium (IRR 1.5) and high (IRR 1.8) internet

use and medium (IRR 1.6) and high (IRR 1.7) user skills were more at risk of polyvictimisation compared to those with low activity and skills. Those reporting high user protection (IRR 0.8) were less at risk of polyvictimisation compared to those reporting low user protection. Finally, both victims of property crime (IRR 1.9) and violence (IRR 2.0) were more at risk of polyvictimisation compared to those who had not been victims.

Discussion

The aim of this study was to analyse the prevalence of different types of cybercrime victimisation and their shared risk factors among Finnish population. In addition, it also examined risk factors for polyvictimisation in the online context, thus providing advanced approach in cybercrime research. Earlier studies using nationally representative data have also been relatively rare (see, e.g. Oksanen & Keipi, 2013; van Wilsem, 2013; Reyns & Henson, 2016; Holt et al., 2018; Reep-van den Bergh and Junger 2018; see also, Virtanen, 2017), which may explain variation in reported victimisation prevalence between different studies. Studies that also examine polyvictimisation in the online context are even rarer (e.g. Hamby et al., 2018).

Our findings indicate that there is substantial variation in the prevalence of different forms of cybercrime victimisation at the population level. Malware and different forms of harassment are by far the most common forms of online victimisation, with circa 10% of the respondents reporting victimisation experiences during the past year. The victimisation prevalence for the five least common forms of online victimisation was only about 1%. Interestingly, the prevalence rates for the most common online offences were roughly at the same level as the prevalence estimates for the "offline" offences in the Finnish National Crime Victim Survey. This is notable, as the fear of cybercrime victimisation greatly exceeds the fear of traditional forms of violence (see Danielsson & Näsi, 2019). Although not shown in the tables, our survey findings also show that 25% of the respondents reported some form of cybervictimisation in the past 12 months. This seems to be significantly higher than Oksanen and Keipi's (2013) findings from a 2009 survey, in which 2.5% of Finns reported experiencing some form of cybervictimisation over the past 3 years. Besides just the increase in different types of online threats, it may also be that people are increasingly more aware of cybercrime, and thus may be more sensitive in recognising and reporting online offences.

Risk Factors for Cybercrime Victimisation

Our main findings concerning the different risk factors for different forms of online victimisation were threefold. Firstly, online routines and activity play a significant role, both in the variety of different types of online victimisation as well as polyvictimisation. Therefore, the theoretical premise of Routine Activity Theory (RAT) also lines up well with our findings. The more active people are online, the more exposed to potential offenders and other dangers, the more likely they are to become victims. Our findings are in line with much of the existing research on online of victimisation (e.g. Leukfeldt & Yar, 2016). While we controlled for internet usage in our models, it is also possible that only certain types of online behavioural patterns expose individuals to, for example, harassment or malware, which may explain the observed results (e.g. Bergmann et al., 2018; Branley & Covey,

2017; Reyns et al., 2019). It appears that our measure of user skills behaves similarly to internet use activity. According to our findings, user skills do not function as a protective factor that would make any given individuals less suitable victims for cyber offenders. This makes sense, however, since earlier research has suggested that the most fluent users also report more diverse internet use (see, e.g. Hargittai, 2010; Hargittai & Hinnant, 2008). This means that users' skills generally tend to reflect more active use of various forms of new technology, thus mirroring the window of exposure. Therefore, it is not surprising that these same elements are associated with a greater risk of polyvictimisation as well. It also shows that in the online context, a more active presence appears to diversify the risk range of victimisation.

The results concerning user protection were not very surprising. Protective measures work better to counteract risks related to malware and viruses than they do with social actions and behaviour. For the average user, the different protective measures are undertaken by the manufacturers, developers, and platform providers of the new forms of technology matter when the machine is the target. The challenge is what to do when a specific person is the target. Future studies would also benefit from a more detailed analysis on malware victimisation, particularly when it comes to specific forms of malware. However, high user protection did reduce the risk of polyvictimisation. It may be that those respondents who pay more attention to aspects of user protection are slightly more wary in their general online behaviour.

