Risk profiles for cybercrime victimization: a conjunctive analysis of case configurations

M. Susanne van 't Hoff-de Goede[1,2] m.s.vanthoff-degoede@hhs.nl

Asier Moneva[1,2] amoneva@nscr.nl

E. Rutger Leukfeldt[1,2] e.r.leukfeldt@hhs.nl

[1] Centre of Expertise Cyber Security, The Hague University of Applied Sciences

[2] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)

This is an Accepted Manuscript of an article published by Taylor & Francis in Deviant Behavior on April 11, 2025, available at: https://doi.org/10.1080/01639625.2025.2481917.

Abstract

It is crucial to understand who is at risk for cybercrime victimization. This study draws on longitudinal data from the Online Behavior and Victimization Study (N=1886) to establish high-risk victimization profiles for cybercrime in general, hacking, malware infection, and fraud. We use Conjunctive Analysis of Case Configurations (CACC) to identify 64 dominant profiles describing personal characteristics (e.g., age, self-control), routine activities (e.g., exposure) and actual self-protective online behavior (e.g., password management) in 1330 respondents. After noting that observations moderately and statistically significantly cluster around dominant profiles, we identify ten high-risk profiles associated with an 18-50 percent probability of cybercrime victimization within the next year. Examining contextual variability in profiles reveals that self-control is most associated with malware infection, and fraud victimization.

Keywords: online crime, victims, CACC, longitudinal, resilience

Introduction

With the ongoing digitization of our society, more and more people fall victim to online crimes. This is true for both ‘‘traditional’’ offences that are now also committed via the internet (i.e. cyber-enabled crimes, e.g., scams) and ‘‘new’’ offences in which information technology (IT) is both the tool and the target (i.e. cyber-dependent crimes, e.g., hacking) (McGuire and Dowling 2013). For example, the Netherlands' Safety Monitor, a nationally representative yearly survey with over 65.000 respondents, showed that in 2023, 16 percent of Dutch citizens aged 15 years old or older were victims of one or more forms of cybercrime (Statistics Netherlands 2024). The Australian Cybercrime Survey with 13,887 respondents showed that in 2023, 47 percent of Australian citizens aged 18 years or older experienced at least one type of cybercrime victimization in the previous year (Voce and Morgan 2023). In order to adequately make policy decisions aimed at reducing cybercrime victimization, it is of vital importance to understand who is at risk for cybercrime victimization.

To date, studies that have aimed to establish a risk profile for cybercrime victimization mostly focused on personal characteristics (e.g., gender, education), routine online activities (e.g., online banking, social media use) and self-protective behavior (e.g., using strong passwords, avoiding unsafe websites) and their relationship with the risk of online victimization. These studies found that very few personal characteristics or routine activities appear to be steadily associated with the risk of the various form of online victimization (Borwell et al. 2018; Leukfeldt and Yar 2016; Reep-van den Bergh and Junger 2018). Overall, these studies point to three specific risk factors for online victimization, namely age, self-control and time spent online (exposure) (e.g., Ahmad and Thurasamy 2022; Akdemir and Lawless 2020; Brady et al. 2016; Cheng et al. 2020; Guerra and Ingram 2020; Herrero et al. 2021; Holt et al. 2020; Jansen and Leukfeldt 2016; Lee and Wang 2022; Leukfeldt 2014; Marret and Choo 2017; Mikkola et al. 2020; Näsi et al. 2021; Ngo et al. 2020; Ngo and

Paternoster 2011; Reyns 2013; Van de Weijer and Leukfeldt 2017; Van Wilsem 2013a). Moreover, studies that tried to determine risk profiles based on self-protective online behavior found that self-protective and avoidance behavior decreased the odds of becoming a victim (Bergmann et al. 2018; Chen et al. 2017; Drew and Farrell 2018; Marret and Choo 2017; Mesch and Dodel 2018; Näsi et al. 2021).

While these studies took an important first step in establishing risk profiles for online victimization, they have methodological shortcomings that should be taken into account. For example, studies focusing on personal characteristics and routine activities rarely took self-protective online behavior into account simultaneously, making it difficult to compare findings and establish risk profiles. Moreover, studies focusing on self-protective online behavior mostly relied on self-reported behavior (Bergmann et al. 2018; Chen et al. 2017; Drew and Farrell 2018; Marret and Choo 2017; Mesch and Dodel 2018; Näsi et al. 2021; Partin et al. 2021), and this likely affected results since how people say they behave online is not necessarily how they actually behave online (Andrews et al. 2015; Ellis et al. 2019; Machuletz et al. 2017; Parry et al. 2021; Van der Kleij et al. 2021; Van de Weijer et al. 2018; Van 't Hoff-de Goede et al. 2019; Wilcockson et al. 2018). The few studies that measured actual self-protective online behavior mostly used small samples (Levesque et al. 2014; Lévesque et al. 2018) or used machine features as proxies for behavior (Ovelgönne et al. 2017). Moreover, the relationship between factors like personal characteristics, routine activities and self-protective online behavior and victimization has almost exclusively been studied retrospectively. These methodological shortcomings make it unclear what factors may constitute a risk profile for online victimization.

We recently did a study into the relationship between personal characteristics, online routine activities, actual self-protective online behavior and future cybercrime victimization (Van 't Hoff-de

Goede et al. 2023). In this paper, we used regression analysis, a common method in the field. We concluded that the field is in need of new and innovative ways to look at cybercrime victimization and the current paper aims to do just that. In the current paper, an alternative method will be introduced to cybercrime studies: the Conjunctive Analysis of Case Configurations (CACC) (Miethe, Hart and Regoeczi 2008).

As opposed to variable-oriented methods like correlations and regressions, CACC adopts a case-oriented strategy to identify relevant subsets of observations (e.g., respondents) with shared characteristics and study them in depth. The unit of analysis becomes the case, configured by a set of theoretically relevant variables (Miethe et al. 2008). In the case of cybercrime victimization, these variables may be, for example, sociodemographic, behavioral, or situational (Moneva, Hart and Miro-Llinares 2020; Paez and Hart 2022). The comparative case approach allows to understand which combinations of variables are simultaneously related to an outcome of interest, with different or even contradictory combinations of factors being possible, which more accurately reflects the underlying complexity of social phenomena such as cybercrime victimization than variable-oriented methods (Hart, Moneva and Esteve 2023; Ragin 2013). Since most cybercrime research has been conducted with variable-oriented methods, using the alternative approach of CACC has the potential to advance the field by revealing new patterns in the data or making existing findings more robust by corroborating them. Prior studies have applied CACC to examine various social issues across various cyber contexts, including online harassment among Spanish students, where distinct situational profiles of repeat victims and offenders were identified (Moneva, Miro-Llinares and Hart 2021), and cyberbullying victimization patterns in youth from the United States, revealing the interplay between traditional bullying and cyber victimization (Paez and Hart 2022). CACC has also been used to examine intimate partner stalking among college students, demonstrating how situational factors

influence police reporting (Augustyn, Rennison, Pinchevsky and Magnuson 2019), and to investigate disclosures of child sexual abuse within the #MeTooInceste movement on Twitter, identifying key tweet characteristics linked to victimization testimonies (Aguerri, Molnar and Miro-Llinares 2023). These applications highlight the versatility of CACC in understanding the complex interactions between individual, situational, and contextual factors in cyber-related crimes.

The second way the current study aims to move the field further is by using data from the Online Behavior and Victimization Study (N=1886), in which a population-based survey experiment was conducted. This allowed us to gather data on actual self-protective online behavior of a large group of respondents. The term ‘‘actual’’ highlights the difference between the measurements this study used for online behavior versus the measurements that are almost exclusively used in previous studies: self-reported behavior. It was observed, for example, how respondents handled a pop-up requesting a software download and the online disclosure of personal information in (simulated) cyber risk situations (Van ’t Hoff-de Goede et al. 2020). Moreover, based on an extensive literature study, measurements were incorporated for numerous explanatory factors, including a broad range of personal characteristics and routine activities. Thirdly, data collection occurred in two waves, with the second wave occurring one year after the first. This longitudinal design allowed us to study the relationship between personal characteristics, routine activities and actual self-protective online behavior (wave 1) and online victimization (wave 2) over time.

Literature Review on Risk Profiles for Cybercrime Victimization

Previous studies on cybercrime victimization have aimed to establish risk profiles for cybercrime victimization. These studies have drawn upon Routine Activities Theory, which suggests that cybercrime, like traditional crime, occurs when a motivated offender encounters a suitable target in

absence of a capable guardian (Cohen and Felson 1979). Within the domain of cybercrime research, the notion of a suitable target has predominantly been explored in three domains: personal characteristics, routine activities and self-protective online behavior.

