sustainability

MDPI

Article

Country Life in the Digital Era: Comparison of Technology Use and Cybercrime Victimization between Residents of Rural and Urban Environments in Slovenia

Igor Bernik *, Kaja Prislan and Anže Mihelič

Faculty of Criminal Justice and Security, University of Maribor, Kotnikova 8, 1000 Ljubljana, Slovenia
* Correspondence: igor.bernik@um.si

Abstract: Cybercrime is one of the most significant security challenges of the 21st century. However, official statistics do not provide insights into its prevalence and nature. Representative cross-sectional field studies may help fill this gap, focusing on differences between urban and rural technology users. We (a) investigated the association between the purpose of computers and other electronic device usage and perceived vulnerability, (b) compared the differences in the purpose of computers or other electronic device use and perceived vulnerability, and (c) compared the perceived cyber victimization between residents of rural and urban areas. We conducted a field study that resulted in a representative sample of the Republic of Slovenia in Europe. We found several significant differences in the purpose of technology use and perceived cyber victimization. Furthermore, the results indicate that the purpose of technology use is somehow associated with perceived vulnerability in cyberspace; however, such associations are different in cyberspace than in the material world.

Keywords: cyber victimization; cybercrime; rural environment; technology use; perceived vulnerability

Citation: Bernik, I.; Prislan, K.; Mihelič, A. Country Life in the Digital Era: Comparison of Technology Use and Cybercrime Victimization between Residents of Rural and Urban Environments in Slovenia. *Sustainability* **2022**, *14*, 14487. https://doi.org/10.3390/su142114487

Academic Editor: Zubair Baig

Received: 29 September 2022
Accepted: 1 November 2022
Published: 4 November 2022

1. Introduction

Over the past few decades, the growth of the Internet has led to the increasing engagement of people in cyberspace, which has significantly impacted many aspects of our society. Daily lives, fundamental rights, social interactions, and economies became critically dependent on information and communication technology (ICT) working seamlessly. Being continuously online became the new norm for many people, often without even being aware. That created a broader attack surface and exposed multiple areas of peoples' lives for criminals to exploit [1]. Cybercrime has become one of the fastest-growing forms of criminality [2], representing a serious threat to cyberspace users, economics, and national security. However, it should be acknowledged that the traditional dynamic between the victim and the offender is different in cyberspace. In cyberspace, an offender and a multitude of targets are brought together, independent of space and time. That means the simultaneous presence of all three elements needed for a crime to occur (i.e., motivated offender, potential victim, absence of guardians) is a constant feature of cyberspace [3–6]. For such reasons, the risks for online victimization are deemed greater than in the physical world [7], while studies also indicate that people experience greater fear of crime in cyberspace than in the physical environment [8,9].

Cybercrime is thus one of the most significant security challenges of the 21st century, which is why cybersecurity and defense became a core of most national and international security strategies [10]. However, there are several issues related to the prevention of and response to cybercrime. Firstly, cybercrime has become exceptionally technologically advanced, and organized with perpetrators using increasingly sophisticated methods, which is why many incidents are hard to detect [1,11,12]. Secondly, perpetrators are hard to identify and prosecute due to their anonymity and the global nature of cyberspace [1,13]. Thirdly, cyber threats are constantly evolving, making it hard to follow development trends

in terms of security technologies [14,15]. Lastly, there is a high diversity in the security of cyberspace users. Different online behaviors, levels of threat awareness, attitudes, and knowledge of protective measures against cybercrime are observed among users, leading to high variability in cybercrime victimization [16–18].

In line with these challenges, it is difficult to assess the actual prevalence of cybercrime and the state of cyber victimization. Due to the low percentage of reported and investigated cybercrime, official statistics are unrepresentative [19,20]. This has created a need for acquiring a more in-depth understanding of how widespread cybercrime actually is, and what are the differences in victimization experiences among different types of cyberspace users.

As a result, cybercrime victimization has become a widespread research topic among scholars in the field of cybersecurity. Victimization studies can help address the problems associated with the existing dark field in the field of cybercrime and the investigation of factors leading to victimization. To date, many cybercrime victimization studies have been conducted, with an aim to explore the prevalence of different types of cybercrimes and factors predicting victimization. Overall, it is estimated that the majority of users fall victim to some form of cybercrime [21–23], with malware and fraudulent activities being the most common [18,23,24]. In terms of predictors, self-protective behavior (related to users' threat and risk perception, their perceptions and attitudes towards security technologies) [25,26], online activities [27–29], psychological traits [30–32], and socio-demographic characteristics [33,34] were established to have a significant influence on cybercrime victimization.

However, cybercrime victimization studies have their limitations. For example, a comparison of such studies indicates that findings regarding the prevalence of cybercrime are different, and that victimization can vary in relation to different threats and users. Due to different methods, studies are also difficult to compare, and national and representative samples are rarely provided [35]. Victimization studies mainly rely on self-reported experience from users, and tend to neglect the fact that some users find it difficult to detect certain threats or do not even know that they have been victimized [24,36,37]. Although perceived vulnerability could be used for the estimation of users' bias in reporting, the connection between perceived vulnerability and perceived victimization has not been investigated yet. Moreover, victimization studies tend to focus on a specific user population or only on specific threats, leaving victimization related to different cyber threats across the general user population under-researched. Moreover, certain factors (e.g., perceived vulnerability, perceived severity) associated with cyber victimization are (over)extensively investigated, while others (e.g., purpose of computer or other electronic device use, residence area) remain under-researched.

For example, several studies so far found that cybercrime victimization varies across countries [21,38,39], and is associated with users' online behavior [28,29,40]. Despite literature indicating that differences among users from different local settings exist in relation to the use of ICT, online behavior, computer skills, and cybersecurity awareness [17,23,39], only few studies so far investigated the influence of environmental settings on cybercrime victimization and victimization-related factors. Although a comparative and geographically oriented approach to the study of security and crime has become popular in criminology, the main focus of studies is primarily the urban environment. For this reason, security phenomena in rural areas are unexplored and somewhat neglected in criminological studies, and are still trivialized and marginalized [41]. Hence, similar knowledge gaps are observable for cybercrime studies as well.

2. Cybercrime Victimization

Cybercrime, which is referred to as criminal acts that are committed online by using electronic communications networks and information systems [42], has been steadily increasing in its prevalence and impact [43,44]. Current trends suggest that there is a considerable increase in the scope of incidents, the sophistication of threats, the number of victims, and damage related to cybercrime. Moreover, it is estimated that cybercrime

has exceeded the prevalence of conventional crime forms, with individual cybercrime victimization being significantly problematic and widespread [38].

Despite general estimations showing that more than 1 million people worldwide fall victim to cybercrime, there is still a lack of reliable figures [1]. Due to the low level of reporting, official statistics portray an unreliable picture of cybercrime [20,37,45], which indicates an extensive dark field of crime. To address the issue of underreporting and unreliable official estimates, cybercrime victimization studies are being increasingly conducted. However, the findings of such studies point to a high variability of victimization across countries and in relation to different types of victims and cyber threats.

