KrimOJ Kriminologie – Das Online-Journal
Criminology – The Online Journal

No. 1/2025

Edith Huber, Bettina Pospisil, Thilo Sauter & Albert Treytl

Cybercrime Victimisation and Categorization – A View from the Perspective of Routine-Activity-Theory (RAT)

This study explores the intersection of cybercrime victimisation and prevention through the lens of Routine Activity Theory (RAT). Using a representative survey in Austria, the research examines the victimisation experiences of private individuals, focussing on financial, data, and personal cybercrimes. The findings reveal significant differences in demographics and guardianship levels among victims of different cybercrime types. Notably, higher levels of physical and personal guardianship were unexpectedly correlated with increased victimisation. This study underscores the heterogeneity of cybercrime and the need for nuanced prevention strategies that take into account the distinct characteristics of various cybercrime types. The implications highlight the complexity of the relationship between cybersecurity measures and victimisation, challenging assumptions about the protective efficacy of increased cybersecurity awareness and measures.

Keywords: Awareness, Cybercrime, Cybersecurity, Routine Activity Theory, Victimization

Cybercrime-Viktimisierung und Kategorisierung – eine Betrachtung aus der Perspektive der Routine-Aktivitäten-Theorie (RAT)

Diese Studie untersucht die Schnittstelle zwischen Cybercrime-Viktimisierung und Prävention durch die Linse der Routine-Aktivitäten-Theorie (RAT). Anhand einer repräsentativen Umfrage in Österreich werden die Viktimisierungserfahrungen privater Personen analysiert, wobei der Schwerpunkt auf finanziellen, datenbezogenen und persönlichen Cyberkriminalität liegt. Die Ergebnisse zeigen signifikante Unterschiede in Demografie und Schutzniveaus der Opfer verschiedener Cybercrime-Typen. Auffallend ist, dass höhere Levels an physischem und persönlichem Schutz unerwarteterweise mit einer erhöhten Viktimisierung korrelierten. Diese Studie unterstreicht die Heterogenität von Cyberkriminalität und die Notwendigkeit nuancierter Präventionsstrategien, die die unterschiedlichen Charakteristika der verschiedenen Arten von Cyberkriminalität berücksichtigen. Die Implikationen heben die Komplexität der Beziehung zwischen Cybersecurity-Maßnahmen und Viktimisierung hervor und stellen Annahmen über die Schutzwirkung erhöhter Cybersecurity-Bewusstseins- und Maßnahmen in Frage.

Schlagwörter: Bewusstseinsbildung, Cybercrime, Cybersecurity, Routine-Aktivitäten-Theorie, Viktimisierung

1. Introduction

It is difficult to obtain valid figures on the actual number of victims of cybercrime, as cybercrime is recorded and defined differently in different countries around the world. The number of Internet and social networking users has increased dramatically in recent years. The Internet in general and social networks in particular are changing the psychological and social needs

https://doi.org/10.18716/ojs/krimoj/2025.1.7

of users, defining belonging and self-esteem and often serving to avoid loneliness (Mikkola, 2020). Cybercriminals are taking advantage of this, seeing this human behavior as a vulnerability to be exploited in their criminal activities. As a result, an increasing number of different types of attacks and crimes have emerged over the years. ENISA (2022) reports that ransomware, malware, social engineering threats, data threats, availability threats such as denial of service, availability threats such as cyber threats, disinformation - misinformation, and supply chain attacks are currently the most common cyberattacks in Europe ~~(Enisa, 2022).~~ However, this report does not cover all types of cybercrime. They vary considerably depending on whether the victim is a company, a state or an individual. At the same time, they show that cybercrime refers to many different phenomena, as if it were an extremely large and diverse field.

This lumping together of different phenomena could reduce the quality of information that can be obtained about them, especially when focusing on cybercrime victimization: This is particularly relevant when thinking about vulnerability and prevention: Victims of phishing need very different information than victims of data breaches or cyberbullying. But in addition to their needs, victims of these heterogeneous types of cybercrime also appear to be different as such (van de Weijer et al., 2020; Dreissigacker & Riesner, 2018).

Combining this interest in victims with the RAT theory, the article at hand will examine, as a research question, how physical and personal guardianship influences the victimization of various forms of cybercrime.

2. Victimization and Cybercrime

While neither of these concepts, cybercrime and victimization, has a clear definition on its own, which already poses several difficulties for researchers, the combination of the two poses an additional challenge: countability. Being a victim of a crime or offense is one thing, recognizing it is another. In cybercrime, the unrecorded number of crimes that are not recognized or perceived as such by victims is enormous. This makes it very difficult to count cybercrime offenses in official statistics.

For the current study, it was decided to use a representative survey in Austria to capture those incidents that do not make it into official statistics. In Austria, for example, 10,308 cases were recorded in official crime statistics in 2012. By 2023, there were already 60,195 cases (BMI, 2023). These are divided into cyber-enable and cyberdependet crime. In the context of this article, respondents are victims if they experience a cyberattack, regardless of whether the attack is successful or not. For example, the recipient of a phishing email is a victim of that attack regardless of how they deal with it.

In this study, we are particularly interested in the relationship between cybercrime victimization and prevention in the form of IT security. More precisely, this research reveals the relation between the perception of victimization and prevention as best estimation of unrecorded number of crimes. Particularly in the area of cybercrime, people do not always perceive criminal behavior as such. To illustrate, if an individual receives 70 WhatsApp messages from another person within a 24-hour period, this behavior could be considered or perceived as a potential instance of cyberstalking. Nevertheless, even in such cases, there are individuals who do not regard this behavior as criminal. Similar examples can be found in numerous other cybercrimes.

Knowledge and knowledge transfer of cybercrime relevant content play a key role here. These phenomena are analyzed within the theoretical framework of Routine Activity Theory (RAT). RAT is a widely accepted explanation for the occurrence of crime and cybercrime. It serves as a practical tool for professionals involved in crime reduction and prevention to assess crime problems. According to RAT, when a crime occurs, three elements coincide in time and space: a) A feasible target is present. b) There is an absence of a capable guardian to deter the crime. c) A likely and motivated offender is in the vicinity (Cohen & Felson, 1979). The results of the present study should provide a more comprehensive understanding of cybercrime victimization and the impact of IT security and prevention measures.

However, there are some participants who are unaware of their own victimization. This must be taken into account when interpreting the results. To get a more complete picture of the situation, it was also decided to include those experiences of victimization for which there is no official evidence.

The work presented here focuses on the victimization of private individuals in Austria.[1] The aim of the research was to gain a better understanding of cybercrime victimization and the victims themselves, as well as the impact of competent guardianship in this regard. We examine how physical and personal guardianship influence victimization by different forms of cybercrime, using RAT theory as the basis for this research question.

3. From Defining and Classifying Cybercrime to the Victim’s Perspective

Addressing the issues of cybercrime and victimization is a major challenge for researchers: There is no common consensus on the definition or demarcation of either term. This lack of a common and clear understanding of the phenomenon of cybercrime is challenging and hinders efforts to combat cybercrime.

As Phillips et al. (2022) recently put it, even today, "... the only consensus in the literature is that there is no single clear, precise, and universally accepted definition of cybercrime ..." (p. 382). Depending on the point of view, a definition may focus on the attack vector, the perpetrator, the victim, or the motives. Although they have been around for a number of years, the definitions of Thomas and Loader (2000) and Gordon and Ford (2006) are still the most popular ones referred to in a scholarly context. Other authors have supported the definition of cybercrime as a type of crime that involves, uses, or is related to computers or information technology (Furnell, 2003; Varghese, 2016; Wilson, 2008).

In line with these assumptions, there have been various attempts to categorize the heterogeneous phenomenon of cybercrime. On the one hand, various authors and institutions propose a dichotomous distinction between ‘cyber-dependent crime’ and ‘cyber-enabled crime’ (McGuire & Dowling, 2013). This distinction has been made by various researchers using alternative terminology. While Furnell (2001) characterizes the terms as ‘computer-focused cybercrime’ and ‘computer-enabled cybercrime’, Gordon and Ford (2006) critically discuss

[1] The study is based on the legal framework in Austria. Cyber-dependent crime: StGB: §§ 107c, 118a, 119, 119a, 126a, 126b, 126c, 148a, 225a; Cyber-enable crime: StGB: §§ 146, 147, 105, 106, 107, 107a, 115, 207b, 218, 223, 224, 228c, 231, 232, 241a, 283.