Personal Characteristics as Risk Factors for Cybercrime Victimization

The literature on the relationship between personal characteristics and cybercrime victimization points towards two factors that seem to be related to an increased risk of cybercrime victimization. The first factor that the literature suggests is related to cybercrime victimization is age. Most studies examining the relationship between age and victimization indicate that the older people are, the more likely they become victims of cybercrime (Holt et al. 2020; Ngo et al. 2020; Ngo and Paternoster 2011; Sheng et al. 2010; Van de Weijer and Leukfeldt 2017; Van Wilsem 2013a). However, there are also studies that found an opposite relationship (Näsi et al. 2021) or no association between age and online victimization, for example, for online fraud, scams and malware (Bossler and Holt 2009, 2010; Leukfeldt and Yar 2016; Mesch and Dodel 2018; Näsi et al. 2021; Parry et al. 2021). These inconsistent finding may partly be the consequence of differences in research samples and statistical methods that were used. It has furthermore been difficult to establish risk factors for cybercrime victimization based on age, since other factors like routine activities are not equally distributed between age groups, e.g., young internet users use the internet more often for social media than older internet users (Büchi et al. 2016; Ngo et al. 2020).

Secondly, self-control theory states that low self-control is associated with impulsive behaviors, a focus on the short term, poor decision-making and a disregard for potential risks (Gottfredson and Hirschi 1990), which may increase the likelihood of engaging in risky online activities and could increase their risk to be victims of cybercrime (Ngo and Paternoster 2011).

Findings from previous studies on the relationship between self-control and cybercrime victimization consistently suggest that individuals with low self-control are more susceptible to cybercrimes and more often become cybercrime victims (Herrero et al. 2021; Holt et al. 2020; Louderback and Antonaccio 2020; Mesch and Dodel 2018; Mikkola et al. 2020; Partin et al. 2021; Reyns et al. 2018). It is unclear, however, if the relationship between self-control and cybercrime victimization is direct or that it works through unsafe online behavior. For example, the association could be mediated through online behavior (Partin et al. 2021) or routine activities (Mikkola et al. 2020). Moreover, to our knowledge, there is a lack of studies that focus on self-control and situational context factors like routine activities and self-protective behavior simultaneously.

Currently, there is no consensus on the relationships between other personal characteristics and cybercrime victimization (Borwell et al. 2018; Reep-van den Bergh and Junger 2018). For example, contradicting results have been found for the relationship between gender and cybercrime victimization, that suggest that both men (Bergmann et al. 2018; Bossler and Holt 2010; Näsi et al. 2021; Reyns 2013; Van de Weijer and Leukfeldt 2017) and women (Anderson 2006; Bossler and Holt 2009, 2010; Holt and Bossler 2013; Sheng et al. 2010) are likely to be victims, or that no difference based on gender has been found (Holt et al. 2020; Louderback and Antonaccio 2020; Mesch and Dodel 2018; Ngo and Paternoster 2011; Van Wilsem 2013a, 2013b; Williams 2016).

Routine Activities as Risk Factors for Cybercrime Victimization

Other studies have focused on the relationship between routine activities and the risk of cybercrime victimization. We define routine activities as the amount of time people spend online and the type of activities they do online (e.g., online shopping, gaming). The assumption is that certain routine online activities can make potential victims visible to criminals (Cohen and Felson 1979). Indeed, studies

have found a link between victimization and the amount of time spent online. This is what is called exposure (i.e. being online longer, e.g., untargeted surfing, watching videos and using social media) and this appear to be positively related to victimization (Bergmann et al. 2018; Cheng et al. 2020; Guerra and Ingram 2020; Herrero et al. 2021; Holt et al. 2020; Mikkola et al. 2020; Näsi et al. 2021; Reyns et al. 2016, 2018; Sharif et al. 2018; Van Wilsem 2013b; Williams 2016). Moreover, the fact that young people are more likely to become victims may even be partly explained by the fact that they are online more often (Büchi et al. 2016; Ngo et al. 2020).

However, evidence for other relationships between routine online activities and the likelihood of cybercrimes victimization is inconclusive (Ahmad and Thurasamy 2022). While some studies suggest that certain online routine activities, including online shopping, gaming, internet banking, and social media use, are related to an increased risk of cybercrime victimization (Chen et al. 2017; Choi 2008; Holt et al. 2020; Leukfeldt and Yar 2016; Ngo et al. 2020; Ovelgönne et al. 2017; Reyns 2013; Van Wilsem 2013a; Williams 2016), other studies did not find routine activities to be associated with cybercrime victimization (Bossler and Holt 2009; Holt and Bossler 2013; Leukfeldt 2014; Mesch and Dodel 2018). The fact that there is no consensus on how to measure routine activities makes it difficult to compare findings (Ahmad and Thurasamy 2022). For example, not all studies take into account the timing of the routine activities versus victimization (was the anti-virus installed before or after victimization?). Moreover, exposure has often been operationalized at time spent online, but studies vary between what constitutes high exposure. Furthermore, the causality of the possible relationship between routine activities and cybercrime victimization is unclear because most studies measure both at the same point in time. Three longitudinal studies suggest that relationships found by other studies between routine activities and cybercrime victimization decreased or disappeared when using longitudinal data (Guerra and Ingram 2020; Van de Weijer 2019; Van 't Hoff-de Goede et al.

2023). Possibly, these former associations were caused by unobserved factors (Van de Weijer 2019) or the direction of the relationship might be reverse, meaning that online victimization may change routine activities instead of the other way around (Guerra and Ingram 2020).

Insufficient Self-protective Online Behavior as a Risk Factor for Cybercrime Victimization

Findings from previous studies mostly suggest that self-protective behavior, like using strong passwords and avoiding clicking on unsafe hyperlinks, decreased the odds of becoming a cybercrime victim (Bergmann et al. 2018; Chen et al. 2017; Drew and Farrell 2018; Marret and Choo 2017; Näsi et al. 2021). Moreover, risky online behavior seems to increase the odds of being a cybercrime victim (Akdemir and Lawless 2020; Mesch and Dodel 2018; Ngo et al. 2020; Partin et al. 2021). However, since most studies use cross-sectional data the causal relationship is unclear. Moreover, other studies found a reverse relationship that suggests that self-protective online behavior was related to an increased risk of cybercrime victimization, meaning that people show more self-protective online behavior after victimization (Ngo et al. 2020; Reyns et al. 2016; Williams 2016). These inconclusive findings might stem from the lack of prospective, longitudinal research on this relationship. Moreover, studies that have claimed that self-protective behavior decreases the odds of cybercrime victimization almost exclusively used self-reported data (Bergmann et al. 2018; Chen et al. 2017; Drew and Farrell 2018; Marret and Choo 2017; Mesch and Dodel 2018; Näsi et al. 2021; Partin et al. 2021). This only illustrates that on average, people who say that they have not been victimized by cybercrime more often claim that they behave in a self-protective manner online. This relationship, however, may also be explained by confounders, such as social desirability. It has been found that what people say they do online often differs from what they actually do online (Andrews et al. 2015; Ellis et al. 2019; Machuletz et al. 2017; Parry et al. 2021; Wilcockson et al. 2018). Thus, conclusions

about the supposed relationship between self-reported behavior and cybercrime victimization should be carefully interpreted and might not apply to the relationship between actual self-protective online behavior cybercrime victimization.

Very few have studies have researched the association between actual self-protective online behavior and cybercrime victimization (Parry et al. 2021). Available studies suggest that unsafe online behavior can directly contribute to an increased risk of victimization. In their study, Sharif et al. (2018) examined the logged online behavior of more than 20,000 participants over a period of three months. The researchers compared participants who had been exposed to malware or phishing URLs during that time frame to those who had not. The findings showed that the exposed participants tended to spend more time online and engage in more frequent internet browsing, particularly during nighttime hours. Interestingly, while certain self-reported behaviors were indicative of exposure, the accuracy of these self-reports was notably lower compared to the actual behavioral data (Sharif et al. 2018). Using a different approach, researchers who collected real-usage data among 50 subjects concluded that behavior such as visiting many different websites, downloading many applications and files (particularly .exe), contacting more different hosts and using peer-to-peer networks is related to an increased risk for malware victimization (Levesque et al. 2014; Lévesque et al. 2018). Finally, using seven machine features (e.g., the number of networks that devices have connected and the number of downloads) as proxies for actual self-protective online behavior on 1.6 million machines, Ovelgönne et al. (2017) found that all seven machine features were positively related to the odds of malware victimization. Currently, to our knowledge, no studies are available that have focused on actual self-protective behavior and factors such as personal characteristics and routine activities simultaneously.

Summarizing, the current literature points to several potential risk factors for cybercrime victimization. These include personal characteristics such as age and self-control, the routine activity of ''exposure'', and self-protective online behavior. Previous studies have examined these factors as separate risk factors. By moving away from a variable-oriented approach and incorporating Conjunctive Analysis of Case Configurations (CACC), the current study aims to reveal risk profiles based on combinations of these risk factors.

Current Study

Examining heterogeneity in risk factors and victimization is essential in addressing cybercrime, as a particular risk factor may not consistently result in the same type of victimization (Lee and Wang 2022; Leukfeldt and Yar 2016; Näsi et al. 2021; Ngo et al. 2020; Reyns et al. 2018). For instance, hacking victimization can stem from various factors such as sharing personal information, downloading malware, or the use of weak passwords. Moreover, malware victimization may occur after clicking on suspicious links or attachments or be related to a lack of regular software updates. By solely concentrating on a single cybercrime (e.g., Holt et al. 2020; Lee et al. 2022; Reyns 2013; Williams 2016), we would overlook the intricate connections between risk factors and the diverse range of cybercrimes. The current paper aims to answer the following research question: What are the risk profiles for cybercrime victimization in general, and for specific prevalent cybercrimes such as hacking, malware, and online fraud?

