

UNAUTHORIZED ACCESS TO COMPUTER INFORMATION: THE EMPIRICAL STUDY OF CHARACTERISTICS OF VICTIMS AND THEIR VICTIMIZATION

ILYA MOSECHKIN¹

Associate Professor at Vyatka State University, Kirov, Russian Federation¹
Weretowelie@gmail.com¹

Abstract - The purpose of this study is to identify the main individual characteristics that contribute to cybervictimization of victims of unauthorized access to computer information. The relevance of the research topic is due to the fact that the number of crimes of this type and the amount of damage from them are growing every year. At the same time, in the scientific literature there is no uniform understanding if gender, relationships with the criminal, behavior of the victim and the type of crime affect victimization. 300 court decisions issued in the Russian Federation regarding the commission of unauthorized access to computer information were analyzed to conduct this study. Based on the analysis it was revealed that accidental victims predominate, but in some cases the crime occurred due to relationships with the criminal. The most risky are the following areas: banking, social networks, and mobile communications. Taking into account peculiarities of areas of activity with increased risk and victim behavior of victims, victimological measures are proposed to prevent cases of unauthorized access to computer information.

Keywords: cyber-victimization; unauthorized access; hacking; cybercrime; prevention

INTRODUCTION

Currently many elements of public relations have undergone digitalization: banking, trade, management and many others. This process can be still observed: various spheres of activities are moving into the Internet space; new ones appear (targeted advertising, crowdfunding); virtual interaction is expanding and improving. It is quite obvious that in the near future the digital environment will continue to be an integral part of our lives. It can also be agreed with the view that digitalization will have far-reaching consequences for individuals, society and organizations¹. At the same time, it seems obvious that the widespread introduction of computer technologies can have negative features. Among them the following are unemployment caused by robotization, the loss of personal boundaries, the risk of technostress and, of course, the spread of cybercrime. The last feature should be considered in more detail.

The Internet space attracts criminals for several reasons. First, it allows traditional crimes (such as pilferage or slander) to be committed remotely. It is known that anonymity and remoteness lead to a high latency of illegal acts. The mismatch between the methods and technologies used by law enforcement officers and the level of innovative methods used by criminals contributes to the low crime detection rate². Secondly, the Internet space allows new crimes to be committed: unauthorized access to computer information or the use of malicious computer programs.

Crimes committed in cyberspace are widespread in countries where citizens actively use the Internet. In particular, in 2018 the Federal Bureau of Investigation recorded more than 350,000 cybercrime cases reporting damages in excess of \$2.7 billion³. Unauthorized access to computer information in the Netherlands has become more common than bicycle theft, one of the most common traditional crimes⁴. According to the survey conducted in Switzerland, about 13% of respondents were victims of unauthorized use of personal data⁵.

¹ H. Trittin-Ulbrich et al. 'Exploring the dark and unexpected sides of digitalization: Toward a critical agenda' (2021) *Organization*, 28, 23-24.

² B. Sturc et al. 'The Specifics and Patterns of Cybercrime in the Field of Payment Processing' (2022). *International Journal of Criminology and Sociology*, 9, 2028-2029.

³ F. Miró-Llinares et al. 'Understanding target suitability in cyberspace: An international comparison of cyber victimization processes' (2020) *International Journal of Cyber Criminology*, 14, 141.

⁴ E. R. Leukfeldt et al. 'Exploring the needs of victims of cyber-dependent and cyber-enabled crimes' (2020) *Victims & Offenders*, 15, 75.

⁵ R. Milani et al. 'Exposure to cyber victimization: Results from a Swiss survey' (2022) *Deviant Behavior*, 43, 229.

A great number of Internet users in China leads to a lot of cyber security problems. Cybercrime accounts for about one third of all crimes in China and is characterized by an annual increase of 30% and damage in excess of 95 billion yuan per year. For example, in 2016 there were approximately 70,000 ransomware attempts, 197 million intercepted phishing attacks, and 20,000 reports of monetary losses and security vulnerabilities⁶.

In the Russian Federation due to the actions of cybercriminals large organizations suffer losses, on average, in the amount of 20 million rubles annually, and medium and small businesses lose about 700 thousand rubles annually. At the same time, according to official statistics, the number of cases of unauthorized access to computer information in 2018 amounted to 1761, in 2019 - 2420, and in 2020 - 4105. The number of registered cases of use and distribution of malicious computer programs in 2018 amounted to 733, for 2019 - 455, and for 2020 - 371⁷.