'Type I' and 'Type II' cybercrime, and the United Nations (2000) makes the distinction between 'cybercrime in the narrow sense' and 'cybercrime in the broader sense'. However, these authors share the same understanding of how these two groups of cybercrimes differ from each other. While "cyber-dependent crime" refers to crimes that can only be committed online, such as malware distribution and hacking, "cyber-enabled crime" refers to traditional crimes that have moved from real life to cyberspace, such as fraud, child pornography, or cyberstalking. This distinction is most common in cyberspace and promotes the understanding that the relationship of the cybercrime offense to information and communication technology is the most important criterion for defining its characteristics (Phillips et al., 2022).

On the other hand, psychologists Kirwan and Power (2013) differentiate cybercrime according to the interaction between offender and victim. They speak of 'property crime', such as identity theft and fraud, and 'cybercrime against the person', such as cybercrime involving the sexual abuse of children. Unlike property crime, cybercrime against the person involves significant interaction between the offender and the victim. Bossler and Holt (2010) choose the target of the crime as a variable for differentiation. They conclude that victimization differs between person-based crimes, where the specific person is the target, and computer-based crimes, where computers in general are the target. The target of the crime, as well as the amount of loss suffered by the victim, is of great importance for sentencing in cybercrime. However, this is not the case for the victim's perception (Graves et al., 2019). "In contrast, the most important factor in the public's assessment of the seriousness of the crime is the attacker's motivation, which has a much less drastic impact on sentencing guidelines." (Graves et al. 2019, p. 352) In line with this finding, Leukfeldt and Yar (2016) differentiate cybercrimes based on the motivation of the offenders. They distinguish the crimes they found into computer-related crimes such as hacking and malware infection, financial crimes such as identity and consumer fraud, and interpersonal crimes such as stalking and threatening communications.

In general, it can be said that a clear and unambiguous classification of cybercrime offenses is not possible. Overlaps can be found in a wide range of areas. For example, ransomware can be categorized as both cyberdependent and cyberenable. Here, a distinction is made between blackmail itself (cyberenable) and the installation of software (cyberdependent). This pattern can be found in numerous cybercrime offenses, such as cyberstalking (Huber & Brandtweiner, 2020), and in a wide range of cyberfraud types.

However, to enable the perspective of cybercrime victims and to question the role of competent guardianship in this regard, the authors of this paper draw on concepts from routine activity theory to support this view.

4. Routine Activity Theory: A Theoretical Framework for Cybercrime Victimization

One of the most popular theories for understanding cybercrime victimization is the RAT. This theory originally evolved focusing on traditional forms of offline crime and thus can be used for other types of crime, too (Cohen & Felson, 1979). Essentially, this theory states that crime occurs when the three tenets of the RAT come together: a suitable target, a motivated adversary, and the absence of a capable guardian (Cohen & Felson, 1979). In recent years, scholars have applied these theories to cyberspace after originally conceptualizing and applying them to the offline world (e. g., Holt & Bossler, 2009; Choi, 2008; Leukfeldt & Holt, 2020). This theoretical framework argues that cybercrime arises from the use of computer networks to connect motivated offenders with potential victims in the absence of capable guardianship. Target suitability is measured by online activity or frequency of Internet use. Capable guardianship, or lack thereof, is measured by cybersecurity management. Despite the lack of physical targets and direct contact, RAT is believed to be an appropriate theory for understanding cybercrime because there is a shift in the types of targets considered suitable in cyberspace (Reyns, 2010). As with anything that exists as digital code in cyberspace, information is becoming the ultimate target (Yar, 2005). However, the form of information depends on the nature of the cybercrime. In the context of cyberstalking, personal information is valuable because it gives offenders access to victims (Reyns, 2010). In cybercrime, the information may be intellectual property, such as software, or systems, such as banking systems (Newman & Clarke, 2003). Similar results are also reported by Bergmann et al., 2018. Based on routine activity theory, their study assumes that crime is influenced by the presence of a motivated offender, suitable targets (internet users) and the absence of capable guardians (prevention measures). Frequent use of internet-enabled devices increases the likelihood of victimization. In this context, it is not relevant how many people live in the same household (Bergmann et al., 2018).

Thus, the current study also explores profiles of cybercrime victimization through RAT by examining how measures of cybersecurity guardianship relate to different types of cybercrime victimization. We use this framework to examine hidden groups of cybercrime victimization in the Austrian context. Echoing the findings of previous RAT research, the study posits that cyber-enabled environments not only create opportunities for motivated offenders to exploit online targets, but such environments may also gradually degrade online users' digital guardianship over time, making users more susceptible to crime victimization.

The RAT has been used in several academic studies to focus on the perspective of cybercrime victims. For example, Lee and Wang (2022) conducted a multilevel latent class analysis (MLCA) in 28 European countries based on individuals' levels of online activity and cybersecurity guardianship. The results of the study identified two distinct groups - the “risk class“ and the “cautious class“ - with a higher or lower likelihood of being victimized online. Several variables are used to define the classes. The risk class is 10 times more likely to be a victim of cybercrime. The ‘risk class’ represents only 19 % of the total sample. The three main causes of cyber victimization are fraudulent emails/calls, malware, and extremism (Lee & Wang, 2022). Other scholars have concluded that groups of victims suffering from different categories of cybercrime differ in terms of variables such as self-control (Bossler & Holt, 2010), as well as accessibility and personal capable guardianship (Leukfeldt & Yar, 2016). Dreissigacker & Riesner's (2018) study shows that victims' sociodemographic variables also differed in terms of the specific crime they were victimized by. For example, while men were more likely to be victimized by financial and data crimes, women were significantly more likely to be victimized by personal cybercrimes such as stalking and sexual harassment.

These insights and findings suggest that just as cybercrime is very heterogeneous and difficult to define, so too is its broad field of victims. This leads the authors of this paper to hypothesize (hypothesis 1) that the demographics and level of guardianship of cybercrime victims differ in terms of the type of incident that victimized them. To test this hypothesis, the authors of this paper have undertaken a further categorization of cybercrime, inspired by these previous ideas and findings.

In addition, the study requires a closer look at the three tenets of the RAT, with a focus on capable guardianship as the underlying research interest.

First, it can be assumed that Internet use correlates with victimization. In 2023, the number of internet users in Austria will be 7.03 million, which corresponds to 91 % of the Austrian population. The number of people who are exclusively offline will decrease to about 0.7 million (INTEGRAL, 2023). This means that there is an almost infinite social space in which potential victims can be contacted, and that a large group of people can be reached with comparatively little effort (sending an email or chat, social media, creating a homepage, or uploading an image, text, or video file to an existing platform). However, there is evidence that simply spending more time on the computer or Internet does not increase the risk of victimization (see, for example, Weber & Wührl, 2023). It seems that it is not only the amount of time people spend online that matters, but also the purpose for which they use it. Holt and Bossler (2009) found that while respondents' general computer use and activities did not have a significant impact on the likelihood of experiencing online harassment, the number of hours respondents spent in chat rooms and using instant messaging did.

Based on an analysis of reported cybercrime incidents in Austria, Huber et al. (2019) identified a variety of motives that cybercriminals may have: the desire for revenge, financial intentions, bragging, conviction, and even following or imitating. Attackers vary, for example, in their composition, from individuals to groups, in their technical skills and expertise, in their modus operandi, and in their goals and targets. Furnell (2021) notes that while a few years ago hackers operated alone, pursuing personal goals such as challenge, ego, and mischief, today they are increasingly organized and pursuing someone else's agenda (cybercrime as a service).

This paper focuses on the lack of capable guardianship as a determinant of victimization by various forms of cybercrime. Regarding the relationship between capable guardianship and cybercrime victimization, previous research has distinguished two forms of guardianship: Physical guardianship, which is computer software designed to protect the computer system from cybercriminals. While some studies found that higher levels of computer security (i. e., antivirus and firewall software) had no effect on the likelihood of cybercrime victimization (Bossler & Holt, 2010; Leukfeldt & Yar, 2016; Marcum, 2008), other studies showed that these guardianship measures offset the risk of online victimization (Choi, 2008). Based on the RAT and these findings, the authors hypothesize (hypothesis 2) that people who use more physical guardianship measures are less likely to be victims of cybercrime.