In answering this question, we aim to assess which contexts—defined by the combination of certain risk factors—are associated with a greater probability of cybercrime victimization the following year. This contextual approach focuses on identifying patterns and configurations of risk factors associated with different types of cybercrime.

Method

Research Instrument

A research instrument was developed using a population-based survey experiment to measure actual self-protective online behavior along with the explanatory factors identified in the literature (Van 't Hoff-de Goede et al. 2019 2020). This instrument, implemented as part of the Online Behavior and Victimization Study, combines the benefits of questionnaire research and experimental design. While completing the survey that included Likert scale and multiple-choice questions, participants were unaware that their responses to fictional online risk situations that occurred throughout the survey were being recorded. The instrument, which included a detailed debriefing, underwent ethical review and approval by the ethical committee of the VU University in Amsterdam, The Netherlands. (For more detailed information about the instrument, see Van 't Hoff-de Goede et al. 2020).

Respondents

During the first wave in 2019, 12,114 Dutch citizens were invited by a panel agency to complete the survey in exchange for reward points. A total of 2,426 respondents filled out the respondents fully and within the allotted time frame (20%).[1] The personal characteristics of the 2,426 respondents were compared with the Dutch population in the same year (Statistics Netherlands 2019). Respondents were representative of Dutch society with respect to gender, employment status and the province in which they lived. However, respondents had more often completed a high level of education than was average in the Netherlands (50% versus 30%). Respondents are also less often younger than 39 years, compared to the Dutch population (13.8% versus 29.4%). A year later, in 2020, the second wave of

[1] See Van 't Hoff-de Goede et al. 2019 for a more detailed description of the response and selection of respondents.

data collection took place and a total of 1886 respondents (77.7%) from wave 1 participated again. Respondents who participated during wave 2 were compared with those who dropped out, and it was found that respondents who participated in wave 2 were more often male (56.5% versus 42.8%, X^2=31.87, p<.001) and older (58.8 versus 54.5 years old, t=201.51, p<.001) and that recent victims were less likely to participate in wave 2 (12.8% versus 16.3%, X^2=4.29, p<.05), but lifetime victimization of a cybercrime did not significantly differ between respondents and non-respondents of wave 2. Moreover, no significant differences were found with respect to most actual self-protective online behaviors measured in wave 1, educational background or cohabiting with a partner (yes/no).[2]

Operationalization

One of the advantages of the CACC is that it allows the identification of patterns in the data by aggregating identical profiles (e.g., Miethe et al. 2008). The number of identical profiles aggregated depends on how the variables are operationalized, since the more variability in the data, the less likely it is to observe identical profiles. This happens because increased variability leads to a greater number of profiles, and the more profiles, the less likely it is that identical profiles are observed. This in turn leads to identifying insignificant profiles in the data. Thus, interpretation of the results becomes increasingly difficult. It is therefore important to find an appropriate balance of variability when using CACC to gain insight from the data. The operationalization of variables for a CACC is often arbitrary, as researchers must set cut-off points on, for example, variables that are continuous, or merge categories together. The justification for these cut-off points is usually based on expert judgment or on the statistical distribution of variables. A rule of thumb when operationalizing the variables to

[2] See Van 't Hoff-de Goede et al. 2019 for a more detailed comparison between respondents who took part in wave 2 versus respondents who dropped out after wave 1.

define profiles is that the number of observable profiles should not exceed the number of observations in the data because it could lead to "incorrect conclusions about dominant case configurations and/or situational clustering" (Hart et al. 2023, p. 5). Our operationalization process is described below.

Wave 1 (Independent Variables)

The *age* of the respondents was provided by the panel agency and categorized into three groups: 18-39 years old, 40-64 years old and 65 years and older. *Self-control* was measured with the Brief Self-Control Scale (BSCS), that for example measures discipline and impulse control (Tangney, Baumeister, and Boone 2004). The BSCS exists of thirteen items rated on a 5-point Likert scale (1 = not at all like me, 5 = very much like me). An example of an item is: "I am good at resisting temptation". On this scale, the mean self-control of the respondents was 3.5954 (SD = 0.5899). We considered self-control *high* when it was above the mean plus one standard deviation (> 4.1852), *low* when it was below the mean minus one standard deviation (< 3.0055), and *medium* in all other cases. To measure *exposure*, respondents were asked how often they use the internet *in their own time*: less than once a month, a minimum of once a month but not weekly, a minimum of once a week but not daily, daily, multiple times a day, at least every hour (during the hours that I am awake), I am (almost) constantly online (during the hours that I am awake). Due to the distribution of the variable, it was dichotomized as "once a day or less" (39.2%) and "more than once a day" (60.8%).

Actual Self-protective Online Behavior. In the current study, four types of actual self-protective online behaviors were measured. *Password strength* was measured by asking respondents to create a user account to take part in the survey. Respondents were shown the following message: "In accordance with data protection legislation, we ask you to first create a temporary user account. For the purposes of this study, some personal information will be stored in this account. You will

need this account once again at the end of the questionnaire. Enter a username and password below." The strength of the password, or entropy[3], was measured based on the length of the passwords and the type of characters used by respondents in their password (lowercase, uppercase, numbers, special characters.[4] Since the scores were right skewed, with more respondents with a low entropy than a high entropy, we transformed the variable to be more normally distributed by applying a square root transformation. The independent variable ''password strength'' is therefore the square root of this entropy. We then dichotomized entropy as *low* when it was below 48 (67.9%) and *high* when it was 48 or more (32.1%). The independent variable ''*downloading software*'' concerns the choice that respondents made when a pop-up appeared during the survey that asked them to download (fictional) software from an unknown source. This occurred when respondents were asked to watch a video as part of the survey, but the video could not be played on their device without the additional software (for more details, see (Van 't Hoff-de Goede et al. 2020). Respondents showed self-protective behavior if they clicked ''no'' or did not click anything on the pop-up but clicked on ''continue to the next question'' (58.3%). They made an unsafe choice if they clicked ''yes'' on the pop-up (41.7%). The independent variable ''*clicking on phishing hyperlink"* measured whether respondents show self-protective behavior when encountered with hyperlinks in emails. This was measured using role-play (Downs et al. 2007); respondents were asked to pretend to be a certain fictional person, with a gender neutral first name and a generic last name. They were shown three emails that this person had received: two phishing emails, in which real phishing emails were adapted by the researchers, supposedly from a bank and a festival organization, and one legitimate email from an internet

[3] The entropy expresses how many passwords could be made with the chosen combination of length and complexity. The higher the entropy of a password, the harder it is to hack/crack.
[4] The correlation between the length and the entropy of the password was r-.99 (P<.001), which indicates that the entropy in this dataset was mainly based on password length rather than on the type of characters.

provider. Respondents were told that the researchers wanted to study how people handle the e-mails they receive and asked what they would do if they were the fictional person and had received this email (e.g., nothing, delete, click on link etc.). Respondents showed self-protective behavior if they did not open either (fictional) phishing link (79.4%) and behaved unsafely if they reported opening the linked website from one or both phishing emails (20.6%). The independent variable ''*sharing personal information"* measures whether respondents disclosed personal information. At the end of the questionnaire, respondents were asked to enter seven types of personal information, namely their full name, email address, email address of a relative of acquaintance, date of birth, zip code, house number and the last three digits of their bank account. For each type of personal information, the respondents had the option to click on a button that said "I'd rather not say". Respondents showed self-protective behavior if they did not share any type of personal information (49%) and made an unsafe choice if they entered any personal information (51%). In line with privacy legislation, it was only recorded *if* respondents entered personal information, not *what* they entered, and thus the researchers do not have access to the respondents' answers.

Wave 2 (Dependent Variable)

Cybercrime Victimization. Respondents were asked in the second wave of data collection if they had become victim of a number of different cybercrimes in the previous year. Cybercrime victimization thus refers to victimization that occurred in the year between waves 1 and 2. Respondents were asked if they had become a victim of the following cybercrimes, for which respondents were provided with definitions and/or examples: shopping fraud, identity fraud, advance-fee fraud, friend-in-need fraud, malware on their device (PC/laptop/smartphone/tablet) and being denied access to their files (e.g., ransomware). The first four of these cybercrimes together constitute "victimization of online fraud"

and the last two of these cybercrimes constitute "victimization of ransomware". Moreover, respondents were a victim of hacking if they indicated that, without their permission, someone had broken into their computer, destroyed/changed/stole data, changed their website or profile page, logged in on their email account and/or gained access to their online account(s). Finally, respondents were asked if they had become a victim of phishing or an unlisted type of cybercrime. If respondents indicated being victimized by at least one of these cybercrimes, this constitutes "general cybercrime victimization".