On one hand, the findings of several cybercrime victimization studies show that different types of harassment, abuse, and attacks related to the use of cyberspace and ICT have been experienced by the majority (up to 80 percent) of all cyberspace users [22,46,47]. On the other hand, some statistics portray a significantly different situation, reporting a much lower victimization rate among Internet users (less than 40 percent) [48]. Moreover, some cyber threats are deemed as much more prevalent than others. A European Union (EU)-wide study on cybersecurity, for example, showed that the most common cyber threats experienced by respondents are fraudulent e-mails or phone calls (36 percent) and infections with malicious software (28 percent) [39]. The types of cybercrime that were recognized as the most common in the victimization study performed by Drew [18] were phishing (51.8 percent), unauthorized card/bank account use (50.3 percent), and malware/ransomware (50.2 percent). The least perceived prevalence was reported for romance scams (11.5 percent) and computer hacking (10.9 percent). In their victimization study, Ref. [49] found that the most prevalent cyber threats experienced among individual users are computer viruses (57.8 percent) and e-mail harassment (23.5 percent). Such differences in reported findings were observed by Ref. [35] as well, who conducted a metanalysis of nine cyber victimization studies. The analysis showed that users most often reported being victims of hacking and malicious software (up to 6 percent and 15 percent, respectively) and less often of other types of fraud (less than 1 percent), while annual cybercrime prevalence rates ranged from 1 to 3 percent for online shopping frauds, online banking/payment frauds, and online bullying. Despite the observed differences, the findings of victimization studies generally indicate that malware (including ransomware) and fraudulent activities such as phishing and scams could be deemed as the most prevalent trends in individual victimization.

Differences in the victimization studies' findings are related to various factors. However, it should be considered that due to the sophistication of many cyber threats, victimization with some cyber threats is difficult to detect. Hence, the findings of self-reported victimization are subject to certain errors. For example, EU and worldwide studies found that certain cyber threats were more prevalent when respondents were asked whether they know someone who has been a victim, compared to their actual experience with such threats [21,48]. Another such example is phishing-related victimization. Although users generally report a relatively high prevalence of victimization related to phishing (e.g., an Australian national survey revealed that 34 percent of users were exposed to phishing scams [50]), real-world studies portray an even more detrimental picture. Experiments investigating users' susceptibility to phishing attacks show that the majority of participants (up to 97 percent) respond to fraudulent messages by disclosing personal information [36,51,52]. Hence, problems associated with establishing the actual victimization based on self-reported studies have led to the increase in studies investigating users' perceptions of their susceptibility to victimization (i.e., perceived vulnerability). Compared to self-reported victimization, such studies provide an insight into users' beliefs about the prevalence and dangers associated with cyber threats. For instance, when comparing self-reported victimization and perceived vulnerability, it could be observed that users' concern of becoming a victim of a certain cybercrime is higher in comparison with their actual experience with such a crime [39].

In the exploration of cybercrime, many researchers have also focused on studying factors predicting victimization. The findings reveal that users' demographic characteristics (such as age, gender, ethnic origin, social status, employment), online (deviant) behavior, and their past experience with victimization predict victimization in cyberspace [53–56]. Moreover, it was also found by several studies that victims' characteristics differ according to the type of cyber threat [29,57–59]. In addition, users' psychological and behavioral traits (e.g., low self-control) were also confirmed to have a significant impact [32]. Furthermore, online habits and the purpose of ICT use, as well as users' attitudes about threats and security measures which affect their self-protective behavior, are important for explaining cybercrime victimization [18,25,28,60,61].

Based on the review of past research, we can conclude that cybercrime victimization differs both in terms of the type of threats and the type of users. There are many different factors associated with victimization experience, with behaviors and attitudes playing a significant role. Moreover, it is also important to note that differences are observed in relation to the environmental settings of users. This indicates the possible influence of users' environment on cybercrime victimization. Although it was already established that victimization varies across macro environmental settings (i.e., country and culture), micro/local-level influence (i.e., rural and urban settings), which proved to be an important element in crime studies in general, remains under-researched in cybercrime literature.

3. Cybervictimization in Rural and Urban Areas

It is widely acknowledged that urban and rural environments are not exposed to crime in the same manner and extent. A review of statistical reports shows differences in crime rates, with urban environments being characterized by different patterns than rural. Study findings indicate that cities with a larger population generally have higher crime rates than suburban or rural cities [62]. A longitudinal analysis of the United States crime victimization survey showed that violent crimes (such as aggravated assaults, rapes and sexual assaults, robberies) are significantly higher in urban than in rural areas [63]. Moreover, it was also found that serious violent victimization has decreased significantly more in urban areas, while the decline in simpler crimes is similar for both areas. A similar higher occurrence of violent and serious crimes in urban areas is typical for the United Kingdom as well [64]. Other studies exploring crime statistics in relation to environmental settings also showed that the number of crimes in rural areas is significantly lower than in urban areas [65,66].

Despite generally lower crime rates, rural environments are characterized by a higher rate of certain types of crime (e.g., domestic violence) [62], which contradicts established beliefs about the impact of population density on crime. Therefore, rurality as such is not a "constant" predictor of crime rates [66]. It is also important to note that the fear of crime in rural areas is increasing and that problems due to social circumstances are more often unreported, which means that official statistics are not highly reliable [41].

Since the same patterns of crime do not apply in both rural and urban areas, more rural-focused research is needed [67]. It is important to facilitate research to provide for an in-depth understanding of such disparity and the potential influences of environmental settings on crime and victimization trends. In initial research, such differences were attributed almost exclusively to the population density and the supply of crime opportunities [68]. While differences in crime rates may be related to population size, they may also be caused by other local factors [62]. It is important to understand that urban and rural areas are different in several aspects, which in combination, lead to a complex dynamic of factors associated with crime and victimization.

Currently, more than 44 percent of the world population resides in rural environments [69]. However, with respect to crime and victimization, rural communities, especially compared to urban ones, are poorly documented. Past criminological studies scarcely focused on investigating crime in rural areas [66], and for this reason, a new

branch of criminology called rural criminology has been increasingly developing in the past decades [67,70].

The lack of studies is also noticeable in the field of cybercrime and user victimization. Although such differences may not seem significant due to the global nature of cyberspace, certain studies in the field of cybersecurity and user awareness have already indicated potential differences between users from different environments (e.g., [71]), which could imply that differences between different types of local communities also exist.

For instance, studies show that cybercrime victimization rates among individual users are higher in countries with lower levels of development [38]. Symantec [72] reported that The Netherlands had the lowest cybercrime rate (14 percent of the population were affected), while Indonesia was subject to the highest cybercrime rate in the world. In relation to local environments, a Europe-wide study found that disparities are observable in Internet access and usage. Those living in large towns are more likely to use the Internet daily compared to respondents living in rural villages. Furthermore, discrepancies were seen for users' awareness as well; the more urbanized a respondent's environment, the more likely they are to be aware of official means to report and react to cybercrime [39]. Differences among respondents from different local environments were observed by a study investigating fear of identity-related cybercrimes [73].

The impact of users' location on cybercrime victimization remains under-researched. Only a handful of studies have addressed this topic. The findings of a study conducted by Al-Ali [25] revealed that the place of users' residence was associated with cybercrime victimization. In their study, Chang et al. [17] found that parents living in rural areas had lower levels of Internet skills and intervened less in their children's use of the Internet compared to parents living in urban areas. Adolescents who live in rural areas have lower levels of Internet literacy but a higher frequency of Internet use, and they also engage in riskier online behaviors and are more often victimized. Overall, they found a clear difference between rural and urban parents and adolescents, with both rural parents and their children being less experienced and knowledgeable of the risks associated with use of the Internet. Similar findings were confirmed by a cyberbullying victimization study conducted by [23], which found that the highest prevalence of victimization exists among urban female respondents. Rural community residence was associated negatively with problem-solving and coping capabilities and with a lower likelihood of coping abilities.