The other type of guardianship is personal guardianship, which refers to the respondent's level of competence with computers and technology. In this regard, some authors highlight the importance of sociodemographic variables such as income, gender, age, and education as key factors of cybersecurity knowledge (Dodel & Mesch, 2017; Lee & Chua, 2023). According to Kang et al. (2015), technical education is one of the two factors that positively influence users' cyber awareness and knowledge. Redmiles et al. (2016) state that it is the process of knowledge acquisition, which is dependent on sociodemographics, that makes a difference in cyber victimization.

Based on the RAT and these findings, the authors hypothesize (hypothesis 3) that the likelihood of becoming a victim of cybercrime decreases for people with an affinity for IT. Furthermore, the authors hypothesize (hypothesis 4) that people who are willing to learn about security risks are less likely to become victims of cybercrime.

5. Methodology

5.1 The Sample

The study was conducted among unregistered victims of cybercrime against private individuals in Austria. A representative online survey was conducted, legally based on Austrian criminal law. Austrian crime statistics include both enabling and disabling cybercrime offenses.
Based on these crimes, a questionnaire[2] was created that took about 15 minutes to complete. After a pre-test, the link to the online questionnaire was sent to the respondent pool of the market and opinion research institute Integral in March 2020. The survey participants were recruited at random from the Integral online pool of about 30,000 individuals between 16 and 69 years of age from all over Austria.[3] The survey was conducted using computer aided web interviewing (CAWI). A total of 8,802 people were invited to take part in the survey, resulting in a sample of (n =)1,007 respondents.
The gender ratio of respondents is balanced, with 50 % of respondents identifying as male and 50 % as female. The respondents are representative of the Austrian population, with approximately half being under 45 years of age (48 %) and the remaining half being older (52 %). Approximately one-third of respondents have completed an apprenticeship (32 %), followed by individuals who have attended high school without obtaining a diploma and those who have graduated from high school (each 22 %). Less frequently, respondents have obtained a university degree (19 %). The majority of participants have a monthly net household income of between 1,000 and 3,900 euros (70 %). A quarter (25 %) of respondents have an income above this range.
This means a response rate of 11 %. The structural similarity between the Austrian population (16-69 years old internet users in Austria) and the sample was ensured by means of quota control: The authors used sampling weights according to the variables gender (two classes), age (ten classes), education (four classes) and federal state (nine classes). Data analysis was performed using SPSS software and included frequency counts as well as multivariate analysis methods.

5.2 Measures

5.2.1 Dependent Variable

As highlighted in the previous chapters, neither the term victimization nor the term cybercrime are easy to define for academics and even more so for lay people. To make the topic easier to grasp for the participants of the quantitative survey, the authors decided to ask about experiences with specific forms of cybercrime. We therefore approximate the victimization variable

[2] Survey questionnaire https://door.donau-uni.ac.at/o:5133
[3] Initially, recruitment was conducted mainly through pop-up tests, as representative surveys did not yield enough new participants. The method of recruitment changed with increasing internet penetration: currently, most pool participants are recruited through telephone or face-to-face interviews, as well as pop-up tests (widely distributed across various websites). A small percentage (<5 %) join via registrations on the homepage or are referred by a friend. All pool participants are stored in a database that is actively maintained. Contact occurs solely between staff members and pool participants; a community site for interactions between pool members is not provided.

by the perception of the victimization. To gain knowledge about cybercrime victimization, respondents were asked whether they had been a victim of any of the 22 types of crime in the official crime statistics (BMI 2023). Respondents could answer 'yes', 'I think so, but I cannot prove it', 'no', or 'don't know'. For the reasons given above, the answers 'yes' and 'I think so' were combined for analysis. Based on the assumption that victims of cybercrime differ according to the type of cybercrime they have experienced, the crimes were grouped for analysis (see Figure 1). Like Leukfeldt and Yar (2016), the authors of this paper distinguish between cybercrimes that target (1) money, (2) data, or (3) a person as such. The first category of cybercrime refers to crimes in which the perpetrators seek financial gain. Examples include phishing attacks, fraud, and extortion. The second category of cybercrime is crimes that attempt to gain unauthorized access to, collect, or manipulate data. Examples include spyware, computer viruses, and data breaches. The third group includes crimes where the offender's primary goal is to harm or harass the victim. Examples include the distribution of hate messages or nude images, as well as deception to initiate sexual contact and stalking. These three categories are not necessarily distinct. The collection of information could be used to gain financial advantage (through extortion) or to harass a victim (through stalking). However, it is possible to distinguish cybercrime offenses in these categories by the entity that the perpetrators are ostensibly and immediately focused on. The authors of this paper hypothesize that the category of cybercrime is related to the characteristics of its victims. This hypothesis is tested through empirical analysis.

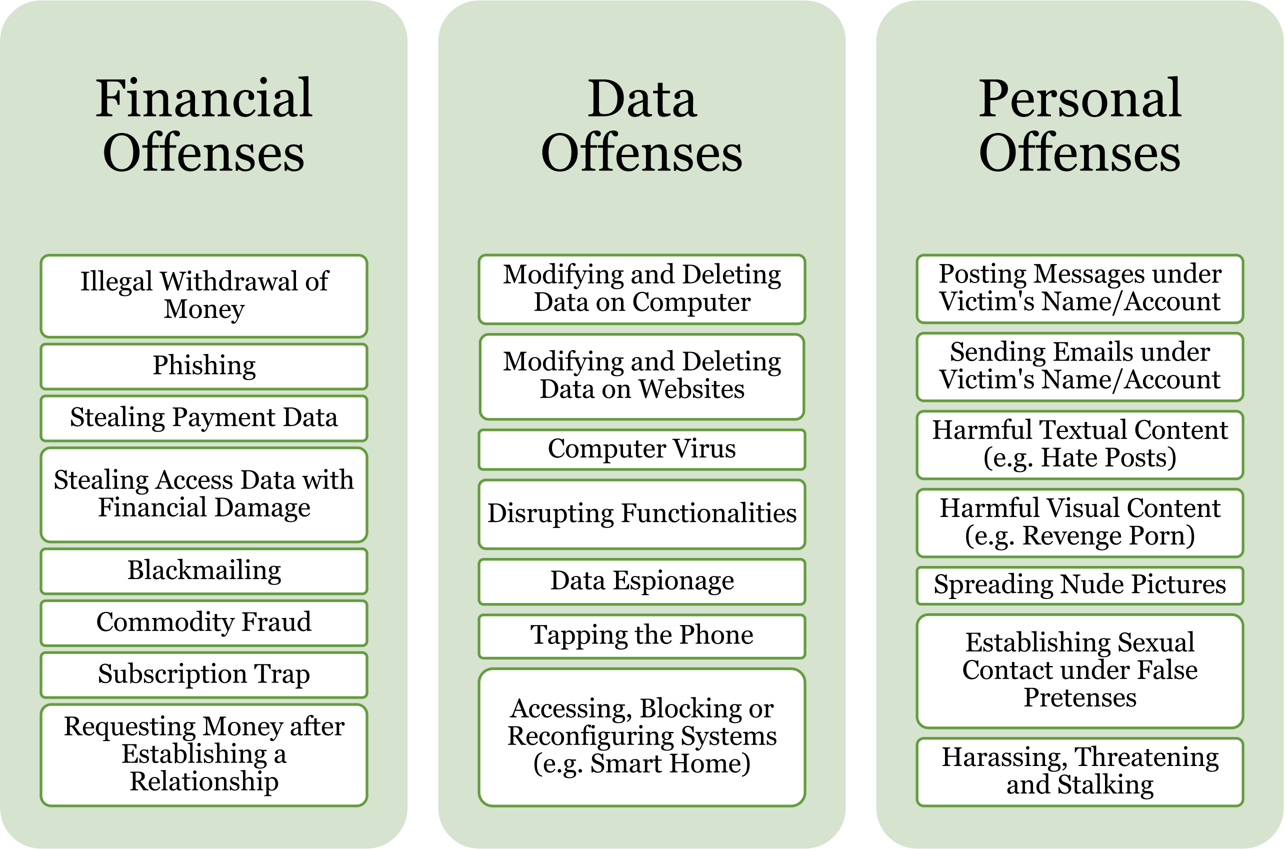
5.2.2 Independent Variables

To determine the respondents' personal guardianship, the authors asked them about their digital skills, in line with previous studies (Graham & Triplett, 2017; Leukfeldt, 2014). Therefore, the survey asked about the participants' background in IT, i.e., whether they had education or training in IT, an IT-related job, a specific interest in IT, or none of the above. This was a multiple-choice question.[4] Participants were also asked if they were aware of the security vulnerabilities of the devices they owned. To determine respondents' physical protection, participants were asked if they used five specific security measures, which could be answered yes, no, or don't know.