Analytic Strategy

To identify the profiles of the respondents most at risk of cybercrime victimization, we conducted Conjunctive Analysis of Case Configurations (CACC) (Miethe et al. 2008; Hart et al. 2023). CACC is a mixed method for multivariate analysis of categorical data that constitutes an alternative to traditional variable-oriented analysis techniques like regression (for a discussion, see Ragin 2013). This allows us to examine cybercrime victimization from a different methodological angle. CACC has been used to examine the situations in which cybercrime occurs and the profiles of the people involved (e.g., Moneva, Miró-Llinares and Hart 2021; Paez and Hart 2021). In our case, CACC allows us to identify the dominant—and theoretically relevant—profiles or case configurations associated with a high risk of cybercrime victimization based on risky behaviors carried out by respondents. Since the sample contains more than 1000 observations, the dominant profiles are those that are observed at least 10 times (Hart 2014). We define high risk as the one that deviates at least 2 standard deviations from the mean risk of victimization, measured probabilistically ("Prob." in the results tables) by the ratio of cases that ended in victimization to the total (Hart and Moneva 2018). We conduct four CACC: one to examine the risk of general cyber victimization, three more for specific

victimization risks: hacking, malware, and fraud. This allows us to compare the combinations of factors that shape the risk of victimization across different types of cybercrime.

We complement these analyses by computing two statistical tests to identify whether and to what extent cybercrime victimization clusters among dominant profiles: a Chi-Square Goodness-of-Fit, and a Situational Clustering Index (SCI) (Hart 2019). In addition, we examine the contextual variability of the dominant profiles to determine and compare the effect that specific variable values have on general and specific victimization outcomes (Hart, Rennison and Miethe 2017). To do this, we match identical profiles except for the variable value of interest (e.g., low self-control) and calculate the difference in the probability of victimization with respect to the other variable values (e.g., medium and high self-control). The result is a set of numeric main effects whose distribution can be examined. Depending on whether the distribution is above or below zero, the value of that variable can be interpreted as having a positive or negative effect.

All analyses are carried out with the cacc R package version 0.1.0 (Moneva, Esteve and Hart 2022), assisted by the tidyverse (Wickham et al. 2019), in RStudio version 2022.07.1 (RStudio Team 2022) and R version 4.2.0 (R Core Team 2022).

Results

Table 1 describes the descriptive statistics for all independent and dependent variables. Most respondents are from the age group 40-64 (48.7%) or older (39.8%). Most respondents had a medium level of self-control (66.4%), were frequently online (60.8%), used a weak password (67.9%), declined to download the malicious software (58.3%), indicated they would not click on the phishing link (79.4%) and shared one or more types of personal information (51%) in the simulated risky

scenario's. Victimization of any type of cybercrime in the last year occurred among 24 percent of the respondents, specifically hacking (4.5%), malware (12.1%) and fraud (6.6%).

Table 1. Frequency distribution of independent and dependent variables (N=1886)

Variable	**Categories**	**%**	**(N)**
Independent (wave 1)			
Age	18-39	11.5	(217)
	40-64	48.7	(919)
	65+	39.8	(750)
Self-control	Low	16.9	(319)
	Medium	66.4	(1253)
	High	16.6	(314)
Exposure	Occasional	39.2	(739)
	Frequent	60.8	(1147)
Password strength	Low	67.9	(1280)
	High	32.1	(606)
Downloading software	Yes	41.7	(786)
	No	58.3	(1100)
Clicking on phishing hyperlink	Yes	20.6	(388)
	No	79.4	(1498)
Sharing personal information	Yes	51.0	(962)
	No	49.0	(924)
Dependent (wave 2)			
Victimization in last year	Yes, any type of cybercrime	24.0	(452)
	Yes, hacking	4.5	(84)
	Yes, malware	12.1	(229)
	Yes, fraud	6.6	(124)

The CACC results reveal 64 dominant profiles containing a total of 1330 respondents, with a mean of 20.8 respondents per profile (*SD* = 12.6). Respondents (observations) cluster weakly to moderately around profiles (*SCI* = 0.307) in a statistically significant way [$X^2(63) = 483.654$, $p < 0.001$]. Figure 1 displays these results visually. The overall risk of cyber victimization associated with

the profiles ranges from a minimum probability of 0.1 to a maximum of 0.5 (M = 0.2; SD = 0.1). The next sections present the results for the dominant victimization profiles identified in the data as those with a particularly high risk of victimization relative to the rest. Tables present only the profiles that reached the cutoff point above 2 SD.

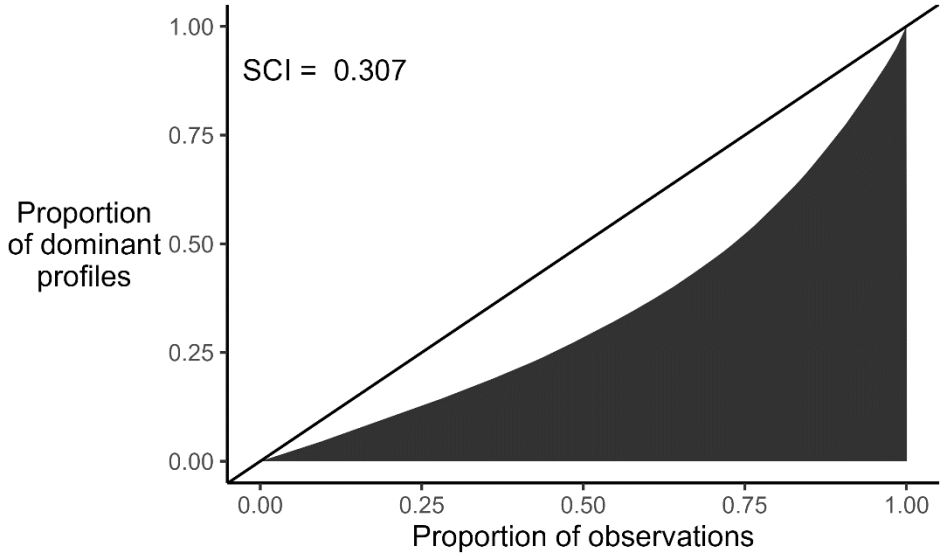

Figure 1. Lorenz curve of the clustering magnitude between the proportion of observations and the proportion of dominant profiles

Risk of General Cybercrime Victimization

Table 2 displays a single high-risk profile for general cybercrime victimization. It highlights the personal and behavioral characteristics of 12 participants, 50% of which were victimized within a year. These participants were middle-aged, had moderate self-control, used the Internet more than once a day, had a weak password, downloaded software, clicked on a phishing hyperlink and shared personal information.

Table 2. High-risk profile for general cyber victimization

ID	Age	Self-control	Exposure	Password strength	Downl. software	Clicked phishing hyperlink	Shared personal info.	Freq.	Prob.
g1	40-64	medium	frequent	low	yes	yes	yes	12	0.5

Risk of Specific Cybercrime Victimization

We then examine the high-risk victimization profiles for each of the three types of cybercrime: hacking, malware, and fraud. Table 3 shows the 4 high-risk profiles identified for hacking victimization. In these profiles the risk of victimization ranges from 18.2% to 25%. All 44 participants in these profiles had a weak password and downloaded software, and 9 of them were hacked the following year. There were 503 participants in 28 profiles with zero risk of hacking victimization. The remaining 783 participants in 32 profiles had a victimization risk between 1.5% and 16.6%.

Table 4 shows the 2 high-risk profiles identified for malware victimization. In these profiles the risk of victimization ranges from 29.4% to 33.3%. The 29 participants comprising these profiles were middle-aged, had an intermediate level of self-control, downloaded software and shared their personal information. One year later, 9 of them reported that they had been infected by malware. There were 119 participants in 9 profiles with zero risk of victimization. The remaining 1182 participants in 53 profiles had a victimization risk between 4% and 27.3%.

Table 5 shows the 3 high-risk profiles identified for fraud victimization. In these profiles the risk of victimization ranges from 23.1% to 26.7%. Out of 45 participants comprising these profiles, 11 were scammed within one year despite exhibiting self-protective behavior concerning phishing hyperlinks. They were over 40 years old and exhibited intermediate or low self-control. There were 385 participants in 24 profiles with zero risk of victimization. The remaining 900 participants in 37 profiles had a victimization risk between 3.3% and 20%.