The COVID-19 pandemic has spurred cybercrime. In conditions of isolation and restrictions, law-abiding and non-law-abiding citizens spent more time on the Internet. Many began remote work for the first time without having the appropriate computer literacy. As a result, according to the study of Chigada and Madzinga, cyberattacks during the COVID-19 pandemic grew exponentially, creating another wave of challenges for the global economy⁸.

Thus, the problem of combating cybercrime is common to most countries. However, countermeasures should be aimed not only at criminals, but also at victims. There are scientific opinions that suggest the need to develop cybervictimology as a separate sub-field of victimology⁹. It is worth noting that victimization in the field of computer information does have its own characteristics. Since it differs from traditional victimization, more research is needed to further develop the most effective crime countermeasures. One of the most pressing issues is the lack of a meaningful understanding of how victim behavior can increase or decrease the probability of cybervictimization. It seems that the study of victims' behavior in the Russian Federation can be useful for the whole world, since this country is multinational (over 160 nationalities), multi-confessional (over 70 confessions) and

This article addresses the following main problems:

- 1) In what behavior is cybervictimization most often manifested?
- 2) Is there a relationship between characteristics of the victim (gender, relationship with the criminal, sphere of the activity and cybervictimization)?
- 3) What measures can help reduce cybervictimization?

1. Literature Review

The review of the literature is mainly devoted to cybervictimization and characteristics of victims of unauthorized access to computer information. Both individuals and associations of persons can be considered as a victim of a crime¹⁰. Lifestyle Exposure Theory (LET) and Routine Activity Theory (RAT) methods were widely used in previous research works to study individual victimization. However, it was not possible to come to a unified point of view regarding the influence of situational and individual factors. Some scholars believe that they play an important role¹¹, while others believe that these facts are not able to determine victimization¹². Most of the studies focus on only one type of cybercrime (for example, malware infection, phishing or online fraud). Smith and Stamatakis consider that effectiveness of Routine Activity Theory is not constant for different forms of crime¹³. So, RAT

⁶ M. Jiang, M. 'Cybersecurity policies in China'. In L. Belli (ed.) *CyberBRICS* (Springer: Cham, 2021) 225.

⁷ V. I. Gladkikh – I. N. Mosechkin, 'Problems of improving criminal law measures of counteracting crimes in the sphere of computer information' (2021) *Russian Journal of Criminology*, 15, 232.

⁸ J. Chigada – R. Madzinga, 'Cyberattacks and threats during COVID-19: A systematic literature review' (2021) *South African Journal of Information Management*, 23, 8.

⁹ K. Jaishankar, 'Cyber victimology: a new sub-discipline of the twenty-first century victimology'. In J. Joseph (ed.) *An International Perspective on Contemporary Developments in Victimology* (Springer: Cham, 2020) 15

¹⁰ M. Näsi et al. 'Cybercrime victimization among young people: a multi-nation study' (2015) *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16, 205.

¹¹ K. S. Choi, 'Computer crime victimization and integrated theory: An empirical assessment' (2008) *International Journal of Cyber Criminology*, 2, 332.

¹² F. T. Ngo – R. Patenoster, 'Cybercrime victimization: An examination of individual and situational level factors' (2011). *International Journal of Cyber Criminology*, 5, 773.

¹³ T. Smith – N. Stamatakis, 'Cyber-victimization trends in Trinidad & Tobago: the results of an empirical research' (2021) *International Journal of Cybersecurity Intelligence & Cybercrime*, 4, 60.

is suitable for crimes that target people (for example, fraud using social engineering). However, in relation to technocentric violations (hacking using a program), RAT is much less suitable. In general, the carried out bibliometric analyzes argue that there remains a polarity of opinion regarding the effect of LET or RAT to explain cybervictimization¹⁴.

Studies show that gender can affect the probability of becoming a victim. Thus, it is found that men are more likely to suffer from cybercrime than women¹⁵. However, if we analyze each type of crime separately, the distribution of victims changes. Women are more likely to be victims of, for example, online romantic relationships¹⁶ and sexual abuses, while men are more likely to be victims of cyber-violence and slander¹⁷.