Secondly, offline victimisation matters. What is notable is that prior offline victimisation serves as a risk factor for such a wide range of online victimisation experiences as well as online polyvictimisation. This further supports and adds to the past research findings that have noted that online and offline victims are not completely separate groups of victims, but rather the online environment has expanded the victimisation environment among those who are already victims offline (Choi et al., 2019; Ioannou et al., 2018; Mitchell et al., 2011; Oksanen & Keipi, 2013; Räsänen et al., 2016; Reyns & Fisher, 2018; Sumter et al., 2012; Weulen Kranenbarg et al., 2019; Zetterström Dahlqvist & Gillander Gådin, 2018), thus, suggesting accumulation of negative experiences, in both an offline and online context where one is not protected even when the offender is not physically present. Recent research has noted how coercive control has expanded into the digital platforms and communication tools (e.g. Dragiewicz et al., 2018; Harris & Woodlock, 2019), therefore perhaps in part explaining the overlap in online harassment victimisation, as well as in having your email or social media account hacked, with offline violence victimisation. However, our findings do still raise further questions, such as why past experiences of violence victimisation raise the risk of victimisation regarding so many different types of online victimisation and polyvictimisation. Is it merely an accumulation of all kinds of negative experiences? There is clearly a need for further research.

Thirdly, our results indicate, not altogether surprisingly, that different types of online offences do have slightly different risk factors. Although offline victimisation increased the risk for online victimisation, the role of different socio-economic background variables was in some cases different compared to risk factors regarding many forms of offline victimisation. For example, a weaker financial situation has been found to be a risk factor for many types of offline victimisation (e.g. Aaltonen et al., 2012; Levitt, 1999; Nilsson & Estrada, 2003; Thacher, 2004; Tilley et al., 2011); yet in our findings, a good financial situation actually increased the risk of malware victimisation and different forms of online harassment, as well as polyvictimisation, even after controlling for age and activities in the online environment. Furthermore, education does not play a particularly clear role when it comes to online victimisation (see also, Bergmann et al., 2018).

It is possible that those in a better financial position are more at risk partly because they tend to be more active internet users (Statistics Finland, 2018) in ways that are not captured by our measures for online activity and thus are potentially more exposed to a wider range of online offenders and offences. It may also simply be that they have a larger "attack surface" or, in other words, have more devices at their disposal. Furthermore, in the online context, the (potentially protective) neighborhood effect also disappears (Thacher, 2004; Tilley et al., 2011). One does not have protective physical surroundings, such as living in a gated community, or living in an otherwise safe part of town, thus potentially levelling the playing field for crime to occur. These are certainly elements that warrant further research.

In terms of other risk factors, findings concerning age and gender were mixed. Men in the older age groups were more likely in harm's way with regard to malware and older respondents becoming victims of fraud (see also Whitty, 2019). In terms of fraud, it may be that older people use the likes of credit and debit cards more actively and in more diverse settings, thus facing greater risk of misuse. It may be that malware victimisation is in part due to the type of content consumption older men undertake, such as visiting sites with pornographic content (see Bergmann et al., 2018). It appears that those in the youngest age group were more at risk when it came to polyvictimisation. It may be that adolescents and young adults are more diverse in their online use and were therefore more exposed to a variety of different online risks. Young women were more at risk for non-sexual online harassment, yet gender did not play a significant role in sexual harassment. This is an interesting finding that warrants further research. A four-nation study by Näsi and colleagues (Näsi et al., 2015) from a few years ago found sexual harassment to be the least common form of online victimisation among adolescents and young adults from Finland, Germany, the UK, and the USA (also see the findings on online harassment from Reep-van den Bergh and Junger 2018). However, our results indicate that online harassment victimisation in general appears increasingly more common, and in many cases, a non-gender specific part of the harassment and abuse toolkit.

All in all, our results line up rather well with prior research on cybercrime victimisation, as well as raise a few points to note in future research. There are only a few studies that have examined online polyvictimisation; thus, our research also helps to extend our understanding of cybervictimisation. Furthermore, by relying on population-level data, our study provides cumulating empirical evidence in the study of online victimisation.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s10610-021-09497-0.

Funding Open access funding provided by University of Helsinki including Helsinki University Central Hospital.

Declarations

Conflict of Interest The authors declare no competing interests.

References

Aaltonen, M., Kivivuori, J., Martikainen, P., & Sirén, R. (2012). Socioeconomic differences in violent victimization: Exploring the impact of data source and the inclusivity of the violence concept. *European Journal of Criminology, 9*(6), 567–583.

Aboujaoude, E., Savage, M. W., Starcevic, V., & Salame, W. O. (2015). Cyberbullying: Review of an old problem gone viral. *Journal of Adolescent Health, 57*(1), 10–18.

Álvarez-García, D., Núñez, J. C., González-Castro, P., Rodríguez, C., & Cerezo, R. (2019). The effect of parental control on cyber-victimization in adolescence: The mediating role of impulsivity and high-risk behaviors. *Frontiers in Psychology, 10*, 1159.