4. Motivation

Despite different available sources of data on cybercrime, current statistics are still insufficient and fragmented. Official statistics do not provide insights into the actual widespread and nature of cybercrime [1]. Although several scientific studies focused on identifying factors predicting cybercrime victimization, certain factors remain less or completely unexplored. Firstly, there is a lack of studies investigating the role of the local environment, the purpose of ICT use, and the perceived users' vulnerability with cybercrime victimization. The importance of the factors mentioned above could be deemed as follows. Despite cybercrime being regarded as a "borderless problem" [42], several circumstances indicate possibilities of their associations with users' local environment. Studies investigating traditional victimization confirmed that differences between crime rates, victimization, and fear of crime are common among rural and urban environments [74]. Cybercrime-related studies also pointed to differences between users from different urbanized environments regarding their security behaviors, ICT usage, and computer/digital skills. Secondly, the purpose of ICT use and users' online behavioral practices have already been established as significant victimization predictors [25]. However, to the best of our knowledge, the associations between local environment, online behavior, and victimization have not been explored. Thirdly, the role of perceived vulnerability in perceived victimization and differences in perceived vulnerability to cyber threats among users from different environmental settings has not been considered in past victimization studies. Fourthly, most victimization studies focus on studying specific types of cybercrime (e.g., cybergrooming, cyberbullying,

cyber-harassment, cyberstalking, online frauds, social engineering, phishing). Although some research already established that the level of victimization varies according to the type of cyber threat [18,49], there is a lack of more comprehensive studies that would include an overview of victimization with different cybercrime types. Lastly, there are few well-performed randomized sampled studies on cybercrime among the general population [35].

To address the aforementioned issues and knowledge gaps in the existing literature, we (a) investigated the association between the purpose of computers and other electronic device usage and perceived vulnerability, (b) compared the differences in the purpose of computers or other electronic device use and perceived vulnerability, and (c) compared the perceived cyber victimization between residents of rural and urban areas. Therefore, this paper answers the following research questions.

RQ1 Is there an association between the purpose of computers and other electronic device usage and the perceived cybercrime vulnerability?

RQ2 Are there differences in computer and other electronic device usage and perceived cybercrime vulnerability and victimization between urban and rural residents?

RQ3 Are there differences between residents of urban and rural areas in perceived cybercrime victimization?

5. Materials and Methods

To answer the research questions, we conducted a national randomized sample field study. The data were collected with a survey. The following subsections describe the questionnaire development and the data collection procedure.

5.1. Questionnaire Development

The questionnaire was designed to measure three key constructs of cybercrime. The first construct was focused on the diversity of respondents' purposes for using computer and other electronic devices ("*Purpose of use*"—PurUse), the second construct measured the perceived cybercrime vulnerability through various online activities ("*Perceived vulnerability*"—PerVul), and the third construct measured the perceived cybercrime victimization ("*Perceived victimization*"—PerVic). Indicators of the first two constructs were measured on a five-point Likert-type frequency scale from 1 ("*Never*") to 5 ("*Always*"), and from 1 ("*Very unlikely*") to 5 ("*Very likely*"), respectively. Indicators of the third construct were measured on a categorical scale ("*Never*", "*Once*", "*Twice or more*"). Respondents had the option not to provide an answer to any of the questions if they were not able or unwilling to respond.

Indicators of the construct *Purpose of use* were selected based on the most common usage patterns among the general population, while indicators of the construct *Perceived vulnerability* were selected based on the most frequent activities in cyberspace. Types of cybercrime in the construct *Perceived victimization* were defined based on the ease of recognition among users, while technically more sophisticated threats were avoided due to their concealed nature.

Control variables included time spent on the Internet for different purposes and demographic variables (e.g., age, gender, area of residency, level of education, employment status). In total, the questionnaire included 44 different variables (*Purpose of use* (12), *Perceived vulnerability* (11), and *Perceived victimization* (21)) and 10 control variables. The questionnaire was developed by one researcher in the Slovenian language and reviewed by several researchers from the program group Security and Safety in Local Communities (hereafter program group). A physical survey was prepared once consensus was reached among researchers regarding the clarity and validity of the questionnaire.

5.2. Data Collection

To collect data from a representative sample of the targeted population (citizens of the Republic of Slovenia), the questionnaire was distributed physically in all geographic areas in 24 municipalities in Slovenia by 43 researchers of the program group and students in the spring of 2017. Sampling was performed as follows. First, within each of the eight police

directorates in Slovenia, we chose three municipalities (one large, one medium, and one small). Second, the respondents were randomly selected in a manner that ensured sample representativeness according to the size of the municipality in terms of gender and age of the population. The geographical distribution of the survey is presented in Figure 1.