Table 3. High-risk profiles for hacking victimization

ID	Age	Self-control	Exposure	Password strength	Downl. software	Clicked phishing hyperlink	Shared personal info.	Freq.	Prob.
h1	40-64	medium	frequent	low	yes	yes	yes	12	0.250
h2	65+	medium	occasional	low	yes	yes	yes	10	0.200
h3	40-64	high	occasional	low	yes	no	no	11	0.182
h4	18-39	medium	frequent	low	yes	no	no	11	0.182

Table 4. High-risk profiles for malware victimization

ID	Age	Self-control	Exposure	Password strength	Downl. software	Clicked phishing hyperlink	Shared personal info.	Freq.	Prob.
m1	40-64	medium	frequent	low	yes	yes	yes	12	0.333
m2	40-64	medium	occasional	high	yes	no	yes	17	0.294

Table 5. High-risk profiles for fraud victimization

ID	Age	Self-control	Exposure	Password strength	Downl. software	Clicked phishing hyperlink	Shared personal info.	Freq.	Prob.
f1	65+	medium	occasional	high	no	no	no	15	0.267
f2	40-64	low	frequent	low	yes	no	no	17	0.235
f3	40-64	low	occasional	low	yes	no	yes	13	0.231

Main Effects

In order to answer the research question, the main effects of each variable value on general and specific types of cybervictimization calculated on the dominant profiles are shown in Figure 2. For

each type of cybercrime, the distribution of the variable values shows the direction and magnitude of their main effect on the risk of cybercrime victimization in the following year, as the boxplots largely cross the threshold marked by 0 towards positive values. The boxplots also rank the variable effects, based on their median, from the most positive to the most negative. For example, it appears that low self-control is related to a higher probability of cybercrime victimization the following year for general, malware, and fraud victimization. In the case of hacking, the association does not seem so clear.

Analysis of main effects on general victimization (a) reveal that low self-control is most strongly associated with an increased likelihood of victimization (M = 0.079; SD = 0.121), followed by sharing personal information (M = 0.057; SD = 0.149), and having a weak password (M = 0.045; SD = 0.164). Except for some atypical profiles, downloading software (M = 0.014; SD = 0.14) and frequent Internet use (M = -0.036; SD = 0.139) do not seem to be associated to a higher chance of victimization. Main effects on hacking victimization (b) show that — despite atypical cases — clicking on a phishing hyperlink is the strongest association (M = 0.059; SD = 0.071), followed by downloading software (M = 0.037; SD = 0.09) and having a weak password (M = 0.012; SD = 0.054). Again, frequent Internet use is not associated with an increased risk of hacking victimization (M = -0.019; SD = 0.081). In the case of malware victimization (c), main effects indicate that low self-control is almost always positively related to the probability of victimization (M = 0.061; SD = 0.063), while the rest of the variables show no clear relationships. Frequent exposure remains the variable least associated with the probability of victimization (M = -0.029; SD = 0.133). Main effects on fraud victimization (d) rank again low self-control as the most important association with victimization (M = 0.068; SD = 0.099), followed by sharing personal information (M = 0.03; SD = 0.069). Being older

than 65 years does not seem to be substantially associated with a higher risk of victimization except for two profiles in which the risk increases sharply (M = -0.008; SD = 0.093).

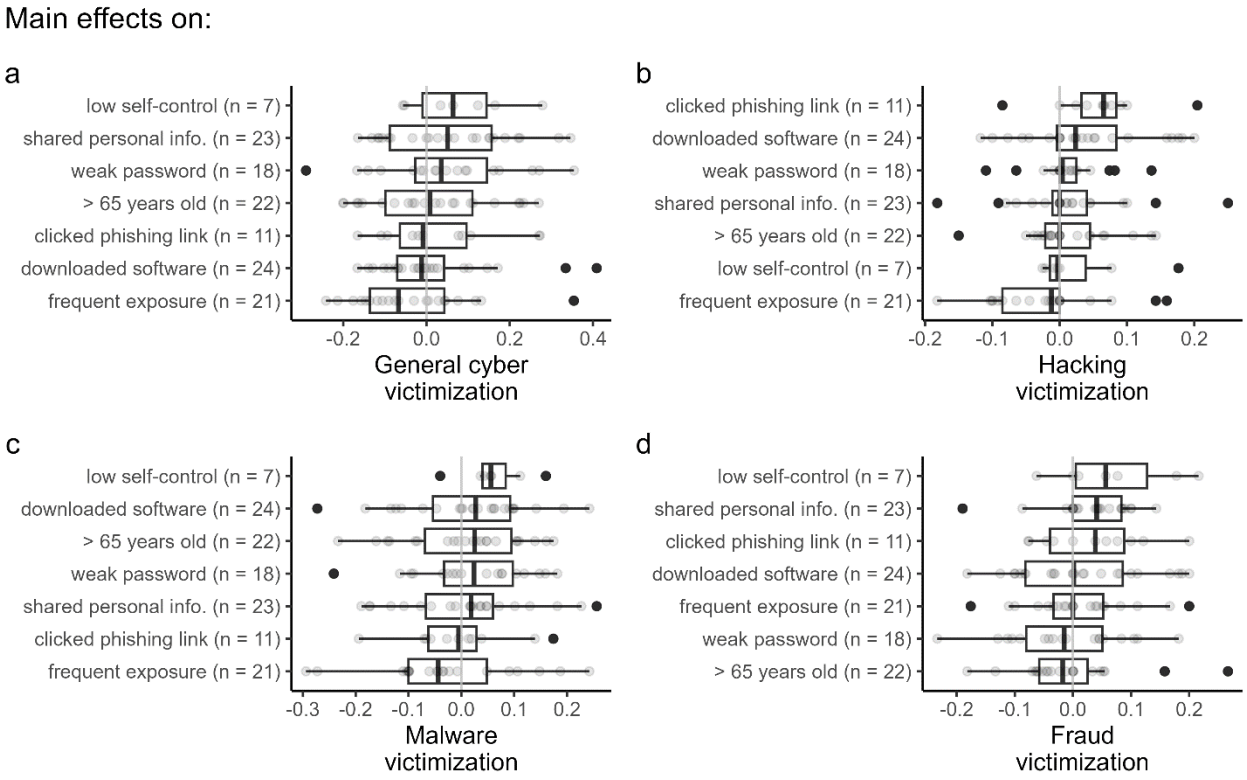

Figure 2. Main effects of seven routine activity variables on general and specific types of cyber victimization. The transparent dots represent individual data points for each contextual comparison per variable (the 'n'), while the solid dots highlight, among them, outliers in the victimization distribution that go beyond 1.5 times the interquartile range of the boxes.

Discussion

This study examined risk profiles for cybercrime victimization in an alternative way to provide a new perspective on the field. Using CACC, we examined the combined relationships of a range of variables to establish risk profiles for cybercrime victimization. Since most cybercrime research in

criminology has been conducted with variable-oriented methods, using the alternative approach of CACC advances the field by revealing new risk profiles (e.g., Moneva, Miró-Llinares and Hart 2021; Paez and Hart 2021). Longitudinal data from the Online Behavior and Victimization Study was used, that was gathered using a population-based survey experiment and included measurements of actual online self-protective behavior. Using longitudinal data allows researchers to go beyond mere cross-sectional associations of variables and makes it possible to research the longitudinal relationship between explanatory factors such as routine activities and self-protective behavior and cybercrime victimization (Leukfeldt 2017; Ngo et al. 2020; Reyns et al. 2016; Williams 2016). The great benefit of measuring actual online self-protective behaviors is avoiding the bias between what people say they do online and what they actually do online (Andrews et al. 2015; Ellis et al. 2019; Machuletz et al. 2017; Parry et al. 2021; Wilcockson et al. 2018).

Results point to the unique insights gained when using CACC for examining risk profiles for cybercrime victimization. For example, a risk profile was found with a 50 percent risk of cybercrime victimization in the following year. The main significant risk factors for general cybercrime victimization were low self-control, using a weak password and sharing personal information. Although the specific characteristics of this risk profile should be interpreted carefully, it does signify that using the CACC method on longitudinal data over different samples could lead to clear risk profiles for cybercrime victimization.

Results also point towards heterogeneity in risk factors for different cybercrimes. Risk factors differed between general cybercrime and specific cybercrimes, and between hacking, malware and fraud victimization. For hacking, four risk profiles were found with a risk of hacking victimization in the following year between 18 and 25 percent. However, there were also inconsistent findings. Contrarily to what was expected, together the different risk profiles included all age groups, both

medium and high self-control, both occasional and frequent exposure and both risk profiles that clicked on the phishing link and risk profiles that did not. Interestingly, the risk factors with larger effects on hacking victimization were all behavioral: choosing a weak password, downloading the (fictional) software and clicking on the phishing link. For malware, two risk profiles were found with a risk of malware victimization in the following year of 29 and 33 percent. Contrarily to what was expected, the risk profiles differed in password strength, clicking on phishing links and exposure. The risk factor with a larger association with malware victimization was low self-control, which in almost all cases was associated with an increased risk of malware victimization. For fraud, three risk profiles were found with a risk of fraud victimization in the following year ranging between 23 and 27 percent. Interestingly, the only risk factor that was in all three risk profiles was a factor indicating self-protective behavior, namely all three risk profiles shared that respondents did not indicate that they would click on the phishing link. The risk factors with larger effects on fraud victimization were low self-control and sharing personal information. Given the heterogeneity in risk profiles for different cybercrimes, future research should distinguish between different types of cybercrime victimization.