Based on findings from previous studies, the questions focused on the use of antivirus software (Bossler & Holt, 2011; Leukfeldt, 2014) and the safe use of passwords (Burnes et al., 2020; Bossler & Holt, 2011). Specifically, the survey asked whether participants used certain security measures, such as having an antivirus program on their computer and an antivirus program on their smartphone, changing their passwords regularly, keeping their passwords secret, and having a password safe.

[4] In principle, individuals who are more actively engaged with information technology and utilize it more frequently are generally considered at a higher risk of becoming victims of cyber-related incidents. However, given that approximately 95 % of the Austrian population regularly uses the internet, it can be inferred that the overall level of internet usage within this population is significantly high (Statistik Austria, 2024).

Figure 1. The authors classified the relevant cybercrime crimes into three groups based on the target of the perpetrators


Financial Offenses
Illegal Withdrawal of Money
Phishing
Stealing Payment Data
Stealing Access Data with Financial Damage
Blackmailing
Commodity Fraud
Subscription Trap
Requesting Money after Establishing a Relationship
Data Offenses
Modifying and Deleting Data on Computer
Modifying and Deleting Data on Websites
Computer Virus
Disrupting Functionalities
Data Espionage
Tapping the Phone
Accessing, Blocking or Reconfiguring Systems (e.g. Smart Home)
Personal Offenses
Posting Messages under Victim's Name/Account
Sending Emails under Victim's Name/Account
Harmful Textual Content (e.g. Hate Posts)
Harmful Visual Content (e.g. Revenge Porn)
Spreading Nude Pictures
Establishing Sexual Contact under False Pretenses
Harassing, Threatening and Stalking

5.2.3 Control Variables

In addition to the theoretically relevant variables, the authors also collected demographic information from the participants. These included gender (male/female/diverse), age as a continuous variable, education level (1=primary school and below to 6=university degree), and net monthly household income in groups (1=below € 1,000 to 10=€ 5,000 and above in increments of € 500). These variables were included to control for any demographic differences between groups of victims of different forms of cybercrime.
To better assess the variables that influence victimization of different forms of cybercrime, the authors ran logistic regressions separately for the three different groups of cybercrimes as well as for cybercrime in general.

5.2.4 Limitations

Approximating victimization by the variable of *perceived* victimization is a limitation to the results. Nevertheless, it allows accessing a large field of unreported incidents within a large representative sample. Undetected and therefore unperceived cybercrime remains, yet this is a principal problem of IT security as research on unreported crime requires the examination of individual perceptions of criminal acts in an effort to make them visible.

A second limitation is given by the survey's intricate nature and extensive duration. No supplementary data was collated concerning the time lag between the implementation of IT security measures and the occurrence of the incident, nor the victimization in relation to particular temporal periods. Consequently, it is only possible to calculate correlations and not connections.

6. Results

6.1 Characterizing Victims of Cybercrime by Frequencies

The results of the survey show that cybercrime is not new to respondents (see Table 1): At 84 % (849 respondents), the majority have been victims of cybercrime at least once in their lives. Of those respondents victimized by cybercrime, 87 % (741) have been victims of cybercrime targeting their financial assets. This is followed by cybercrime against data with 69 % (589). Finally, only 35 % (295) have experienced cybercrime against their personal domain. The figures show that numerous respondents got victimized by more than one of these three types of cybercrime.

Victims of cybercrime in general are almost equally divided between men and women. However, men are slightly more likely to be victims of cybercrime across all types of crime. The average age of cybercrime victims is around 45. Müller et al. (2022) also come to similar conclusions. The researchers conducted a study in Lower Saxony (Germany) on the topic of cybercrime against private individuals. Here, too, it was possible to provide significant evidence that men are more likely to be victims of cybercrime than women, especially in the area of cyberenabled crime (Müller et al., 2022). Victims of personal crime are younger (43 years) than victims of data and financial offenses (45 years). The descriptive statistics also show that the educational level of victims is relatively balanced across the different types of cybercrime. However, victims of personal cybercrime appear to have a slightly lower level of education (mean 3.49) than victims of data (3.56) and financial offenses (3.55). A similar picture emerges with regard to the income of victims, where the differences are somewhat greater. With an average of 5.07, the average income of personal offenses victims is lower than that of financial (5.71) or data (5.65) crime victims. The table also shows that an IT-related education, job, or interest is relatively balanced among victims of the different types of cybercrime. Victims of personal offenses are slightly more likely to be educated or employed in the IT field.

In order to investigate the correlation between victimization across different groups of cybercrimes, a cross-tabulation was conducted. The results in Table 2 show that the perceived victimization by the three different groups of cybercrime stands in significant correlation with each other.[5] While all victims are almost equally likely to inform themselves about security

[5] The correlation value between financial and data offenses counts 0.250, data offenses and personal offenses counts 0.238, and personal offenses and financial offenses counts 0.258. All correlation values refer to contingency coefficient with an error tolerance of less than 0.001.

vulnerabilities of the smart systems and devices they use, victims of personal (2.81) and financial (2.79) offenses are slightly more likely to take security measures than victims of cybercrime in general (2.76) and data offenses (2.75).[6]

Table 1. Frequencies of the three groups of cybercrimes as well as cybercrime in general.

	Victimization by cybercrime in general (n=849)					Victimization by financial offenses (n=741)				
Variable	n	Min	Max	Mean	Std. Dev	n	Min	Max	Mean	Std. Dev
Demographics										
Gender	849	1	2	1.48	0.50	741	1	2	1.46	0.50
Age	849	16	69	45.07	13.93	741	17	69	45.21	13.76
Education	849	1	6	3.52	1.59	741	1	6	3.55	1.60
Income	826	1	10	5.61	2.61	724	1	10	5.71	2.64
Personal guardianship										
IT-related training/education	849	0	1	0.09	0.29	741	0	1	0.10	0.30
IT-related workplace	849	0	1	0.11	0.31	741	0	1	0.11	0.32
IT-related interests	849	0	1	0.32	0.47	741	0	1	0.33	0.47
None	849	0	1	0.53	0.50	741	0	1	0.51	0.50
Inform oneself about vulnerabilities	849	0	1	0.59	0.49	741	0	1	0.58	0.49
Physical guardianship										
Security measures (up to 5)	849	0	5	2.76	1.08	741	0	5	2.79	1.07

	Victimization by data offenses (n=589)					Victimization by personal offenses (n=295)				
Variable	n	Min	Max	Mean	Std. Dev	n	Min	Max	Mean	Std. Dev
Demographics										
Gender	589	1	2	1.46	0.50	295	1	2	1.46	0.50
Age	589	16	69	44.54	13.76	295	17	69	42.67	13.97
Education	589	1	6	3.56	1.59	295	1	6	3.49	1.59
Income	576	1	10	5.65	2.59	284	1	10	5.07	2.63
Personal guardianship										
IT-related training/education	589	0	1	0.10	0.30	295	0	1	0.12	0.33
IT-related workplace	589	0	1	0.11	0.32	295	0	1	0.14	0.35
IT-related interests	589	0	1	0.33	0.47	295	0	1	0.32	0.47
None	589	0	1	0.50	0.50	295	0	1	0.47	0.50
Inform oneself about vulnerabilities	589	0	1	0.61	0.49	295	0	1	0.61	0.49
Physical guardianship										
Security measures (up to 5)	589	0	5	2.75	1.09	295	0	5	2.81	1.14

[6] Since the cybercrime groups, next to other variables in the table, are part of a multiple response set, the authors additionally calculated the Chi-square test. The results show significant correlations between the groups of cybercrimes and gender (9.975, p<0,05), age (37.123, p<0.001), income (39.669, p<0.001), IT-background (40.632, p<0,001) and informing oneself about vulnerabilities (21.740, p<0.05). The correlation between the groups of cybercrimes and educational level as well as security measures was not significant.