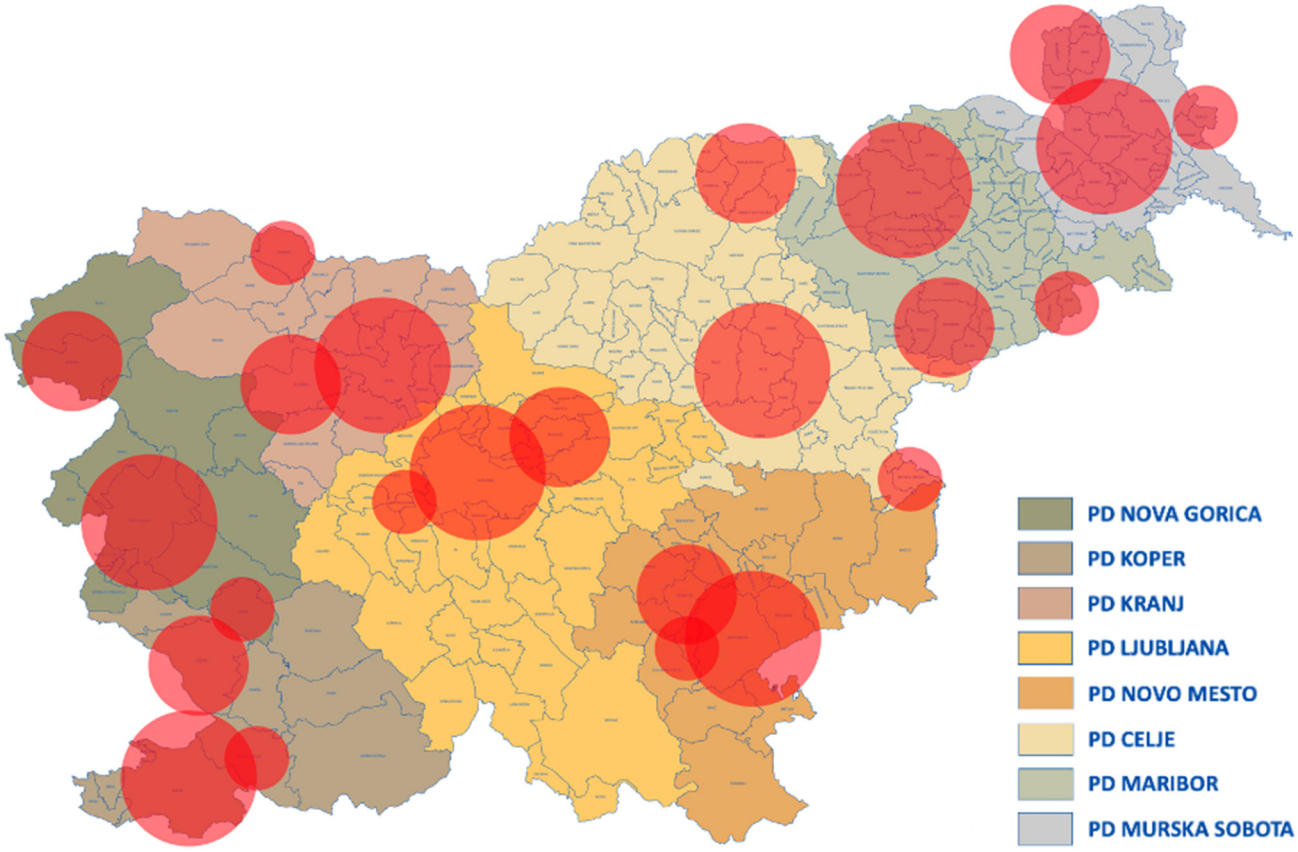

Figure 1. Graphical representation of geographical questionnaire distribution (PD—police directorate).

A total of 1266 respondents completed the survey. The share of missing values per variable ranged from 2.5 to 20.4 percent, with 4.3 percent of missing values in a complete dataset. Due to an average of 38 percent of missing values in social sciences (Dodeen, 2018), we concluded that reaching into a dataset was not necessary. The demographic data of the respondents are presented in Table 1.

Because the respondents were asked to share sensitive information with the researchers (e.g., the amount of income in comparison to average income in Slovenia), safeguards were used to encourage honest responses. First, respondents were informed about the anonymity and voluntariness of their participation. Second, the respondents were assured that the results would be presented in an aggregated form. Finally, to ensure anonymity, respondents were explicitly asked not to sign the questionnaire or write any other identification data on the survey sheets.

Table 1. Demographic data of the survey respondents.

Variable		Frequency	Share (%)
Gender	Female	668	52.8
	Male	596	47.1
	Not specified	2	0.2
Age	18–30	273	21.6
	31–45	344	27.2
	46–60	334	26.4
	61–	313	24.7
	Not specified	2	0.2
Education	Elementary school (not finished)	11	0.9
	Elementary school (finished)	159	12.6
	High school	587	46.7
	2-year college	131	10.3
	University degree	291	23
	Specialization, master's degree	61	4.8
	Doctorate	16	1.3
	Not specified	10	0.8
Status	Employed in the industry	349	27.6
	Employed (not in the industry)	289	22.8
	Self-employed	76	6
	Farmer/Housewife	16	1.3
	Retired	311	24.6
	Student	157	12.4
	Unemployed	53	4.2
	Other	11	0.9
	Not specified	4	0.3
Size of the residence area	Village or settlement with school, post office, shop	541	42.7
	Suburb or town	712	56.3
	Not specified	13	1

5.3. Instrument Validation

This study aimed to explore the current state of the perceived cybercrime victimization, perceived cybercrime vulnerability, and the purpose for which computers and other electronic devices are used among residents of rural and urban areas. The mentioned constructs were modeled as formative. Therefore, we did not perform reliability analysis, as suggested by Coltman et al. (2008). To answer the research questions, we tested both constructs measured with a Likert-type scale (*Purpose of use* and *Perceived vulnerability*) if the data have an approximately normal distribution for skewness and kurtosis, following the procedure suggested by [75]. Absolute values for skewness and kurtosis (suggested measure for samples larger than n = 300) range between −0.32 and 1.41, and between −1.59 and 1.41, respectively. Thus, we assume the data are approximately normally distributed across all variables. Additionally, assumptions for an independent sample *t*-test and simple linear regression analysis (i.e., equality of variances, homoscedasticity, linearity, and normality of the residual errors) were carefully considered.

6. Results

To answer the first research question (RQ1), we performed a simple linear regression analysis and robust regression. Table 2 summarizes the results of descriptive statistics (means, standard deviations, and one sample *t*-test significance levels), while Table 3 summarizes the results of linear and robust regressions, where *purpose of technology use* is considered as a predictor and *perceived vulnerability* as a dependent variable.

Table 2. Results of descriptive statistics (***—$p < 0.001$, **—$p < 0.005$, *—$p < 0.05$ (one-sample *t*-test, reference value = 3).

Activity	PurUse		PerVul	
	Mean	**SD**	**Mean**	**SD**
accessing social networks	2.89 ***	1.38	3.40 *	1.19
online banking	2.44 ***	1.48	3.16 ***	1.25
online shopping	2.15 ***	1.19	3.31 ***	1.19
web browsing	3.32 **	1.33	3.11 ***	1.18
downloading music and video content	2.32 ***	1.34	3.18 ***	1.26
e-mail exchange	3.16 ***	1.40	3.12 ***	1.15
data analysis	2.22 ***	1.27	2.71 ***	1.17
gaming	1.77 ***	1.07	2.76 ***	1.29
playing music and videos, reading e-books and articles	2.77 ***	1.34	2.61 ***	1.19

Table 3. Results of simple linear regression and robust regression (***—$p < 0.001$, **—$p < 0.005$, *—$p < 0.05$).

Activity	Linear Regression			Robust Regression		
	Std. Error	***t***	R^2	***Beta***	***Std. Error***	***t***
accessing social networks	0.025	5.94	0.029	0.169 ***	0.026	5.53
online banking	0.024	1.20	0.001	0.035	0.026	0.94
online shopping	0.029	1.82	0.003	0.053	0.031	1.10
web browsing	0.025	6.61	0.035	0.187 ***	0.027	6.67
downloading music and video content	0.027	3.47	0.010	0.100 **	0.029	3.21
e-mail exchange	0.023	9.03	0.066	0.257 ***	0.025	8.98
data analysis	0.027	2.14	0.004	0.062 *	0.028	2.24
gaming	0.035	0.85	0.001	0.025	0.038	0.86
playing music and video, reading e-books and articles	0.026	2.03	0.003	0.059 *	0.027	2.11

The descriptive statistics results indicate that respondents are primarily using computers and other electronic devices for web browsing and e-mail exchange, and least for gaming. However, they feel that they are most vulnerable while accessing social networks, online shopping, and using online banking services.

Furthermore, the results of regression models show that the frequency of use can explain up to approximately 7 percent of the variance in perceived vulnerability due to the use of particular software. However, a notable statistically significant association ($p < 0.005$) was found only in four instances (e-mail exchange, downloading music and video content, web browsing, and accessing social networks).

To answer the second research question (RQ2), we performed an independent sample *t*-test. We considered residents living in villages or settlements with schools, post offices, shops as "residents of the rural area" and residents living in suburbs or towns as "residents of the urban area". Table 4 summarizes the results of descriptive statistics separated by the residence area and comparison of means.

The results indicate that in most instances, there is a statistically significant difference in the purpose for which computers and other electronic devices are used between urban and rural residents, except in online banking. The same pattern cannot be seen in perceived cybercrime vulnerability. In most instances, respondents of both groups equally perceive which particular activities can expose them to cyber threats, except for online shopping, online banking, and accessing social networks, where residents of urban areas feel more vulnerable.