Personal characteristics and routine activities were less often found to be risk factors for cybercrime victimization than was found in previous studies. However, this finding is in line with other longitudinal studies (Guerra and Ingram 2020; Van de Weijer 2019), suggesting that future studies should incorporate a longitudinal design. In line with what was expected, low self-control was found to be one of the main risk factors for general, malware and fraud victimization, but not for hacking. Contrarily to what was expected, while age and frequent exposure increased the likelihood of cybercrime victimization in some risk profiles, they did not have a clear (main) effect in any cybercrime category. This is in line with findings that cybercrime victimization is likely affected by factors that are simultaneously related to age and exposure, but that age (Bossler and Holt 2009;

Leukfeldt and Yar 2016; Mesch and Dodel 2018; Parry et al. 2021) and exposure (Büchi et al. 2016; Ngo et al. 2020) have a limited direct effect on cybercrime victimization.

Most main effects were behavioral in nature. In line with what was expected, all behavioral factors that were measured in the current study were present in at least one high-risk profile for cybercrime victimization. However, there was heterogeneity found in the associations between self-protective behavior and cybercrime victimization. Namely, choosing a weak password was found to be a risk factor for general cybercrime and hacking victimization, downloading (fictional) software and clicking on a phishing link were found to be risk factors for hacking victimization, and sharing personal information was found to be a risk factor for general cybercrime and fraud victimization. This points to a heterogeneity within the relationship between self-protective behavior and cybercrime victimization, where certain types of behavior only increase the risk of certain types of cybercrimes. This is in line with studies that, using the method of crime scripting, found that the crime commission process and behaviors of victims differ between cybercrimes (e.g., Loggen and Leukfeldt 2022; Matthijsse et al. 2023). Future studies should therefore incorporate different types of actual self-protective behavior. Moreover, in three out of four cybercrime victimization categories a behavioral risk factor was found to have a positive effect on the outcome, the exception being malware victimization. This underlines the importance of incorporating behavioral risk factors in future research aiming to establish risk profiles for cybercrime victimization.

Although the current study uses an innovative method and unique data to study cybercrime victimization, it also has some shortcomings that should be taken into account. Firstly, our sample reflects the gender distribution, employment statuses, and geographical distribution within Dutch society. However, the finding that respondents are more often highly educated and, on average, older than the average Dutch citizen limits the generalizability of our findings. Furthermore, the Dutch

sample may limit the generalizability of our findings to citizens from other countries. On the one hand, due to its high Internet penetration rate, citizens in the Netherlands may have a higher chance of becoming a cybercrime victim. On the other hand, in other countries like Australia a much higher cybercrime victimization rate has been found than in the Netherlands (Voce and Morgan 2023).

Secondly, in line with other case-oriented methods, CACC results may also not be generalizable regardless of the representativeness of the sample used, since dominant profiles constitute constructed populations (Hart et al. 2023). By identifying dominant profiles, we identify relevant groups of observations and discard others. With regard to contextual variability analyses, it is worth noting that the low numbers of comparable pairs of profiles for some variables may impact the robustness of the findings. For instance, in the data, there were only seven identical pairs of dominant profiles except for the self-control variable (although e.g., up to 23 pairs in the variable for sharing personal information). This means that our estimation of the main effect of self-control on victimization outcomes is based on these seven comparisons. In this sense, the main effects can be interpreted as a meta-analysis of cases, where the interpretation relies on the distribution of outcomes, rather than being the sole estimate resulting from a regression analysis. The peculiarities of the CACC and its complementary analyses represent one of the main differences between case-oriented methods and variable oriented-methods, and also one of the main reasons why they offer an alternative view.

Thirdly, participants from wave 1 who were recently victimized by cybercrime, were less inclined to participate in wave 2, which may have led to an underestimation of victimization in the second wave. This may have caused an underestimation of the number of risk profiles, the number of victims within each profile and the strength of main effects. Future research should therefore aim to minimize between-wave non-response, for example through incentives. Also, the current study compared victims to non-victims but did not distinguish for repeat-victimization. Further reasons that

victimization might have been underestimated lie in the nature of self-reported victimization; victims may not always be aware when they have been successfully targeted by online attacks or may choose not to report all instances of victimization. Nonetheless, it is worth noting that the prevalence of victimization remained substantial in wave 2. Future research should aim to include repeat victimization and to measure victimization in new ways (Holt 2023), for example by not only asking respondents about victimization but also consequences of victimization they might have noticed but not recognized as a successful cybercrime attack (Holt et al. 2020). Future research should also include repeat measurements of risk factors, as risk factors may change over time, possibly prompted by the research measurement itself.

Fourthly, although the measurements of actual online self-protective behaviors have great advantages, they also have their limitations (Van 't Hoff-de Goede et al. 2020). In the measurement involving the downloading of (fictional) software, a pop-up designed to resemble the Windows operating system was utilized. Individuals who do not use the Windows operating system might exhibit greater suspicion and be less inclined to consent to downloading the software. Moreover, some respondents revealed that they opted for passwords that were either more complex or simpler compared to their usual password choices. Furthermore, when using the CACC as a method of analysis, we also had to decide how to categorize the variables, which in some cases led to a loss of information. We justified our operationalization, but it is possible that a different operationalization produces different results.

Lastly, respondents may have behaved differently than in real life, since all risk scenarios were simulated. There is also a possibility that respondents feel a sense of security within the online environment of the survey. Consequently, they may be more inclined to engage in unsafe behaviors compared to real-life cyber-risk situations. This suggests that the percentage of unsafe behavior within

the home environment may be lower than what is captured by the research instrument. However, it is crucial to note that the purpose of the research instrument is to assess self-protective online behavior within an apparently safe environment. This is important because criminals often mimic safe environments, such as online banks or web shops, to deceive individuals into divulging personal information.

As cybercrime is on the rise, we need insights into who is at risk for cybercrime victimization. Studies to date have not been able to establish risk profiles, partly because they often incorporate a limited range of risk factors or rely on self-reported measurements for behavioral data. We recently did a study that used regression analysis to examine the relationship between personal characteristics, online routine activities, actual self-protective online behavior and future cybercrime victimization (Van 't Hoff-de Goede 2023). We concluded that the field is in need of new and innovative ways to look at cybercrime victimization and the current paper did so by introducing CACC to cybercrime studies. We believe the current article shows that alternative and innovative methods should be used. Indeed, we now identified high-risk profiles for victimization across different cybercrimes with a detailed breakdown of their composition, as well as patterns of clustering around a set of individual characteristics together with the main effects produced by particular profile configurations on cybercrime victimization. Of course, we don't want to overstate our findings. The current paper took a first step into establishing risk profiles for cybercrime victimization using CACC and we urge other researchers to execute more studies that measure more and different factors. When future studies further develop risk profiles for cybercrime victimization, policy implications may be developed for cybercrime prevention. Furthermore, we strongly encourage longitudinal data collection and the measurement of actual behavior. We therefore welcome others to use the measurement instrument of the Online Behavior and Victimization Study.

Declaration of Interest

This work was supported by the WODC (Research and Documentation Centre) of the Ministry of Justice and Security.

Author bio's

Susanne van 't Hoff-de Goede is an associate professor at the Centre of Expertise Cybersecurity at The Hague University of Applied Sciences and a research fellow at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). She studies the human factor in cybercrime: offenders, victims and law enforcement and focusses, amongst other things, on cybervictimization and interventions aimed at reducing cybercrime.

Asier Moneva is a researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and the Centre of Expertise Cybersecurity at The Hague University of Applied Sciences. His research focuses on how, when, and where cybercrime occurs, focusing on the human factors involved.

Rutger Leukfeldt is a senior researcher Cybercrime at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), director of the Centre of Expertise Cybersecurity at The Hague University of Applied Sciences and full professor at Leiden University. His research addresses the human factor in cybercrime, and focusses on cybercriminal networks, pathways into cybercrime, cybercrime victimization, cybersecurity and law enforcement.

References

Aguerri, Jesús C., Lorena Molnar, and Fernando Miró-Llinares. 2023. "Old crimes reported in new bottles: the disclosure of child sexual abuse on Twitter through the case# MeTooInceste." *Social Network Analysis and Mining* 13(1): 27.

Ahmad, Rahayu, and Ramayah Thurasamy. 2022. "A Systematic Literature Review of Routine Activity Theory's Applicability in Cybercrimes." *Journal of Cyber Security and Mobility* 11(3): 405–32. doi: 10.13052/jcsm2245-1439.1133.

Akdemir, Naci, and Christopher J. Lawless. 2020. "Exploring the Human Factor in Cyber-Enabled and Cyber-Dependent Crime Victimisation: A Lifestyle Routine Activities Approach." *Internet Research* 30(6): 1665–87. doi: 10.1108/INTR-10-2019-0400.

Anderson, Keith B. 2006. "Who Are the Victims of Identity Theft? The Effect of Demographics." *Journal of Public Policy and Marketing* 25(2): 160–71. doi: 10.1509/jppm.25.2.160.

Andrews, Sally, David A. Ellis, Heather Shaw, and Lukasz Piwek. 2015. "Beyond Self-Report: Tools to Compare Estimated and Real-World Smartphone Use." *PLoS ONE* 10(10): 1–9. doi: 10.1371/journal.pone.0139004.