Table 2. Cross-tabulation of the three groups of cybercrimes (total numbers)

		Financial offenses		Data offenses		Personal offenses	
		Yes	No	Yes	No	Yes	No
Data offenses	Yes	490	99	x	x	x	x
	No	251	167	x	x	x	x
Personal offenses	Yes	x	x	228	67	x	x
	No	x	x	361	351	x	x
Financial offenses	Yes	x	x	x	x	271	470
	No	x	x	x	x	24	242

6.2 Explaining Victims' Characteristics and the Influence of Capable Guardianship

In a next step, we tested whether there was a relationship between the independent variables of guardianship and the dependent variables of victimization by the different types of cybercrime as well as cybercrime in general. The objective is to investigate whether the probability of an individual becoming a victim of cybercrime can be predicted by socio-demographic data and guardianship factors. Given that the dependent variables of victimization are binary (i. e., yes/no), the authors conducted a logistic regression analysis. The independent variables were recoded as dummy variables. Unlike linear regression analyses, which employ the least squares method, logistic regression analysis is based on maximum likelihood estimation (MLE). The system SPSS employs the logarithm of the value of the likelihood function, which was maximized during the estimation of the model. This logarithmic value is designated as "log-likelihood" or "LL" for brevity. For the estimation of the model quality, this value is multiplied by -2 (-2LL). The value -2LL characterizes an error term.

The results of the logistic regression analysis presented in Table 3 show the extent to which RAT-based variables could explain cybercrime victimization. The table also includes demographic variables as control variables. All models are significant with an error probability under 0.001. While gender has no significant effect on cybercrime victimization in general or on personal cybercrime offenses, it does have an effect on financial and data offenses.

Being male increases the likelihood of being a victim of both financial (OR=1.465, p<0.05, SER 0.169) and data (OR=1.467, p<0.05, SER 0.149) offenses by almost one and a half times. The findings revealed that age has a significant impact on the probability of becoming a victim of cybercrime, encompassing both financial and personal offenses. The influence of age on the likelihood of victimization by cybercrime manifested in different ways. Individuals aged between 45 and 54 years were found to be at a significantly elevated risk of victimization by cybercrime in general (OR=2.145, p<0.05, SER 0.387) and financial offenses (OR=2.366, p<0.01, SER 0.329) in comparison to those younger than 25 years of age. The likelihood of victimization was found to be more than two times higher. In contrast, the data indicated that individuals aged 55 and above were less likely to be victims of personal offenses than those below the age of 25. The odds ratio (OR) was 0.445 (SER 0.293), with a p-value of less than 0.01, indicating a decrease in likelihood of over 50 %.

Table 3. Logistic regression model concerning the three groups of cybercrime offenses as well as cybercrime in general

	Victimization by cybercrime in general (n=849)	Victimization by financial offenses (n=741)	Victimization by data offenses (n=589)	Victimization by personal offenses (n=295)
Demographics				
Gender				
Female	.	.	.	.
Male	.259 (1.295)	.382* (1.465)	.383* (1.467)	.174 (1.190)
Age				
24 or less	.	.	.	.
25-34	.178 (1.195)	.104 (1.110)	.374 (1.454)	-.339 (.713)
35-44	.323 (1.382)	.275 (1.317)	.477 (1.612)	-.369 (.692)
45-54	.763* (2.145)	.861** (2.366)	.204 (1.226)	-.270 (.764)
55 or more	.158 (1.171)	.207 (1.230)	-.051 (.950)	-.809** (.445)
Level of education				
No school or compulsory school	.	.	.	.
Apprenticeship	.268 (1.307)	-.183 (.832)	.318 (1.375)	-.221 (.802)
High School, no diploma	.449 (1.567)	.023 (1.023)	.564 (1.758)	-.240 (.787)
High school graduate	.403 (1.496)	.229 (1.257)	.342 (1.408)	-.130 (.878)
University degree	1.310** (3.705)	.724 (2.064)	.762* (2.143)	-.202 (.817)
Monthly household income net				
999 or less	.	.	.	.
1.000-1.999	-.482 (.618)	-.278 (.757)	-.402 (.669)	-.517 (.596)
2.000-2.999	-.128 (.879)	-.264 (.768)	-.199 (.820)	-.924** (.397)
3.000-3.999	.023 (1.024)	.219 (1.245)	-.153 (.858)	-.712* (.491)
4.000-4.999	-.647 (.524)	-.272 (.762)	-.309 (.734)	-1.242*** (.289)
5.000 or more	-.149 (.862)	.273 (1.313)	-.438 (.645)	-1.303*** (.272)
Personal guardianship				
IT-related training/education	.284 (1.329)	.222 (1.248)	.115 (1.122)	.333 (1.395)
IT-related workplace	.483 (1.621)	.328 (1.388)	.140 (1.150)	.244 (1.276)
IT-related interests	.165* (1.179)	.179** (1.196)	.098 (1.103)	.066 (1.068)
None of them	.	.	.	.
Inform oneself about vulnerabilities				
Yes, always	.730* (2.076)	.263 (1.301)	.626** (1.871)	.337 (1.401)
Yes, partly	.493* (1.638)	.062 (1.064)	.338* (1.403)	.088 (1.092)
No	.	.	.	.
Physical guardianship				
Security measures (up to 5)	.203* (1.224)	.209** (1.232)	.032 (1.033)	.104 (1.110)
Constant	.079 (1.082)	-.257 (.774)	-.629 (.533)	-.067 (.935)

Model X^2	70.950	81.282	54.397	54.860
df	20	20	20	20
SER (Konstant)	.089	.073	.065	.070
p	.000	.000	.000	.000
-2LL	770.304	1036.332	1268.497	1122.942
Nagelkerkes-R^2	.121	.117	.073	.078
Entries are unstandardized coefficients; odds ratio are in parentheses.				
* p < .05; ** p < .01; *** p < .001				

Education was partly found to be predictive of being a victim of cybercrime. The risk of victimization by cybercrime in general was found to be more than three and a half times higher for those with a university degree than for those who had not completed school or compulsory school (OR=3.705, p<0.01, SER 0.484). Furthermore, the risk of data offenses was found to be more than two times higher for those with a university degree than for those who had not completed school or compulsory school (OR=2.143, p<0.05, SER 0.366). The analysis demonstrated that income had a considerable impact on the probability of being a victim of personal offenses. Individuals with a monthly household income net of less than 1,000 euros exhibited a significantly elevated probability of becoming victims of personal offenses, with a 60 % reduction observed among those with incomes between 2,000 and 2,999 euros (OR = 0.397, p<0.01, SER 0.328) and a 51 % reduction among those with incomes between 3,000 and 3,999 euros (OR = 0.491, p<0.05, SER 0.327). The same is true for individuals with incomes between 4,000 and 4,999 euros (OR = 0.289, p<0.01, SER 0.360), who have a 71 % lower probability of becoming victims of personal offenses, and individuals with an income above 4,999 euros (OR = 0.272, p<0.01, SER 0.392), who have a 73 % lower probability of becoming victims of personal offenses.

In examining the role of personal protection variables, it was found that while IT-related education and training, and the presence of an IT-related workplace, do not significantly influence the probability of victimization, the presence of IT-related interests does. In comparison to individuals with no IT-related activities, those with an interest in IT are approximately 18 % more likely to be victims of cybercrime in general (OR=1.179, p<0.05, SER 0.076). This is particularly the case with financial offenses, with an approximate 20 % increase (OR=1.196, p<0.01, SER 0.062). The results do not support hypothesis 3, which posits that individuals with an affinity for IT are less likely to become victims of cybercrime. Neither an IT-related education nor an IT-related job, nor an interest in IT, is significantly negatively correlated with any type of cybercrime victimization. Furthermore, individuals who proactively seek information regarding the security vulnerabilities of their devices are more likely to become victims of cybercrime and data offenses, in comparison to those who do not. Those who always inform themselves have a probability of becoming victims of cybercrime that is more than two times higher than those who do not (OR=2.076, p<0.05, SER 0.370). Meanwhile, the probability is more than one and a half times higher for those who only partially inform themselves (OR=1.638, p<0.05, SER 0.201). The same is true for data offense victimization, where always informing oneself increases the probability by slightly less than twofold (OR=1.871, p<0.01, SER 0.232) and informing oneself partly increases it by slightly less than one and a half fold (OR=1.403, p<0.05, SER 0.146). There is no significant correlation with financial and personal offenses. These results do not support hypothesis 4, which states that individuals who are willing to inform themselves about security risks are less likely to become victims of cybercrime. Conversely, the results indicate a significant positive correlation between awareness of security risks and the probability of becoming a victim of cybercrime and data offenses.