Old age was noted as a risk factor. As a rule, people from this category experience difficulties with the interface of sites or the use of browsers in general¹⁸. However, there is also an opposite point of view. Thus, based on the results of the survey, the authors note that they could not find a risk-increasing effect of age. At the same time, they were able to find out that people with a migration background are at higher risk of being infected with ransomware, which is explained by potential language difficulties¹⁹. The scientific literature also notes that high-income individuals are more likely to report DDoS attacks and identity theft. The results of the same study confirm the frequent occurrence of multiple victimization. This is usually explained by a chain of crimes. For example, identity theft leads to bank account fraud²⁰. A team of researchers from the Netherlands studied needs of victims of cybercrime and noted that they are often not taken seriously and discouraged from reporting to the police. In addition, the authors specifically emphasized that victims of account hacking deserve special attention in subsequent research, as they are different from other victims²¹. Cybervictimization has become a major area of research in recent decades. Choi (2008) investigated the "digital sentinel" construct that was associated with the use of security software and the duration of such use²². At the same time, the scientist proved that online behavior and digital protection tools must be taken into account when building a model of computer crime patterns. Bossler and Holt clarified that the possession of a computer and the duration of Internet activity do not always increase the probability of being a victim²³. This also requires other circumstances. In addition, the commission of computer deviations by a person increases his/her own victimization. On the other hand, the scientific literature argues and justifies that neither individual nor situational characteristics have the same stable effect on the probability of becoming a victim in cyberspace²⁴. After analyzing user behavior, the authors of one of the studies concluded that the culture of cybersecurity is not enough to reduce the probability of becoming a victim. Developed technical solutions are needed: continuous education on cybersecurity issues; vulnerability analysis using social engineering tests; anti-phishing solutions and behavior-based endpoint protection²⁵. The results of the study of Akdemir are very important, according to which the big problem is the use of the same

¹⁴ H. T. N. Ho – H. T. Luong, 'Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis' (2022). *SN Social Sciences*, 2, 30.

¹⁵ Näsi, above.

¹⁶ M. T. Whitty – T. Buchanan, 'The online romance scam: A serious cybercrime' (2012) *CyberPsychology, Behavior, and Social Networking*, 15, 182.

¹⁷ Ho – Luong, above.

¹⁸ N. Akdemir, Contextual vulnerabilities approach to understand victimization in cyberspace (Kriter: Istanbul, 2021). 73.

¹⁹ M. C. Bergmann et al. 'Cyber-dependent crime victimization: the same risk for everyone?' (2018). *Cyberpsychology, Behavior, and Social Networking*, 21, 88.

²⁰ M. Junger et al. 'Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe' (2017) In 2017 international conference on cyber situational awareness, data analytics and assessment (Cyber SA), 8.

²¹ Leukfeldt, above.

²² Choi, above.

²³ T. J. Holt – A. M. Bossler, 'Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization' (2009) *Deviant Behavior*, 30, 23.

²⁴ Ngo – Paternoster, above.

²⁵ C. Krasnay – P. B. Hámornik, 'Analysis of cyberattack patterns by user behavior analytics' (2018) *AARMS–Academic and Applied Research in Military and Public Management Science*, 17, 113.

password for different accounts. Additional user verification systems contribute to reducing victimization from this factor²⁶.

Odunze correctly notes that countering unauthorized access to computer information requires interaction of authorities, organizations and consumers²⁷. By all means the latest software must be available to protect against viruses, malware and other online threats (which are the gateway through which hackers enter user accounts). The author also developed recommendations for potential victims, including destruction of personal information and installation of a variety of secure passwords. These findings are supported by the study of cyber threats in the banking sector²⁸. Dodel and Mesch explain effectiveness of non-digital prevention interventions²⁹. The authors discuss the concept of “health belief model approach” and conclude that beliefs can reduce online threats.

Features of cybervictimization are covered in the works of Russian scientists, but the number of studies devoted specifically to victims of unauthorized access to computer information (hacking) remains very small. Zhmurov and Klyuchko rightly point out that the scientific community does not pay enough attention to this problem, even despite a tenfold increase in cybercrime and its victims during 2013-2018³⁰. Nevertheless, there are a number of works devoted to victims and victimization from crimes in the field of computer information. Thus, the study of judicial and investigative practice showed that the average age of the victims is about 30. Criminals can purposefully choose the victim, but random victims are the main category. In addition, it is indicated that crimes often occur due to insufficient victims' knowledge of methods and means of protecting computer information³¹.