Table 4. Results of the independent samples *t*-tests for the purpose of use and perceived cybercrime vulnerability (***—$p < 0.001$, **—$p < 0.005$, *—$p < 0.05$).

Activity	Location	PurUse			PerVul		
		Mean	SD	*t*	Mean	SD	*t*
accessing social networks	rural	2.77	1.40	−2.673 **	3.30	1.21	−2.452 *
	urban	2.98	1.37		3.47	1.17	
online banking	rural	2.34	1.46	−1.867	3.05	1.25	−2.822 **
	urban	2.51	1.50		3.25	1.25	
online shopping	rural	2.08	1.15	−1.977 *	3.17	1.20	−3.667 ***
	urban	2.21	1.21		3.42	1.17	
web browsing	rural	3.13	1.35	−4.449 ***	3.07	1.20	−0.862
	urban	3.47	1.31		3.13	1.17	
downloading music and video content	rural	2.11	1.23	−4.732 ***	3.16	1.27	−0.280
	urban	2.48	1.40		3.18	1.26	
e-mail exchange	rural	2.95	1.39	−4.415 ***	3.11	1.19	−0.432
	urban	3.31	1.39		3.14	1.12	
data analysis	rural	2.06	1.19	−3.721 ***	2.68	1.15	−0.866
	urban	2.34	1.33		2.74	1.19	
gaming	rural	1.66	0.99	−3.272 **	2.78	1.30	0.232
	urban	1.86	1.12		2.76	1.29	
playing music and video, reading e-books and articles	rural	2.56	1.31	−4.796 ***	2.62	1.18	0.169
	urban	2.93	1.34		2.61	1.20	

Since perceived cybercrime victimization was measured on a categorical scale ("*Never*", "*Once*", "*Twice or more*"), we answered the third research question (RQ3) with Pearson's chi-square test of independence. The results given in percentages are summarized in Table 5.

Table 5. Pearson's chi-square test results (***—$p < 0.001$, **—$p < 0.005$, *—$p < 0.05$).

Victimization	Location	Never	Once	Twice or More	Not Specified	χ^2
cyber harassment	rural	71.0	9.1	15.7	4.3	1.48
	urban	68.4	10.8	16.9	3.9	
extortion in cyberspace	rural	86.7	5.0	4.8	3.5	2.87
	urban	89.3	3.2	4.2	3.2	
malware infection	rural	61.9	17.0	17.9	3.1	3.79
	urban	58.0	21.3	17.6	3.1	
impersonation/phishing	rural	79.5	8.9	8.7	3.0	3.95
	urban	75.4	12.1	9.7	2.8	
dissemination of indecent material	rural	81.1	8.5	7.6	2.8	13.49 **
	urban	75.1	7.7	14.2	2.9	
spreading hate speech	rural	76.2	10.7	10.2	3.0	14.66 **
	urban	71.2	8.3	17.6	2.9	
spreading rumors	rural	76.2	10.4	10.7	2.8	17.23 ***
	urban	68.8	9.0	19.2	2.9	
online banking frauds	rural	91.1	2.2	2.4	4.3	2.12
	urban	90.0	3.7	2.4	3.9	
ransomware	rural	90.4	3.5	2.8	3.3	2.24
	urban	91.0	3.4	1.5	4.1	
wireless network interference	rural	81.5	7.9	6.8	3.7	7.65 *
	urban	75.6	10.5	10.3	3.7	

The results show statistically significant differences in perceived cybercrime victimization between residents of rural and urban areas in four out of six forms of victimization. Therefore, residents of urban areas report slightly lower victimization by wireless network interference, spreading rumors and hate speech, and dissemination of indecent material. In other instances, there is no statistically significant difference between both groups of residents.

7. Discussion

Our results (RQ1) demonstrate the partial association between the purpose of technology (computers and other electronic devices) and the perceived vulnerability to cyber threats while using a particular technology. Even though users use technology for online shopping, data analysis, playing music, videos, and reading e-books and articles, its use

does not statistically significantly predict their perceived vulnerability to cyber threats during these activities. On the other hand, their use of social networks, online banking, web browsing, downloading music, video content, emailing, and gaming can predict their perceived vulnerability during these activities. With only three exceptions (gaming, online shopping, and online banking), we detected the association between the purpose of technology use and perceived vulnerability in activities users perform more frequently. Furthermore, we found the strongest associations with the most frequent activities such as e-mail exchange, web browsing, and accessing social networks, even though only accessing social networks does not pose as much of a threat as, for example, downloading music and video content.

The abovementioned results indicate that technology users may feel more threatened by the technologies and services they use more frequently, despite the objective probability of realizing the threat may lie among the less frequently used ones. Such cybersecurity awareness (or lack thereof) may dilute users from being more likely to realize threats. Users are inevitably less proficient with technologies and services they use less frequently. They are more vulnerable to cyber threats with (ever-changing) technologies with which they are unfamiliar. The less a particular technology or service is used, the more emphasis on cybersecurity should be put on while using it. Just like an individual who is used to daily walking, rollerblades only once a month for a few minutes should emphasize rollerblading safety more than walking safety while in traffic.

Similar to the studies we mentioned in the theoretical part of the article, our results (RQ2) indicate several differences in technology use; however, we found few differences in perceived vulnerability to cyber threats. Computers and other technological devices are used differently (or at least with different frequency) in rural and urban communities. Except for online banking, users from rural environments tend to use technology less frequently, although differences regarding online shopping and social media use are relatively small between urban and rural communities. Users from urban domains use technology for downloading audio and video content, web browsing, playing audio and video content, and emailing significantly more frequently.

On the other hand, the same cannot be observed in their perceived vulnerability to cyber threats using the technology. The differences between residents of rural and urban environments in perceived vulnerability to cyber threats can only be detected when individuals access social networks, use online banking services, and shop online. In other words, in two-thirds of cases, there is no difference in perceived vulnerability between residents of rural and urban environments. In one-third of cases, residents of rural environments feel less vulnerable. Such findings do not entirely support previous studies on differences between perceived vulnerability and fear of crime [74]. Cyberspace may equally be considered as an (un)safe place by all its users, regardless of their place of residence, general fear of crime, or perceived vulnerability.

To answer the third research question (RQ3), we compared how frequently residents of different areas were victimized in cyberspace. The results indicate that in most cases, two-thirds of respondents have never been victimized in cyberspace or were unaware of their victimization (the minimum percentage was observed for malware infection at 58 percent). Online banking frauds, victimization from ransomware, and extortion in cyberspace were three incidents with the lowest frequency of occurrence. Online banking is traditionally well secured; hence, its users unsurprisingly do not feel particularly vulnerable while using it (see the answer to RQ2 above). Additionally, and for the same reason, they rarely detect any form of victimization from online banking fraud. Furthermore, ransomware is commonly directed toward entities with greater information assets, such as enterprises and other organizations. Unsurprisingly, individual users rarely report such victimization. The results of cyber extortion frequency are comparable to the frequency of ransomware since these two criminal activities may correlate.