The results in the table show that taking specific security measures related to physical guardianship was found to significantly increase the likelihood of being a victim of cybercrime (OR=1.224, p<0.05, SER 0.085), such that for every one-point increase in security measures taken, the likelihood of being a victim increases by 22 %. This is particularly evident for financial offenses, where the likelihood of victimization increases by 23 % (OR=1.232, p<0.01, SER 0.071). However, there was no significant correlation between data and personal offenses. This implies mixed results for hypothesis 2, which states that people who use more physical protection measures are less likely to be victims of cybercrime. The results for data and personal offenses do not support this hypothesis as there is no significant correlation. The results for cybercrime in general and financial offenses support the hypothesis of a relationship between measures of physical guardianship and victimization, but in an unexpected direction: The results suggest that people with more physical guardianship are more likely to be victims of cybercrime in general and financial offenses.

Finally, the Nagelkerkes-R2 shows the extent to which the variables in this study describe the dependent variable of cybercrime victimization. While demographics and the variables of capable guardianship describe 12 % of cybercrime victimization in general and 12 % of financial offenses, they describe only 7 % of personal offenses and 8 % of data offenses.[7]

All of these results suggest that there is reason to believe, in line with hypothesis 1, that the demographics and level of guardianship of cybercrime victims differ in terms of the type of incident that victimized them. This once again demonstrates the heterogeneity of cybercrime and the need for scholarship to take a more nuanced look at the phenomenon.

One might contend that, given the focus on perceptions of victimization rather than the act of victimization itself, the subjective assessment of participants introduces a degree of bias into the results. This is particularly the case with regard to cybercrime, where offenses are often not even perceived as such. This is not a limitation of this study alone, as research on unreported crime requires the examination of individual perceptions of criminal acts in an effort to make them visible. In order to make this bias more explicit, the authors attempted to make an adjustment. If one assumes that a lack of awareness of the presence of security measures is indicative of a lack of awareness of victimization, it would be possible to exclude those individuals who responded ‘I don’t know’ to any of the questions regarding the presence of security measures from the sample. This will not eliminate bias; however, it can be viewed as an attempt to exclude those individuals who are most likely to misreport or fail to observe cybercrime. For comparison, the authors conducted the same regression for the new sample of (n=) 798 individuals.

As illustrated in Table 4, the regression analysis conducted with the smaller sample set reveals notable discrepancies when compared to the regression analysis performed with the entire sample. Upon exclusion of those uncertain of their security measures, the model for data offenses is no longer significant (p=0.065) and thus cannot be interpreted.

[7] The figures have been rounded.

Table 4. Logistic regression model concerning the three groups of cybercrime offenses as well as cybercrime in general excluding those individuals who responded ‘I don't know’ to any of the questions regarding the presence of security measures from the sample (n=798)

	Victimization by cybercrime in general (n=683)	Victimization by financial offenses (n=602)	Victimization by data offenses (n=481)	Victimization by personal offenses (n=231)
Demographics				
Gender				
Female	.	.	.	.
Male	.156 (1.169)	.318 (1.374)	.297 (1.346)	.079 (1.082)
Age				
24 or less	.	.	.	.
25-34	.078 (1.081)	.054 (1.055)	.354 (1.425)	-.493 (.611)
35-44	.325 (1.383)	.196 (1.217)	.612 (1.843)	-.210 (.810)
45-54	.853 (2.347)	.875* (2.398)[8]	.351 (1.421)	-.317 (.728)
55 or more	.221 (1.248)	.284 (1.329)	.055 (1.057)	-.795* (.452)[9]
Level of education				
No school or compulsory school	.	.	.	.
Apprenticeship	-.108 (.897)	-.530 (.588)	.377 (1.458)	-.295 (.745)
High School, no diploma	-.093 (.911)	-.432 (.649)	.538 (1.712)	-.434 (.648)
High school graduate	-.109 (.897)	-.200 (.819)	.439 (1.551)	-.339 (.712)
University degree	.833 (2.300)	.350 (1.418)	.870* (2.386)[10]	-.205 (.815)
Monthly household income net				
999 or less	.	.	.	.
1.000-1.999	-.248 (.780)	.043 (1.044)	-.365 (.694)	-.270 (.764)
2.000-2.999	-.041 (.959)	-.122 (.894)	-.172 (.842)	-.726 (.484)
3.000-3.999	.097 (1.102)	.331 (1.392)	-.147 (.864)	-.461 (.631)
4.000-4.999	-.481 (.618)	-.060 (.942)	-.355 (.701)	-.982* (.375)[11]
5.000 or more	-.101 (.904)	.231 (1.259)	-.256 (.774)	-1.260** (.284)[12]
Personal guardianship				
IT-related training/education	.552 (1.736)	.504 (1.655)	.029 (1.030)	.396 (1.485)
IT-related workplace	.403 (1.497)	.349 (1.418)	.121 (1.129)	.239 (1.269)
IT-related interests	.197* (1.218)[13]	.181** (1.198)[14]	.070 (1.073)	.090 (1.094)
None of them	.	.	.	.
Inform oneself about vulnerabilities				

[8] SER 0.382
[9] SER 0.337
[10] SER 0.421
[11] SER 0.403
[12] SER 0.454
[13] SER 0.086
[14] SER 0.068

Yes, always	.513 (1.670)	.226 (1.254)	.331 (1.392)	.415 (1.514)
Yes, partly	.433 (1.542)	.088 (1.092)	.245 (1.278)	.151 (1.163)
No	.	.	.	.
Physical guardianship				
Security measures (up to 5)	.149 (1.161)	.145 (1.156)	.048 (1.049)	.141 (1.151)
Constant	.602 (1.826)	.138 (1.148)	-.646 (.524)	-.311 (.732)
Model X2	43.505	53.529	30.298	46.085
df	20	20	20	20
SER (Konstant)	.103	.083	.073	.079
p	.002	.000	.065	.000
-2LL	590.527	811.438	1011.674	889.751
Nagelkerkes-R2	.098	.099	.052	.082
Entries are unstandardized coefficients; odds ratio are in parentheses.				
* p < .05; ** p < .01; *** p < .001				

The effect of gender on the probability of becoming a victim of financial offenses is no longer statistically significant. The results of the second regression model indicate that age continues to exert a significant influence on the likelihood of becoming a victim of financial and personal offenses, with only slight alterations in the magnitude of this impact. In contrast, the results for education underwent a significant change, as the new model yielded no significant results that could be interpreted. These findings are particularly noteworthy in the context of cybercrime, where the odds ratios in Table 3 were not only statistically significant but also relatively high. Additionally, Table 3 revealed that income has a notable influence on the likelihood of becoming a victim of personal offenses. This is consistent across both models, with the exception of the second model with a smaller sample, where only the two highest income groups exhibited a significantly lower probability of victimization, and the odd ratios were more moderate.

With respect to the variables pertaining to guardianship, interest in IT continues to exert a considerable influence on the probability of becoming a victim of cybercrime in general and financial crime. The figures have undergone only slight alterations. However, awareness of vulnerabilities no longer has a significant impact on the probability of being a victim of cybercrime in general and data crime. A similar relationship is observed with regard to the role of security measures and the likelihood of being a victim of cybercrime in general and financial crime.

7. Discussion

The results of this study are varied and open to different interpretations. Based on our hypotheses, the following results can be stated:

7.1 Cybercrime Categorization (Hypothesis 1)

Hypothesis 1 posited that the demographics and level of guardianship of cybercrime victims would differ in terms of the type of incident that victimized them. The results presented in this paper support this hypothesis, as the significance and direction of the correlation differ between the three types of cybercrime.

In principle, a clear classification of cybercrime is difficult. There are always distortions between the offenses. Nevertheless, the results show, that a separation like the one in the paper at hand makes sense. For example, personal offenses are the only type of crime that do not correlate significantly with any of the various variables of guardianship (security measures, IT relationship, awareness of vulnerabilities).

7.2 Security Measures (Hypothesis 2)

Hypothesis 2 states that people who use more physical security measures are less likely to be victims of cybercrime. Based on previous literature, a negative relationship was expected between these variables. While the results for data and personal crime do not show a significant relationship, the numbers for cybercrime in general and financial crime support the assumption of a positive relationship between measures of physical guardianship and risk of victimization. Although these are unexpected results, the present paper is not the first to report such findings. Similarly, the study by Bossler et al. (2012) showed that protection software appeared to increase the likelihood of harassment victimization, which was also inconsistent with previous research. This would be relevant for the Theory of Planned Behavior (TPB), which argues that behavioral intentions are determined by attitudes, subjective norms, and perceived behavioral control. This theory was applied by Pahnila, Siponen, and Mahmood (2007) to explain how organizational policies and training influence employees' attitudes and behavior regarding compliance with cybersecurity practices.