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior, and Social Networking, 21*(2), 84–90.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*(3), 227–236.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society, 44*(4), 500–523.

Branley, D. B., & Covey, J. (2017). Is exposure to online content depicting risky behavior related to viewers' own risky behavior offline? *Computers in Human Behavior, 75*, 283–287.

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports, 17*.

Castells, M., & Himanen, P. (2002). *The information society and the welfare state: The Finnish model*. Oxford University Press Inc.

Cénat, J. M., Smith, K., Hébert, M., & Derivois, D. (2019). Polyvictimization and cybervictimization among college students from France: The mediation role of psychological distress and resilience. *Journal of Interpersonal Violence,* 1–20.

Cheng, C., Chan, L., & Chau, C. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior, 108*, 106311.

Choi, K., Cho, S., & Lee, J. R. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. *Computers in Human Behavior, 100*, 1–10.

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

Danielsson, P., & Näsi, M. (2019). Suomalaiset väkivallan ja omaisuusrikosten kohteena 2018 - Kansallisen rikosuhritutkimuksen tuloksia [Finns as victims of violence 2018 – Results from the National Crime Victim survey] Kriminologian ja oikeuspolitiikan instituutti, Katsauksia; nro 35/2019.

Van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking, 20*(7), 407–412.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies, 18*(4), 609–625.

Eckert, S. (2018). Fighting for recognition: Online abuse of women bloggers in Germany, Switzerland, the United Kingdom, and the United States. *New Media & Society, 20*(4), 1282–1302.

Eurostat. (2021). *Digital economy and society*. https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database. Accessed 27.5.2021.

Hamby, S., Blount, Z., Smith, A., Jones, L., Mitchell, K., & Taylor, E. (2018). Digital poly-victimization: The increasing importance of online crime and harassment to the burden of victimization. *Journal of Trauma & Dissociation, 19*(3), 382–398.

Hargittai, E. (2010). Digital na (t) ives? variation in internet skills and uses among members of the "Net Generation." *Sociological Inquiry, 80*(1), 92–113.

Hargittai, E., & Hinnant, A. (2008). Digital inequality: Differences in young adults' use of the internet. *Communication Research, 35*(5), 602–621.

Harris, B. A., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology, 59*(3), 530–550.

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*(4), 546–562.

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse, 19*(2), 195–208.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25.

Holt, T. J., Fitzgerald, S., Bossler, A. M., Chee, G., & Ng, E. (2016). Assessing the risk factors of cyber and mobilephone bullying victimization in a nationally representative sample of Singapore youth. *Journal of Offender Therapy and Comparative Criminology, 60*(5), 598–615.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2018). Assessing the macro-level correlates of malware infections using a routine activities framework. *International Journal of Offender Therapy and Comparative Criminology, 62*(6), 1720–1741.

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review, 38*(2), 187–206.

Ioannou, M., Synnott, J., Reynolds, A., & Pearson, J. (2018). A comparison of online and offline grooming characteristics: An application of the victim roles model. *Computers in Human Behavior, 85*, 291–297.

ITU (2021) *Measuring digital development: Facts and figures 2020.* https://www.itu.int/en/ITU-D/Statistics/Pages/ff2020interactive.aspx. Accessed 27.5.2021.

Kaakinen, M., Oksanen, A., & Räsänen, P. (2018). Did the risk of exposure to online hate increase after the November 2015 Paris attacks? A group relations approach. *Computers in Human Behavior, 78*, 90–97.

Kaakinen, M., Koivula, A., Savolainen, I., Sirola, A., Mikkola, M., Zych, I., Paek, H-J, & Oksanen, A. (2021). Online dating applications and risk of youth victimization: A lifestyle exposure perspective. *Aggressive Behavior* (Advance online publication).

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470–486.

Kigerl, A. (2021). Routine activity theory and malware, fraud, and spam at the national level. *Crime, Law and Social Change*, 1–22.

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

Levitt, S. D. (1999). The changing relationship between income and crime victimization. *Economic Policy Review, 5*(3).

Li, Q., Luo, Y., Hao, Z., Smith, B., Guo, Y., & Tyrone, C. (2020). Risk factors of cyberbullying perpetration among school-aged children across 41 countries: A perspective of routine activity theory. *International Journal of Bullying Prevention*, 1–13.