However, we found several significant differences in victimization between residents of rural and urban areas. Even though cyberspace is typically considered "borderless",

where anyone can access any site, there appears to be more victims of spreading rumors online, hate speech, and disseminating indecent material among residents of urban areas. Social life and interpersonal connections are transferable from the material world to cyberspace. For example, rural youth are more likely to have siblings as friends on social media than urban and suburban youth, while suburban youth are more likely to have their parents as friends than urban youth; fewer residents of rural areas are using social media, and urban users have more connecting subjects (i.e., friends) on social media [76,77]. Exposure to more social media users can contribute to a higher degree of vulnerability to cyber threats and incidents such as spreading rumors, hate speech, and disseminating indecent material.

Our study complements the existing literature in several ways. Firstly, it offers insight by presenting the results collected in a field study with a nationally representative sample. Such samples with comparable sampling methods are particularly scarce in the cybersecurity literature. Secondly, since official statistics on cybercrime are unreliable, it represents an alternative source of cyber victimization statistics on a national level. Thirdly, it offers a possibility for the categorization of technology users. Categorizing technology users is essential (or at least encouraged) while designing and planning information and cybersecurity training [78]. Therefore, the results of this study are aimed at the decision makers to better understand (1) the relationship between technology use and perceived vulnerability during its use, (2) national cyber victimization, and (3) differences between perceptions among residents of urban and rural environments. By fusing these findings, professionals can plan and design the most effective multi-skill and digital literacy training for all demographic groups. Cybersecurity education and training should become a staple in more than just informal settings [49]. It should be embedded in formal education as early in the education process of an individual as possible to minimize the difference between the urban and rural demographic groups, which can potentially impact the perceived vulnerability to cyber incidents and fear of cybercrime. Even though the fear should be managed, lowering it to minimal levels can be counterproductive and cause less caution and, consequently, more victimization [79].

8. Limitations and Future Work

As with any other study, this study has several limitations the reader should consider when interpreting the results. Firstly, this study was conducted before the COVID-19 crisis, which brought broader technology use due to work-from-home policies. Secondly, the analyses are based on single items, which were necessary to keep the survey understandable and short for all demographic groups. Thirdly, the survey was conducted in Slovenia; hence, the results may not be generalized to any population. Fourthly, all results are based on self-reported data. Additionally, it is possible that some respondents provided their answers without knowing the technical details of victimization types, perceived vulnerability, and purpose of use, even though they had the option not to answer a question. Even though there is a possibility of lower reliability, such studies are currently the most common approach to large-sample victimization studies in the criminology literature. Lastly, even though we collected a relatively large sample in a field study that can be considered representative of the population, the sampling method cannot be regarded as actual simple random sampling.

There are several opportunities for future work in this field. First, future research should focus on exploring differences between urban and rural areas in more detail, especially in terms of their cybersecurity awareness and skills. Second, a longitudinal study spanning several years would contribute to a greater understanding of development and changes in users' technology use and perceived vulnerability over time. Third, future studies should focus on exploring how individuals perceive different terms frequently used and researched in cybersecurity research (e.g., wireless network interference, ransomware, phishing). Fourth, future research on cyber victimization would greatly benefit from developing a methodological approach to exploring cyber victimization beyond self-reported

studies. Even though self-reported studies have value in the literature, they are limited by their definition. Fifth, future cyber victimization studies should also include geographical mapping to highlight the geographical dimension of cyber victimization. Therefore, preventive measures can be individualized according to geographic location. Finally, comparative international (longitudinal) research based on the same questionnaire would contribute to a broader and deeper understanding of cyber victimization.

Author Contributions: Conceptualization, I.B. and K.P.; methodology, A.M.; validation, A.M. and K.P.; formal analysis, A.M.; investigation, I.B. and K.P.; resources, I.B.; data curation, A.M.; writing—original draft preparation, I.B. and A.M.; writing—review and editing, A.M. and K.P.; supervision, I.B. and K.P.; project administration, I.B.; funding acquisition, I.B. and K.P. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is based on the research programme Security and Safety in Local Communities (P5-0397, 2015–2018). The research was carried out by the Faculty of Criminal Justice and Security, University of Maribor, Slovenia, and co-financed by the Slovenian Research Agency (ARRS).

Institutional Review Board Statement: Ethical review and approval were waived for this study. Following the legislation of the Republic of Slovenia (where the survey was conducted), surveys in which collected data are processed as one unit, and there is no possibility of identifying an individual respondents, the Ethics Committee or Institutional Review Board approval is not required. Additionally, respondents were informed that their participation is voluntary and anonymous and that they could resign from filling out the questionnaire at any time.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data underlying the research findings reported in this article were deposited at Mendeley Data (https://doi.org/10.17632/5xh9x68b2x.1, accessed on 3 November 2022).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Verleysen, C. Cybercrime: A theoretical overview of the growing digital threat. *EUCPN Theor. Pap. Ser.* **2015**, 1–39. Available online: https://eucpn.org/document/eucpn-thematic-paper-no-8-cybercrime-a-theoretical-overview-of-the-growing-digital-threat (accessed on 28 September 2022).
2. Saunders, J. Tackling cybercrime—The UK response. *J. Cyber Policy* **2017**, *2*, 4–15. [CrossRef]
3. Agustina, J.R. Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. *Int. J. Cyber Criminol.* **2015**, *9*, 35–54. [CrossRef]
4. Leukfeldt, E.R.; Yar, M. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behav.* **2016**, *37*, 263–280. [CrossRef]
5. Melander, L.A. College Students' Perceptions of Intimate Partner Cyber Harassment. *Cyberpsychol. Behav. Soc. Netw.* **2010**, *13*, 263–268. [CrossRef]
6. Welsh, A.; Lavoie, J.A.A. Risky eBusiness: An Examination of Risk-taking, Online Disclosiveness, and Cyberstalking Victimization. *Cyberpsychol. J. Psychosoc. Res. Cyberspace* **2012**, *6*, 1–13. [CrossRef]
7. Reyns, B.W.; Henson, B.; Fisher, B.S. Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Crim. Justice Behav.* **2011**, *38*, 1149–1169. [CrossRef]
8. Henson, B.; Reyns, B.W.; Fisher, B.S. Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization. *J. Contemp. Crim. Justice* **2013**, *29*, 475–497. [CrossRef]
9. Roberts, L.D.; Indermaur, D.; Spiranovic, C. Fear of Cyber-Identity Theft and Related Fraudulent Activity. *Psychiatry Psychol. Law* **2013**, *20*, 315–328. [CrossRef]
10. Kurebwa, J.; Tanhara, J.R. Cybercrime as a Threat to Zimbabwe's Peace and Security. In *Global Cyber Security Labor Shortage and International Business Risk*; Christiansen, B., Piekarz, A., Eds.; IGI Global: Hershey, PA, USA, 2019; pp. 365–380. [CrossRef]
11. Broadhurst, R.; Choo, K.-K.R. Cybercrime and On-Line Safety in Cyberspace. In *International Handbook of Criminology*; Routledge: New York, NY, USA, 26 July 2009. Available online: https://papers.ssrn.com/abstract=2171559 (accessed on 26 September 2022).
12. Poonia, A.S. Cyber Crime: Challenges and its Classification. *Int. J. Emerg. Trends Technol. Comput. Sci.* **2014**, *3*, 119–121.
13. Brown, C.S.D. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *J. Cyber Criminol.* **2015**, *9*, 55–119. [CrossRef]
14. Brunton-Smith, I. Fear 2.0: Worry about cybercrime in England and Wales. In *The Routledge International Handbook on Fear of Crime*; Lee, M., Mythen, G., Eds.; Routledge: London, UK, 2017.
15. Tsakalidis, G.; Vergidis, K. A Systematic Approach toward Description and Classification of Cybercrime Incidents. *IEEE Trans. Syst. Man Cybern. Syst.* **2017**, *49*, 710–729. [CrossRef]