Augustyn, Megan B., Callie M. Rennison, Gillian M. Pinchevsky, and Amy B. Magnuson. 2020. "Intimate partner stalking among college students: Examining situational contexts related to police notification." *Journal of family violence* 35(7): 679-691.

Bergmann, Marie C., Arne Dreißigacker, Bennet von Skarczinski, and Gina R. Wollinger. 2018. "Cyber-Dependent Crime Victimization: The Same Risk for Everyone?" *Cyberpsychology, Behavior, and Social Networking* 21(2): 84–90. doi: 10.1089/cyber.2016.0727.

Borwell, Jildau, Jurjen Jansen, and Wouter Stol. 2018. "Human Factors Leading to Online Fraud Victimisation: Literature Review and Exploring the Role of Personality Traits." Pp. 26-45 in *Psychological and behavioural examinations in cyber security*, edited by John Mcalaney, Lara A. Frumkin, and Vladlena Benson. IGI Global.

Bossler, Adam M., and Thomas. J. Holt. 2009. "On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory." *International Journal of Cyber Criminology* 3(1): 400–420.

Bossler, Adam M., and Thomas. J. Holt. 2010. "The Effect of Self-Control on Victimization in the Cyberworld." *Journal of Criminal Justice* 38(3): 227–36. doi: 10.1016/j.jcrimjus.2010.03.001.

Brady, Patrick Q., Ryan Randa, and Bradford W. Reyns. 2016. "From WWII to the World Wide Web: A research note on social changes, online 'places', and a new online activity ratio for routine activity theory." *Journal of Contemporary Criminal Justice* 32(2): 129-147.

Büchi, Moritz, Natascha Just, and Michael Latzer. 2016. "Modeling the Second-Level Digital Divide: A Five-Country Study of Social Differences in Internet Use." *New Media and Society* 18(11): 2703–22. doi: 10.1177/1461444815604154.

Chen, Hongliang, Christopher E. Beaudoin, and Traci Hong. 2017. "Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors." *Computers in Human Behavior* 70: 291–302. doi: 10.1016/j.chb.2017.01.003.

Cheng, Cecilia, Linus Chan, and Chor I. Chau. 2020. "Individual Differences in Susceptibility to Cybercrime Victimization and Its Psychological Aftermath." *Computers in Human Behavior* 108. doi: 10.1016/j.chb.2020.106311.

Choi, Kyung-shick. 2008. "Computer Crime Victimization and Integrated Theory: An Empirical Assessment." *International Journal of Cyber Criminology* 2(1): 308–33.

Cohen, Lawrence E., and Marcus Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review:* 588–608.

Downs, Julie S., Mandy Holbrook, and Lorrie F. Cranor. 2007. "Behavioral Response to Phishing Risk." Pp. 37–44 in *Proceedings of the anti-phishing working groups - 2nd annual eCrime researchers summit*. New York, New York, USA: ACM Press.

Drew, Jacqueline M., and Lucy Farrell. 2018. "Online Victimization Risk and Self-Protective Strategies: Developing Police-Led Cyber Fraud Prevention Programs." *Police Practice and Research* 19(6): 537–49. doi: 10.1080/15614263.2018.1507890.

Ellis, David A., Brittany I. Davidson, Heather Shaw, and Kristoffer Geyer. 2019. "Do Smartphone Usage Scales Predict Behavior?" *International Journal of Human Computer Studies* 130: 86–92. doi: 10.1016/j.ijhcs.2019.05.004.

Gottfredson, Michael R., and Travis Hirschi. 1990. "*A General Theory of Crime"*. Stanford: Stanford University Press.

Guerra, Chris, and Jason R. Ingram. 2020. "Assessing the Relationship between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data." *Deviant Behavior:* 1–17. doi: 10.1080/01639625.2020.1774707.

Hart, Timothy C. 2014. "Conjunctive analysis of case configurations." *JDiBrief Series*. Retrieved February 2, 2024. (https://www.ucl.ac.uk/jill-dando-institute/sites/jill-dando-institute/files/conjunctive_analysis_of_case_configurations_1-5_all.pdf)

Hart, Timothy C. 2019. "Identifying Situational Clustering and Quantifying Its Magnitude in Dominant Case Configurations: New Methods for Conjunctive Analysis." *Crime and Delinquency 66*(1): 143159.

Hart, Timothy C., and Asier Moneva. 2018. "Análisis conjunto de configuraciones de caso: Una introducción al pensamiento configural." *Revista Española de Investigación Criminológica 16:* 119.

Hart, Timothy C., Asier Moneva, and Miriam Esteve. 2023. "Conjunctive analysis of case configurations*."* Pp. 287-298 in *Understanding Crime and Place*, edited by Elizabeth R. Groff and Cory P. Haberman. Temple University Press.

Hart, Timothy C., Callie M. Rennison, and Terance D. Miethe. 2017. "Identifying Patterns of Situational Clustering and Contextual Variability in Criminological Data: An Overview of Conjunctive Analysis of Case Configurations." *Journal of Contemporary Criminal Justice 33*(2): 112120. https://doi.org/10.1177/1043986216689746

Herrero, Juan, Andrea Torres, Pep Vivas, Antonio Hidalgo, Francisco J. Rodríguez, and Alberto Urueña. 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). doi: 10.3390/ijerph18073763.

Holt, Thomas J. 2023. "Understanding the State of Criminological Scholarship on Cybercrimes." *Computers in Human Behavior* 139. doi: 10.1016/j.chb.2022.107493.

Holt, Thomas J., and Adam M. Bossler. 2013. "Examining the Relationship Between Routine Activities and Malware Infection Indicators." *Journal of Contemporary Criminal Justice* 29(4): 420–36. doi: 10.1177/1043986213507401.

Holt, Thomas J., Johan van Wilsem, Steve van de Weijer, and Eric R. Leukfeldt. 2020. "Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization." *Social Science Computer Review* 38(2): 187–206. doi: 10.1177/0894439318805067.

Jansen, Jurjen, and Eric R. Leukfeldt. 2016. "Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization." *International Journal of Cyber Criminology* 10(1): 79–91. doi: 10.5281/zenodo.58523.

Lee, Claire S., and Yan Wang. 2022. "Typology of Cybercrime Victimization in Europe: A Multilevel Latent Class Analysis." *Crime and Delinquency* 70(4). doi: 10.1177/00111287221118880.

Lee, Yi Y., Chin L. Gan, and Tze W. Liew. 2022. "Phishing Victimization among Malaysian Young Adults: Cyber Routine Activities Theory and Attitude in Information Sharing Online." *Journal of Adult Protection* 24(3–4): 179–94. doi: 10.1108/JAP-06-2022-0011.

Leukfeldt, Eric R. 2014. "Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization." *Cyberpsychology, Behavior, and Social Networking* 17(8): 551–55. doi: 10.1089/cyber.2014.0008.

Leukfeldt, Eric R., ed. 2017. "*Research Agenda: The Human Factor in Cybercrime and Cybersecurity*." The Hague: Eleven International Publishing.

Leukfeldt, Eric R., and Majid Yar. 2016. "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis." *Deviant Behavior* 37(3): 263–80. doi: 10.1080/01639625.2015.1012409.

Lévesque, Fanny L., Sonia Chiasson, Anil Somayaji, and José M. Fernandez. 2018. "Technological and Human Factors of Malware Attacks." *ACM Transactions on Privacy and Security* 21(4): 1–30. doi: 10.1145/3210311.

Lévesque, Fanny L., Jose M. Fernandez, and Anil Somayaji. 2014. "Risk Prediction of Malware Victimization Based on User Behavior." *Proceedings of the 9th IEEE International Conference on Malicious and Unwanted Software, MALCON 2014*. Pp 128–34. doi: 10.1109/MALWARE.2014.6999412.

Loggen, Joeri, and Eric R. Leukfeldt. 2022. "Unraveling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands." *Trends in Organized Crime* 25(2): 205-225.

Louderback, Eric R., and Olena Antonaccio. 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 and Delinquency* 67(3): 366–98. doi: 10.1177/0011128720906116.

Machuletz, Dominique, Henrik Sendt, Stefan Laube, and Rainer Böhme. 2017. "Users Protect Their Privacy If They Can: Determinants of Webcam Covering Behavior." *Proceedings of the European Workshop on Usable Security at the Privacy Enhaning Technologies Symposium (EuroSEC'16)*. doi: 10.14722/eurousec.2016.23014.

Marret, Mary J., and Wan Y. Choo. 2017. "Factors Associated with Online Victimisation among Malaysian Adolescents Who Use Social Networking Sites: A Cross-Sectional Study." *BMJ Open* 7(6): 1–11. doi: 10.1136/bmjopen-2016-014959.

Matthijsse, Sifra R., Maria S. van 't Hoff-de Goede, and Eric R. Leukfeldt. 2023. "Your files have been encrypted: A crime script analysis of ransomware attacks." *Trends in Organized Crime*: 1-27.

McGuire, Mike and Samantha Dowling. 2013. "*Cyber Crime: A Review of the Evidence. Research Report 75."* London: Home Office.