However, when those respondents who are most likely to misreport or fail to observe cybercrime are excluded from the sample, the relationship becomes insignificant. In this model, there is no significant correlation between the overtaking of security measures and the probability of victimization with any of the cybercrime types.

7.3 Technological Background (Hypothesis 3)

Based on previous literature, the authors also hypothesized that the likelihood of becoming a victim of cybercrime would decrease for individuals with an affinity for IT. Similar to hypothesis 2, a negative correlation was assumed, while the empirical results showed a positive or no correlation. Compared to the group of individuals who had nothing to do with IT, the results are not significant for education/training in IT and working in an IT workplace. However, having an interest in IT increases the likelihood of being a victim of cybercrime in general and financial offenses. The results of other authors, such as Ngo & Paternoster (2011), also showed that they were surprised by a significant correlation between cybercrime affinity and victimization, in the opposite direction to that assumed. However, in their case, the results were related to education: Individuals who attended educational workshops were more likely to receive - in this case - unwanted pornographic material.

The positive correlation between interest in IT and the probability of being a victim of cybercrime, and particularly financial crime, persists when the sample size is reduced, with only slight alterations to the figures.

7.4 Interest in Safety Risks (Hypothesis 4)

Hypothesis 4 posited that people who are willing to learn about security risks are less likely to become victims of cybercrime. Again, a negative correlation was hypothesized, while the results suggest a positive or no correlation. Compared to the group of individuals who do never inform themselves about security vulnerabilities, to always or partly inform oneself increased the likelihood of being victimized by cybercrime in general and data crimes. The correlation was not significant for financial and personal crimes.

The model of data offenses is rendered insignificant when individuals lacking awareness of security measures are excluded. Consequently, awareness of vulnerabilities no longer has a significant impact on the probability of becoming a victim of data offenses, or even of cybercrime in general.

Possible explanations for the rejection of hypotheses 2-4 could be:

(1) Timing issues: guardianship could have been established after victimization. The authors did not measure whether respondents engaged in prevention or avoidance behaviors before or after being victimized by any of the above crime types. For example, it is possible that respondents used antivirus software only after experiencing a malware infection, which would be a classic ‘false positive’ because the guardian was not in place during the attack.

(2) False sense of security and exposure: Guardianship may have led to a false sense of security or greater exposure of the individual believing it can detect an attack, thus increasing vulnerability. Also, guardianship often provides functionality to notify the user of attacks. Depending on the configuration, different users may receive different levels and numbers of alerts. In particular, increasing IT knowledge (both from work and personal interest) may correlate with this false sense of exposure.

(3) Complex relationship between knowledge and behavior (e. g. privacy paradox): A possible explanation may also lie in the complex relationship between knowledge and behavior. Physical and personal protection are related, but it is a complex relationship. For example, Zwilling et al. (2022) showed that some cybersecurity awareness led to minimal protective measures, such as installing antivirus software, but had no effect on users’ willingness to share personal information. Lee and Chua (2023) concluded: “Due to the complexities and differences in definitions, the role of cybersecurity and cybercrime knowledge and awareness in one’s behavior and intention remains diverse and dependent on specific issues.“ (Lee & Chua, 2023).

(4) Greater workplace experience and interest in IT facilitate the identification of cybercriminal acts: Experience in IT increases awareness, which in turn may make it easier to identify actual or perceived attacks. A person with less IT experience may simply not recognize potential cybercrime as such. This discrepancy is revealed when the differences between the first and second regression models are examined. When individuals lacking

knowledge of security measures are excluded from the sample, the positive correlation between the probability of victimization by certain types of offenses and the presence of security measures, as well as the awareness of vulnerabilities, becomes insignificant.
(5) Success of the attack: A major challenge is the definition of victimization, as it does not distinguish between a successful and an unsuccessful attack. Thus, although the guardianship may do its job and prevent a successful attack, it lists the attack and increases the user's perception of victimization.
(6) Security level of devices: We need to further investigate the number and type of devices owned by the participants. On the one hand, a higher number of devices increases the attack surface and thus the number of victimizations. There may be a correlation with income, education, and IT skills. On the other hand, the data does not focus on traditional IT, but also includes smart home devices (Sauter & Treytl, 2023). No data were collected on the security level of these devices, which obscures a possible influence (Sasi et al., 2023). However, it is known that the architecture of such devices (and IoT devices in general) makes them more vulnerable to attacks (Sauter & Treytl, 2023).

8. Conclusion

Based on the present study, it can be concluded that although the Routine-Activity Theory (RAT) can be adapted to cybercrime as a field of investigation, it comes with some challenges. In particular, the notion of guardianship faces a diverse field of IT-related security measures, ranging from preventive to reactive measures, from systems operating in the background to those requiring recurring involvement. Further studies can take these specifics into account. As explained at the beginning, this method of collecting data on unreported crime has strengths and limitations. This is particularly evident in the decision to include incidents of cybercrime, in which people were not sure whether they had been victimized. This approach facilitates a more comprehensive and nuanced portrayal of cybercrime victimization, as such incidents frequently occur unconsciously. Conversely, this approach is subject to bias due to individuals who misreported cybercrime incidents. In an attempt to counteract this potential bias, a secondary calculation was devised, excluding individuals deemed most likely to have misreported, thereby ensuring a more accurate depiction of cybercrime victimization (see also section 6 Table 4).

Thus, the study provided insights into how guardianship affects victimization by different forms of cybercrime.

We have shown that the term “cybercrime“ encompasses very heterogeneous forms of crime, ranging from financial to data to personal offenses. Lumping these types of crimes under the umbrella of cybercrime in general would obscure interesting differences between the victims of such crimes. This finding is not new, as Bossler and Holt (2010) have already criticized this lack of granularity in categorization. “Thus, simply collapsing victimization into categories may miss important differences” (Bossler & Holt 2010, p. 234).

In line with this, this paper contributes to the ongoing academic debate on cybercrime victimization by demonstrating that the lack of clear definitions is an obstacle to proper analysis. While public crime reports often refer to a single characteristic of cybercrime, a clear distinction between the different offenses is needed to develop a targeted prevention strategy. This raises the question of whether a traditional view and statistical count of cybercrime cases is still appropriate. With AI, Crime-as-a-Service and other new forms of attacks and new criminal business models, as well as the adaptation of countermeasures and protection, we believe that the categorization of crimes should focus on the target (financial, data, personal), which better fits the victims' perspective than technical definitions.

In addition, an interesting finding of the study is that increased knowledge in terms of experience or additional cybersecurity measures does not necessarily lead to less successful cyberattacks. Whilst the RAT theory is well-suited to the issue under discussion in the present paper, further research using other theoretical concepts is required to more closely investigate the connection between perceived victimization and guardianship or awareness measures. This might include the concept of lifestyles according to Pierre Bourdieu or the Sinus-Milieus, in order to consider milieu-specific components of cybercrime (Bourdieu, 1987).

Nevertheless, this finding should encourage to scrutinize common security approaches: companies are currently investing significant amounts of money in employee awareness and training. The question is, is it justified? There is no doubt that a basic knowledge of IT security helps to create a certain level of awareness in this area and to better recognize potential criminal threats. However, security awareness or knowledge alone is not enough, both technically and in terms of accountability, and needs to be complemented by other measures. The challenge for the future is to find ways to reduce the number of successful cybercrime attacks through security technology and regulation. Considering recent technological developments, such as the Internet of Things (IoT), which is inundating our work and personal environments with information technology and more sophisticated and automated attacks, the future of cybersecurity lies in better and more flexible extension of IT security, with the goal of countering the individualization of cybersecurity responsibility at the expense of the end user.

References

Bergmann, M.C., Dreißigacker, A., von Skarczinski, B., Wollinger, G.R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? *Cyberpsychol Behav Soc Netw, 21*(2), 84-90. doi: 10.1089/cyber.2016.0727. Epub 2017 Jun 28. PMID: 28657785

Bossler, A. M., Holt, T. J. (2010). The Effect of Self-Control on Victimisation in the Cyberworld. *Journal of Criminal Justice, 38* (3), 227–236. https://doi.org/10.1016/j.jcrimjus.2010.03.001

Bossler, A. M., Holt, T. J. (2011). Malware victimisation: A routine activities framework. *Cyber criminology, 3*(1), 317–346.