16. Bishop, L.M.; Morgan, P.L.; Asquith, P.M.; Raywood-Burke, G.; Wedgbury, A.; Jones, K. Examining Human Individual Differences in Cyber Security and Possible Implications for Human-Machine Interface Design. In *HCI for Cybersecurity, Privacy and Trust*; Springer: Cham, Switzerland, 2020; pp. 51–66. [CrossRef]
17. Chang, F.-C.; Miao, N.-F.; Chiu, C.-H.; Chen, P.-H.; Lee, C.-M.; Chiang, J.-T.; Chuang, H.-Y. Urban–rural differences in parental Internet mediation and adolescents' Internet risks in Taiwan. *Health Risk Soc.* **2016**, *18*, 188–204. [CrossRef]
18. Drew, J.M. A study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies. *J. Criminol. Res. Policy Pract.* **2020**, *6*, 17–33. [CrossRef]
19. Shan-A-Khuda, M.; Schreuders, C. Understanding Cybercrime Victimisation: Modelling the Local Area Variations in Routinely Collected Cybercrime Police Data Using Latent Class Analysis. *Undefined* 2019. Available online: https://www.semanticscholar.org/paper/Understanding-Cybercrime-Victimisation-%3A-Modelling-Shan-A.-Khuda-Schreuders/2fc441e1ecdf99dbe394ee5e0ce014bde66f43fa (accessed on 26 September 2022).
20. Van De Weijer, S.G.; Leukfeldt, R.; Bernasco, W. Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *Eur. J. Criminol.* **2018**, *16*, 486–508. [CrossRef]
21. Statista. *Cyber Threat Encounter Rate by Country 2021*; Statista: Hamburg, Germany, 2022. Available online: https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/ (accessed on 26 September 2022).
22. Pereira, F.; Spitzberg, B.H.; Matos, M. Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Comput. Hum. Behav.* **2016**, *62*, 136–146. [CrossRef]
23. Ronis, S.; Slaunwhite, A. Gender and Geographic Predictors of Cyberbullying Victimization, Perpetration, and Coping Modalities among Youth. *Can. J. Sch. Psychol.* **2017**, *34*, 3–21. [CrossRef]
24. Bidgoli, M.; Knijnenburg, B.P.; Grossklags, J. When cybercrimes strike undergraduates. In Proceedings of the 2016 APWG Symposium on Electronic Crime Research (eCrime), Toronto, ON, Canada, 1–3 June 2016; pp. 1–10. [CrossRef]
25. Al-Ali, A.A.H.; Al-Nemrat, A. Cyber Victimization: UAE as a Case Study. In Proceedings of the 2017 Cybersecurity and Cyberforensics Conference (CCC), London, UK, 21–23 November 2017; pp. 19–24. [CrossRef]
26. Doane, A.N.; Boothe, L.G.; Pearson, M.R.; Kelley, M.L. Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Comput. Hum. Behav.* **2016**, *60*, 508–513. [CrossRef]
27. De Kimpe, L.; Ponnet, K.; Walrave, M.; Snaphaan, T.; Pauwels, L.; Hardyns, W. Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Comput. Hum. Behav.* **2020**, *108*, 106310. [CrossRef]
28. Saridakis, G.; Benson, V.; Ezingeard, J.-N.; Tennakoon, H. Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technol. Forecast. Soc. Chang.* **2016**, *102*, 320–330. [CrossRef]
29. Wachs, S.; Michelsen, A.; Wright, M.F.; Gámez-Guadix, M.; Almendros, C.; Kwon, Y.; Na, E.-Y.; Sittichai, R.; Singh, R.; Biswal, R.; et al. A Routine Activity Approach to Understand Cybergrooming Victimization among Adolescents from Six Countries. *Cyberpsychol. Behav. Soc. Netw.* **2020**, *23*, 218–224. [CrossRef]
30. AlBladi, S.M.; Weir, G.R.S. User characteristics that influence judgment of social engineering attacks in social networks. *Hum.-Cent. Comput. Inf. Sci.* **2018**, *8*, 5. [CrossRef]
31. Louderback, E.R.; Antonaccio, O. 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 Delinq.* **2020**, *67*, 366–398. [CrossRef]
32. Van Wilsem, J. Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *Eur. J. Criminol.* **2011**, *8*, 115–127. [CrossRef]
33. Levesque, F.L.; Fernandez, J.M.; Somayaji, A. Risk prediction of malware victimization based on user behavior. In Proceedings of the 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), Fajardo, PR, USA, 28–30 October 2014; pp. 128–134. [CrossRef]
34. Oksanen, A.; Keipi, T. Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Child. Youth Stud.* **2013**, *8*, 298–309. [CrossRef]
35. Reep-van den Bergh, C.M.M.; Junger, M. Victims of cybercrime in Europe: A review of victim surveys. *Crime Sci.* **2018**, *7*, 5. [CrossRef]
36. Mihelič, A.; Jevšček, M.; Vrhovec, S.; Bernik, I. Testing the Human Backdoor: Organizational Response to a Phishing Campaign. *J. Univers. Comput. Sci.* **2019**, *25*, 1458–1477. [CrossRef]
37. Wall, D. Cybercrime and the Culture of Fear. *Inf. Commun. Soc.* **2008**, *11*, 861–884. [CrossRef]
38. United Nations Office on Drugs and Crime. *Comprehensive Study on Cybercrime*; United Nations Office on Drugs and Crime: Vienna, Austria, 2013.
39. European Commission. Special Eurobarometer 499: Europeans' Attitudes towards Cyber Security. Directorate-General for Communication. 2020. Available online: https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en (accessed on 26 September 2022).
40. Akdemir, N.; Lawless, C.J. Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach: Perceptions of the police in a rural county of England. *Internet Res.* **2020**, *30*, 1665–1687. [CrossRef]
41. Mawby, R. Myth and reality in rural policing. *Polic. Int. J. Police Strateg. Manag.* **2004**, *27*, 431–446. [CrossRef]
42. European Commission. Cybercrime. In *Migration and Home Affairs*; 2022. Available online: https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en (accessed on 26 September 2022).