Mesch, Gustavo S., and Matias Dodel. 2018. "Low Self-Control, Information Disclosure, and the Risk of Online Fraud." *American Behavioral Scientist* 62(10): 1356–71. doi: 10.1177/0002764218787854.

Miethe, Terance D., Timothy C. Hart, and Wendy C. Regoeczi. 2008. "The conjunctive analysis of case configurations: An exploratory method for discrete multivariate analyses of crime data." *Journal of Quantitative Criminology* 24: 227-241.

Mikkola, Marko, Atte Oksanen, Markus Kaakinen, Bryan L. Miller, Iina Savolainen, Anu Sirola, Izabela Zych, and Hye J. Paek. 2020. "Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-National Context." *International Journal of Offender Therapy and Comparative Criminology*. doi: 10.1177/0306624X20981041.

Moneva, Asier, Miriam Esteve, and Timothy C. Hart. 2022. "*Cacc: Conjunctive analysis of case configurations*." (Version 0.1.0) [R package]. CRAN. Retrieved February 2, 2024 (https://cran.r-project.org/package=cacc)

Moneva, Asier, Fernando Miró-Llinares, and Timothy C. Hart. 2021. "Hunter or Prey? Exploring the situational profiles that define repeated online harassment victims and offenders." *Deviant Behavior* 42(11): 1366-1381.

Näsi, Matti, Petri Danielsson, and Markus Kaakinen. 2021. "Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors." *European Journal on Criminal Policy and Research*. doi: 10.1007/s10610-021-09497-0.

Ngo, Fawn T., and Raymond Paternoster. 2011. "Cybercrime Victimization: An Examination of Individual and Situational Level Factors." *International Journal of Cyber Criminology* 5(1): 773.

Ngo, Fawn T., Alex R. Piquero, Jennifer LaPrade, and Bao Duong. 2020. "Victimization in Cyberspace: Is It How Long We Spend Online, What We Do Online, or What We Post Online?" *Criminal Justice Review* 45(4): 430–51. doi: 10.1177/0734016820934175.

Ovelgönne, Michael, Tudor Dumitras, B. Aditya Prakash, Venkatramana S. Subrahmanian, and Benjamin Wang. 2017. "Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks." *ACM Transactions on Intelligent Systems and Technology* 8(4): 1–25. doi: 10.1145/2890509.

Paez, Gabriel R., and Timothy C. Hart. 2022. "Context matters (but some contexts matter more): disentangling the influence of traditional bullying victimization on patterns of cyberbullying outcomes." *International journal of bullying prevention*: 1-13.

Parry, Douglas A., Brittany I. Davidson, Craig J. R. Sewall, Jacob T. Fisher, Hannah Mieczkowski, and Daniel S. Quintana. 2021. "A Systematic Review and Meta-Analysis of Discrepancies

between Logged and Self-Reported Digital Media Use." *Nature Human Behaviour*. doi: 10.1038/s41562-021-01117-5.

Partin, Raymond D., Ryan C. Meldrum, Peter S. Lehmann, Sinchul Back, and Elisa M. Trucco. 2021. "Low Self-Control and Cybercrime Victimization: An Examination of Indirect Effects Through Risky Online Behavior." *Crime and Delinquency* 68(13–14): 2476–2502. doi: 10.1177/00111287211061728.

R Core Team. 2022. "*R: A language and environment for statistical computing*." Vienna. Retrieved February 2, 2024 (https://www.R-project.org/)

Ragin, Charles C. 2013. "New directions in the logic of social inquiry." *Political Research Quarterly*: 171-174.

Reep-van den Bergh, Carin M.M., and Marianne Junger. 2018. "Victims of Cybercrime in Europe: A Review of Victim Surveys." *Crime Science* 7(1): 1-15. doi: 10.1186/s40163-018-0079-3.

Reyns, Bradford 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): 216–38. doi: 10.1177/0022427811425539.

Reyns, Bradford W., Bonnie S. Fisher, Adam M. Bossler, and Thomas J. Holt. 2018. "Opportunity and Self-Control: Do They Predict Multiple Forms of Online Victimization?" *American Journal of Criminal Justice* 44(1): 63–82. doi: 10.1007/s12103-018-9447-5.

Reyns, Bradford W., Ryan Randa, and Billy Henson. 2016. "Preventing Crime Online: Identifying Determinants of Online Preventive Behaviors Using Structural Equation Modeling and

Canonical Correlation Analysis." *Crime Prevention and Community Safety* 18(1): 38–59. doi: 10.1057/cpcs.2015.21.

RStudio Team. (2022). "*RStudio: Integrated development environment for r*." Boston, MA. Retrieved February 2, 2024 (http://www.rstudio.com/)

Sharif, Mahmood, Jumpei Urakawa, Nicolas Christin, Ayumu Kubota, and Akira Yamada. 2018. "Predicting Impending Exposure to Malicious Content from User Behavior." *Proceedings of the ACM Conference on Computer and Communications Security:* 1487–1501. doi: 10.1145/3243734.3243779.

Sheng, Steve, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie F. Cranor, and Julie Downs. 2010. "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems:* 373–82. doi: 10.1145/1753326.1753383.

Statistics Netherlands (2019). "*Population; gender, age and martital status*." Retrieved May 2, 2019 (https://opendata.cbs.nl/statline/#/CBS/nl/dataset/7461BEV/table?fromstatweb)

Statistics Netherlands (2024). "*Safety monitor 2023*." The Hague: Statistics Netherlands.

Van de Weijer, Steve G. A. 2019. "Predictors of Cybercrime Victimization: Causal Effects or Biased Associations?" Pp. 83–110 in *The human factor of cybercrime*, edited by E. R. Leukfeldt and T. J. Holt. New York: Routledge.

Van de Weijer, Steve G. A., and Eric R. Leukfeldt. 2017. "Big Five Personality Traits of Cybercrime Victims." *Cyberpsychology, Behavior, and Social Networking* 20(7): 407–12. doi: 10.1089/cyber.2017.0028.

Van der Kleij, Rick, Maria S. van 't Hoff-de Goede, Steve van de Weijer, and Eric R. Leukfeldt. 2021. "How Safely Do We Behave Online? An Explanatory Study into the Cybersecurity Behaviors of Dutch Citizens." *Proceedings of the International Conference on Applied Human Factors and Ergonomics*. Vol. 2: Pp. 238–46. Springer International Publishing.

Van 't Hoff-de Goede, Maria S., Rick van der Kleij, Steve G. A. van de Weijer, and Eric R. Leukfeldt. 2019. "*Hoe Veilig Gedragen Wij Ons Online? Een Studie Naar de Samenhang Tussen Kennis, Gelegenheid, Motivatie En Online Gedrag van Nederlanders. [How Safely Do We Behave Online? A Study of the Relationship between Knowledge, Opportunity, Motivation and the Online Behaviour of Dutch Citizens]".* Den Haag: The Hague University of Applied Sciences.

Van 't Hoff-de Goede, Maria S., Eric R. Leukfeldt, Rick van der Kleij, and Steve G. A. van de Weijer. 2020. "The Online Behaviour and Victimization Study: The Development of an Experimental Research Instrument for Measuring and Explaining Online Behaviour and Cybercrime Victimization." Pp. 21-41 in *Cybercrime in Context*, edited by Marleen Weulen Kranenbarg and Eric R. Leukfeldt. Springer.

Van 't Hoff-de Goede, Maria S., Steve G. A. van de Weijer, and Eric R. Leukfeldt. 2023. "Explaining Cybercrime Victimization Using a Longitudinal Population-Based Survey Experiment. Are Personal Characteristics, Online Routine Activities, and Actual Online Behavior Related to Future Cybercrime Victimization?" *Journal of Crime and Justice: 472-491*.

Van Wilsem, Johan. 2013a. "'Bought It, but Never Got It' Assessing Risk Factors for Online Consumer Fraud Victimization." *European Sociological Review* 29(2): 168–78. doi: 10.1093/esr/jcr053.

Van Wilsem, Johan. 2013b. "Hacking and Harassment-Do They Have Something in Common? Comparing Risk Factors for Online Victimization." *Journal of Contemporary Criminal Justice* 29(4): 437–53. doi: 10.1177/1043986213507402.

Voce, Isabella, and Anthony Morgan. 2023. "*Cybercrime in Australia 2023*." Australian Government, Statistical Report 43.

Wickham, Hadly, Mara Averick, Jennifer Bryan, Winston Chang, Lucy D'Agostino McGowan, Romain François, Garrett Grolemund, Alex Hayes, Lionel Henry, Jim Hester, et al. 2019. "Welcome to the tidyverse." *Journal of Open Source Software* 4(43): 1686. https://doi.org/10.21105/joss.01686

Wilcockson, Thomas D. W., David A. Ellis, and Heather Shaw. 2018. "Determining Typical Smartphone Usage: What Data Do We Need?" *Cyberpsychology, Behavior, and Social Networking* 21(6): 395–98. doi: 10.1089/cyber.2017.0652.

Williams, Matthew L. 2016. "Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level." *British Journal of Criminology* 56(1): 21–48. doi: 10.1093/bjc/azv011.