Louderback, E. R., & Antonaccio, O. (2020). New applications of self-control theory to computer-focused cyber deviance and victimization: A comparison of cognitive and behavioral measures of self-control and test of peer cyber deviance and gender as moderators. *Crime & Delinquency.*

Macaulay, P. J., Steer, O. L., & Betts, L. R. (2020). Factors leading to cyber victimization. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 1–25). Academic Press.

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2014). Exploration of the cyberbullyingvictim/offender overlap by sex. *American Journal of Criminal Justice, 39*(3), 538–548.

Milani, R., Caneppele, S., & Burkhardt, C. (2020). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behavior,* 1–13.

Miró-Llinares, F., Drew, J., & Townsley, M. (2020). Understanding target suitability in cyberspace: An international comparison of cyber victimization processes. *International Journal of Cyber Criminology, 14*(1), 139–155.

Mitchell, K. J., Finkelhor, D., Wolak, J., Ybarra, M. L., & Turner, H. (2011). Youth internet victimization in a broader victimization context. *Journal of Adolescent Health, 48*(2), 128–134.

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

Nilsson, A., & Estrada, F. (2003). Victimization, inequality and welfare during an economic recession: A study of self-reported victimization in sweden 1988â€“99. *British Journal of Criminology, 43*(4), 655–672.

Notten, N., & Nikken, P. (2016). Boys and girls taking risks online: A gendered perspective on social context and adolescents' risky online behavior. *New Media & Society, 18*(6), 966–988.

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.

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, 17*(4), 418–432.

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies, 8*(4), 298–309.

Reep-vanden Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*(1), 5.
Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216–238.
Reyns, B. W. (2017). Routine activity theory and cybercrime: A theoretical appraisal and literature review. *Technocrime and criminological theory* (pp. 35–54) Routledge.
Reyns, B. W., & Fisher, B. S. (2018). The relationship between offline and online stalking victimization: A gender-specific analysis. *Violence and Victims, 33*(4), 769–786.
Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology, 60*(10), 1119–1139.
Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149–1169.
Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice, 32*(2), 148–168.
Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice, 44*(1), 63–82.
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.
Sargent, K. S., Krauss, A., Jouriles, E. N., & McDonald, R. (2016). Cyber victimization, psychological intimate partner violence, and problematic mental health outcomes among first-year college students. *Cyberpsychology, Behavior, and Social Networking, 19*(9), 545–550.
Statistics Finland. (2018). Use of information and communications technology by individuals. http://www.stat.fi/til/sutivi/2018/sutivi_2018_2018-12-04_tie_001_en.html. Accessed 10th of March 2020.
Sumter, S. R., Baumgartner, S. E., Valkenburg, P. M., & Peter, J. (2012). Developmental trajectories of peer victimization: Off-line and online experiences during adolescence. *Journal of Adolescent Health, 50*(6), 607–613.
Thacher, D. (2004). The rich get richer and the poor get robbed: Inequality in US criminal victimization, 1974â€“2000. *Journal of Quantitative Criminology, 20*(2), 89–116.
Tilley, N., Tseloni, A., & Farrell, G. (2011). Income disparities of burglary risk: Security availability during the crime drop. *The British Journal of Criminology, 51*(2), 296–313.
Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior, 26*(3), 277–287.
Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115–127.
Van Wilsem, J. (2013). Hacking and harassment—Do they have something in common? comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437–453.
Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323–338.
Wachs, S., Michelsen, A., Wright, M. F., Gámez-Guadix, M., Almendros, C., Kwon, Y., et al. (2020). A routine activity approach to understand cybergrooming victimization among adolescents from six countries. *Cyberpsychology, Behavior, and Social Networking, 23*(4), 218–224.
Wachs, S., Costello, M., Wright, M. F., Flora, K., Daskalou, V., Maziridou, E., ... & Hong, J. S. (2021). "DNT LET'EM H8 U!": Applying the routine activity framework to understand cyberhate victimization among adolescents across eight countries. *Computers & Education*, 160.
WeulenKranenbarg, M., 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.
White, C. M., Gummerum, M., Wood, S., & Hanoch, Y. (2017). Internet safety and the silver surfer: The relationship between gist reasoning and adults' risky online behavior. *Journal of Behavioral Decision Making, 30*(4), 819–827.
Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277–292.
Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior, 40*(9), 1119–1131.
Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society.* SAGE Publications Limited.

ZetterströmDahlqvist, H., & GillanderGådin, K. (2018). Online sexual victimization in youth: Predictors and cross-sectional associations with depressive symptoms. *European Journal of Public Health, 28*(6), 1018–1023.