43. Bissell, K.; LaSalle, R.; Cin, P.D. The Cost of Cybercrime. Accenture Security. 2019. Available online: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 (accessed on 26 September 2022).
44. Pupillo, L. *EU Cybersecurity and the Paradox of Progress*; Centre for European Policy Studies: Brussels, Belgium, 2018.
45. Furnell, S. Cybercrime: Vandalizing the Information Society. In *Web Engineering*; Springer: Berlin, Heidelberg, Germany, 2003; pp. 8–16. [CrossRef]
46. Halder, D.; Jaishankar, K.; Periyar, E.E.; Sivakumar, R. Cyber Victimization in India: Preliminary Study. In *Global Criminology*; Routledge: London, UK, 2013.
47. Raskauskas, J.; Stoltz, A.D. Involvement in traditional and electronic bullying among adolescents. *Dev. Psychol.* **2007**, *43*, 564–575. [CrossRef]
48. Statista. Online Adult Cyber Crime Victimization 2017. 2018. Available online: https://www.statista.com/statistics/294684/online-adult-cyber-crime-victimization/ (accessed on 26 September 2022).
49. Meško, G.; Bernik, I. Internet study of familiarity with cyber threats and fear of cybercrime [Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto]. *Rev. Krim. Kriminol.* **2011**, *62*, 242–252.
50. Australian Bureau of Statistics. Personal Fraud, 2020–21 Financial Year. 2022. Available online: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release (accessed on 26 September 2022).
51. Bakhshi, T. Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. In Proceedings of the 2017 13th International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, 27–28 December 2017; pp. 1–6. [CrossRef]
52. Musuva, P.M.; Getao, K.W.; Chepken, C.K. A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Comput. Hum. Behav.* **2019**, *94*, 154–175. [CrossRef]
53. Li, Q. Cyberbullying in Schools: A Research of Gender Differences. *Sch. Psychol. Int.* **2006**, *27*, 157–170. [CrossRef]
54. Marret, M.J.; Choo, W.Y. Factors associated with online victimisation among Malaysian adolescents who use social networking sites: A cross-sectional study. *BMJ Open* **2017**, *7*, e014959. [CrossRef]
55. Shabnam, N.; Faruk, O. Kamruzzaman Underlying Causes of Cyber-Criminality and Victimization: An Empirical Study on Students. *Soc. Sci.* **2016**, *5*, 1–6. [CrossRef]
56. Tynes, B.M.; Rose, C.A.; Williams, D.R. The Development and Validation of the Online Victimization Scale for Adolescents. *Cyberpsychol. J. Psychosoc. Res. Cyberspace* **2022**, *4*, 2. Available online: https://cyberpsychology.eu/article/view/4237 (accessed on 26 September 2022).
57. Berson, I.R.; Berson, M.J.; Ferron, J.M. Emerging Risks of Violence in the Digital Age. *J. Sch. Violence* **2002**, *1*, 51–71. [CrossRef]
58. Cassidy, W.; Jackson, M.; Brown, K.N. Sticks and Stones Can Break My Bones, But How Can Pixels Hurt Me? *Sch. Psychol. Int.* **2009**, *30*, 383–402. [CrossRef]
59. Hinduja, S.; Patchin, J.W. Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behav.* **2008**, *29*, 129–156. [CrossRef]
60. Dodel, M.; Mesch, G. Cyber-victimization preventive behavior: A health belief model approach. *Comput. Hum. Behav.* **2017**, *68*, 359–367. [CrossRef]
61. Näsi, M.; Danielsson, P.; Kaakinen, M. Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors. *Eur. J. Crim. Policy Res.* **2021**, 1–19. [CrossRef]
62. Berg, M.T.; Lauritsen, J.L. Telling a Similar Story Twice? NCVS/UCR Convergence in Serious Violent Crime Rates in Rural, Suburban, and Urban Places (1973–2010). *J. Quant. Criminol.* **2015**, *32*, 61–87. [CrossRef]
63. United States Department Of Justice. *Office of Justice Programs. Bureau of Justice Statistics, National Crime Victimization Survey, Concatenated File, 1992–2015: Version 1*; ICPSR—Interuniversity Consortium for Political and Social Research: Ann Arbor, MI, USA, 2016. Available online: https://www.icpsr.umich.edu/web/NACJD/studies/36456/versions/V1 (accessed on 27 September 2022).
64. Government Statistical Service. *Statistical Digest of Rural England*; Department for Environment, Food & Rural Affairs: London, UK, 2020. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1002698/04_Statistical_Digest_of_Rural_England_2020_August_edition.pdf (accessed on 27 September 2022).
65. Glaeser, E.L.; Sacerdote, B. Why is There More Crime in Cities? *J. Politi-Econ.* **1999**, *107*, S225–S258. [CrossRef]
66. Hacin, R.; Eman, K. Police Officers Perception of Threats in Urban and Rural Environments. *Rev. Krim. Kriminol.* **2019**, *70*, 455–468.
67. Donnermeyer, J. The Importance of Place: Safety and Security of Rural Peoples and Communities in an Urbanising World. *Rev. Krim. Kriminol.* **2019**, *70*, 399–408.
68. Crime in Urban & Rural Areas—Safe Places. Säkraplatser: 2022. Available online: https://www.sakraplatser.abe.kth.se/crime-in-urban-rural-areas/ (accessed on 27 September 2022).
69. The World Bank. *Rural Population (% of Total Population) | Data*; The World Bank: Washington, DC, USA, 2022. Available online: https://data.worldbank.org/indicator/SP.RUR.TOTL.ZS (accessed on 27 September 2022).
70. Donnermeyer, J.; DeKeseredy, W. *Rural Criminology*, 1st ed.; Routledge: Abingdon, Oxon, UK, 2013.
71. Näsi, M.; Oksanen, A.; Keipi, T.; Räsänen, P. Cybercrime victimization among young people: A multi-nation study. *J. Scand. Stud. Criminol. Crime Prev.* **2015**, *16*, 203–210. [CrossRef]
72. Symantec. Internet Security Threat Report. 2016. Available online: https://docs.broadcom.com/doc/istr-21-2016-en (accessed on 27 September 2022).

73. Roberts, L.D.; Indermaur, D.; Pietsch, J.; Aarons, H. Are Neighbourhood Incivilities Associated with Fear of Crime. In *Australia: Identity, Fear and Governance in the 21st Century*; ANU Press: Canberra, Australia, 2012; pp. 61–78. Available online: https://www.jstor.org/stable/j.ctt24hbqz.10 (accessed on 27 September 2022).
74. Meško, G.; Šifrer, J.; Vošnjak, L. Fear of Crime in Urban and Rural Environments in Slovenia. *J. Crim. Justice Secur.* **2012**, *3*, 259–276.
75. Kim, H.-Y. Statistical notes for clinical researchers: Assessing normal distribution (2) using skewness and kurtosis. *Restor. Dent. Endod.* **2013**, *38*, 52–54. [CrossRef]
76. Madden, M.; Lenhart, A.; Cortesi, S.; Gasser, U.; Duggan, M.; Smith, A.; Beaton, M. Part 2: Information Sharing, Friending, and Privacy Settings on Social Media. *Pew Res. Cent. Internet Sci. Tech*. 21 May 2013. Available online: https://www.pewresearch.org/internet/2013/05/21/part-2-information-sharing-friending-and-privacy-settings-on-social-media/ (accessed on 7 September 2022).
77. Perrin, A. Social Media Usage: 2005–2015. *Pew Res. Cent. Internet Sci. Tech*. 8 October 2015. Available online: https://www.pewresearch.org/internet/2015/10/08/social-networking-usage-2005-2015/ (accessed on 27 September 2022).
78. Fujs, D.; Vrhovec, S.; Vavpotic, D. Know Your Enemy: User Segmentation Based on Human Aspects of Information Security. *IEEE Access* **2021**, *9*, 157306–157315. [CrossRef]
79. Meško, G.; Areh, I. Fear of Crime in Urban Environment [Strah pred kriminaliteto v urbanih okoljih]. *Rev. Za Kriminalistiko Kriminol.* **2003**, *54*, 144–152.