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

BMI Österreich, Bundeskriminalamt. (2023). Angezeigte Fälle von Cybercrime (gesamt) in Österreich von 2004 bis 2022 Statista. https://de-1statista-1com-1a7xmh7kd0100.han3.donau-uni.ac.at/statistik/daten/studie/294141/umfrage/cybercrime-in-oesterreich/

(Abrufdatum: 27.11.2023).

Bourdieu, P. (1987). *Die feinen Unterschiede. Kritik der gesellschaftlichen Urteilskraft.* Suhrkamp.

Burnes, D., DeLiema, M., Langton, L. (2020). Risk and protective factors of identity theft victimisation in the United States. *Preventive Medicine Reports, 17,* 1–8. https://doi.org/10.1016/j.pmedr.2020.101058

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

Cohen L. E., Felson M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.4324/9781439817803-12

Dodel, M., Mesch, G. (2017). Cyber-victimisation preventive behavior: A health belief model approach. *Computers in Human Behavior, 68,* 359–367. https://doi.org/10.1016/j.chb.2016.11.044.

Dreißigacker, A.; Riesner L. (2018*). Private Internetnutzung und Erfahrung mit computerbezogener Kriminalität. Ergebnisse der Dunkelfeldstudien des Landeskriminalamtes Schleswig-Holstein 2015-2017. F*orschungsbericht Nr. 139. Kriminologisches Forschungsinstitut Niedersachsen e.V.

Enisa, European Union Agency for Cybersecurity. 2022. ENISA Threat Landscape NOVEMBER 2022. doi:10.2824/764318

Furnell, S. (2001). The Problem of Categorising Cybercrime and Cybercriminals. Second Australian Information Warfare and Security Conference 2001. *Journal of Information Warfare, 1*(2), 35–44. https://www.jstor.org/stable/26486092

Furnell, S. (2021). Categorising Cybercrime and Cybercriminals: The Problem and How It Has Changed. *Journal of Information Warfare, 20*(4), 68–76.

Gordon, S., Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2,* 13–20.

Graham, R., Triplett, R. (2017). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimisation. *Deviant Behavior, 38*(12), 1371–1382. https://doi.org/10.1080/01639625.2016.1254980

Graves, J. T., Acquisti, A., Anderson, R. (2019). PERCEPTION VERSUS PUNISHMENT IN CYBERCRIME. *The Journal of Criminal Law & Criminology, 109*(2), 313-363.

Holt, T. J., Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimisation. *Deviant Behavior, 30*(1), 1-25. https://doi.org/10.1080/01639620701876577

Huber, E.; Brandtweiner, R. (2020). Cyberstalking: The New Threat on the Internet. *Encyclopedia of Criminal Activities and the Deep Web, 628-639.* IGI Global.

Huber, E., Pospisil, B., Seböck, W. (2019). Without a trace: Cybercrime, who are the defendants? *Magdeburger Journal zur Sicherheitsforschung, 17,* 938–948.

INTEGRAL. (2021). Begleitende Eigenforschung zur Internetnutzung 2020 und 2021, Methode: 2020/2021: 4.000 CAPI und 2.000 CATI, rep. Österr. ab 14 Jahren.

Kang, R., Dabbish, L, Fruchter, N., Kiesler, S. (2015). “My data just goes everywhere:” User mental models of the internet and implications for privacy and security. *Symposium on Usable Privacy and Security,* 39-52.

Kirwan, G., Power, A. (2013). *Cybercrime: The Psychology of Online Offenders.* Cambridge University Press.

Lee, C. S., & Wang, Y. (2022). Typology of Cybercrime Victimisation in Europe: A Multilevel Latent Class Analysis. *Crime & Delinquency. 70*(4). https://doi-1org-102zvpj9b03fc.han3.donau-uni.ac.at/10.1177/00111287221118880

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

Leukfeldt, E. R., Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263–280. doi: 10.1080/01639625.2015.1012409

Leukfeldt E. R., Holt T. J. (2020). Examining the social organization practices of cybercriminals in the Netherlands online and offline. *International Journal of Offender Therapy and Comparative Criminology, 64*(5), 522–538. https://doi.org/10.1177/0306624x19895886

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimisation for high school seniors. *International Journal of Cyber Criminology, 2*(2), 346-67.

McGuire, M., Dowling, S. (2013). *Cyber crime: A review of the evidence.* Research Report 75. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf (Abrufdatum: 03.12.2018).

Mikkola, M., et al. (2020). Situational and Individual Risk Factors for Cybercrime Victimisation in a Cross-national Context. *International Journal of Offender Therapy and Comparative Criminology*. 0 (0) https://doi-1org-102zvpj9b03ed.han3.donau-uni.ac.at/10.1177/0306624X20981041

Müller, P., Dreissigacker, A. & Isenhardt, A. (2022). *Cybercrime gegen Privatpersonen - Ergebnisse einer repräsentativen Bevölkerungsbefragung in Niedersachsen*. Forschungsbericht 168.

Newman G. R., Clarke R. V. (2003). *Superhighway robbery: Preventing E-commerce crime*. Willan.

Ngo, F. T., & Jaishankar, K. (2017). Commemorating a decade in existence of the International Journal of Cyber Criminology: A research agenda to advance the scholarship on cyber crime. *International Journal of Cyber Criminology, 11*(1), 1. doi: 10.5281/zenodo.495762

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimisation: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology, 5*(1), 773-793.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07),* 156b-156b. IEEE. doi: 10.1109/HICSS.2007.206

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *ForensicSci., 2*(2), 379–398. https://doi.org/ 10.3390/forensicsci2020028

Redmiles, E. M., Malone, A. R., Mazurek, M. L. (2016). I think they're trying to tell me something: Advice sources and selection for digital security, Conference session, *IEEE Symposium on Security and Privacy (SP),* 272–288.

Reyns B. W. (2013). Online routines and identity theft victimisation: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216–238.

Sasi, T., Habibi Lashkari A., Lu R., Xiong P., Iqbal S. (2023). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence*. https://doi.org/10.1016/j.jiixd.2023.12.001

Sauter, T., Treytl, A. (2023). IoT-Enabled Sensors in Automation Systems and Their Security Challenges. *IEEE Sensors Letters, 7(12)*~~,~~ doi: 10.1109/LSENS.2023.3332404

Statistik Austria. (2024). Verbreitung der Internet- und E-Commerce-Nutzung in Österreich von 2002 bis 2024. *In Statista*. https://de.statista.com/statistik/daten/studie/298233/umfrage/eckdaten-zur-internetnutzung-in-oesterreich/ (Abrufdatum:25.01.2025).

Thomas, D., Loader, B. (2000). *Introduction Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. Routledge.

United Nations. (2000). Crimes related to computer networks. Report of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf (Abrufdatum:06.12.2018).

Van de Weijer, S., Leukfeldt, R. & Van der Zee, S. (2020). Reporting cybercrime victimisation: Determinants, motives, and previous experiences. *Policing: An International Journal of Police Strategies & Management, 43*(1), 17-34.

Varghese, G. (2016). A sociological study of different types of cyber crime. *International Journal of Social Science and Humanities Research, 4*(4), 599-607.

Weber, C., Wührl, J. M. (2023). Opfererfahrungen im Internet – Ergebnisse des Deutschen Viktimisierungssurvey (DVS). Rüdiger, TG., Bayerl, P.S. (eds). *Handbuch Cyberkriminologie 2. Cyberkriminologie – Theorien, Methoden, Erscheinungsformen*. Springer VS. https://doi.org/10.1007/978-3-658-35442-8_44

Wilson, C. 2008. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service – Report for Congress. https://fas.org/sgp/crs/terror/RL32114.pdf (Abrufdatum: 03.12.2018).

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

Zwilling, M., Klien, G., Lesjak, D., Wilchetek, L, Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Kontakt | Contact

Edith Huber | Universität für Weiterbildung Krems | Head of Research Office und Department für Sicherheitsforschung | edith.huber@donau-uni.ac.at

Bettina Pospisil | Universität für Weiterbildung Krems | Department für Sicherheitsforschung| bettina.pospisil@donau-uni.ac.at

Thilo Sauter | Universität für Weiterbildung Krems | Department für Integrierte Sensorsysteme | thilo.sauter@donau-uni.ac.at

Albert Treytl | Universität für Weiterbildung Krems | Department für Integrierte Sensorsysteme | albert.treytl@donau-uni.ac.at