During the survey of respondents a significant discrepancy was found in the gender structure of victimization for hacking an account on social networks (6% for men versus 49% for women); installing malware on a computer (14% versus 8%); insults (20% versus 10%), obscene offers (10% versus 25%), and theft of confidential information (3% versus 1%). Thus, men were more likely to become victims of passport data theft (payment cards), ransomware attacks, or deception by unscrupulous sellers. Women were victims of social media account hacking and sexual abuses at a higher rate³². On the other hand, Khomenko emphasizes that men become victims of cybercrime more often than women, and older people are victims more often than young people, primarily due to the failure to take measures to protect their personal systems. Thus, 73.8% of victims did not use technical means to protect information and monitor unauthorized penetration³³.

In Russian victimology the features of legal entities as victims of computer crimes are discussed. Alexandrina notes that most often legal entities face hacker attacks on the operating system³⁴. Among them it is worth highlighting the theft or blocking of confidential information, as well as the threat of their destruction for the purpose of ransom. Every year the number of DDoS attacks, as well as their consequences, increases significantly. The author also points out that corporate victims directly influence the latency of crimes, as they hide them because they do not want to suffer reputational damage or do not believe in justice³⁵.

Mayorov concluded that online victims often have little knowledge of dangers of digital spaces, legal measures available in the event of victimization, and limitations of such measures. In addition, the

²⁶ Akdemir, above.

²⁷ D. Odunze, ‘Cyber victimization by hackers: A criminological analysis’ (2018) *Public Policy and Administration*, 8, 13.

²⁸ L. Ali et al. ‘The effects of cyber threats on customer’s behaviour in e-Banking services’ (2017) *International Journal of e-Education, e-Business, e-Management and e-Learning*, 7, 78.

²⁹ M. Dodel – G. Mesch, ‘Cyber-victimization preventive behavior: A health belief model approach’ (2017) *Computers in Human behavior*, 68, 365.

³⁰ D. V. Zhmurov – R. N. Klyuchko, ‘Cyber-Victimology as A New Reality of The Technotronic Society (Gender Research)’ (2020) *Baikal Research Journal*, 11, 29.


³¹ V. V. Polyakov – A.V. Shiryaev, ‘Forensic aspects of the identity of victims of cybercrime’ (2018) In *Criminal procedure and forensic readings in Altai*, 170

³² Zhmurov – Klyuchko, above.

³³ A. N. Khomenko, ‘On the Victimization of Cybercrime Victims’ (2021) *Victimology*, 8, 147.

³⁴ N. M. Alexandrina, ‘Victimological characteristics of computer crimes committed against legal entities’ (2019) *Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 45, 226.

³⁵ Alexandrina, above.



author argues that older people were initially less susceptible to digital crime due to their remoteness from the digital space. However, now there is an increase in the number of Internet users among such individuals, which also increases the risk of cybervictimization³⁶.

Among the factors of victimization Rodina names insufficient computer literacy of users. The author points out that in parallel with the ubiquity of computers, tablets and smartphones, the average level of computer literacy is not increasing, but decreasing. At the same time it is proposed to change teaching of computer literacy to include the technical aspects of functioning of computer networks and basic aspects of safe behavior in cyberspace³⁷. In addition, it is proposed to strengthen state support for commercial and non-profit organizations that contribute to the prevention of computer crime³⁸.

Thus, victimization of victims of unauthorized access to computer information (hacking) in science was not unnoticed. However, the studies were conducted selectively and in individual countries, and therefore they are fragmented and incomplete. It seems that an additional study of cybervictimization of this category of victims based on empirical data from the Russian Federation will deepen the available scientific results and allow us to establish more effective solutions to existing problems.

2. Methods and Materials

The empirical base of the study consists of 300 acts of courts (sentences and decisions), by which persons were found guilty of committing unauthorized access to computer information. This offense is provided for in Art. 272 of the Criminal Code of the Russian Federation, which includes the following wording: "Unauthorized access to legally protected computer information, if this act entailed the destruction, blocking, modification or copying of computer information." This article qualifies all cases of hacking computers (laptops, smartphones), accounts, e-mail and other devices or Internet systems. If the hacking entailed the theft of property or information, then the action is additionally qualified under a different article.

The acts of the courts were issued in the period from 2016 to 2021. The source of data is legal reference systems (the state automated system "Pravosudie") and the official websites of the Russian courts, where the issued acts are presented. The sample of judicial acts made it possible to cover 71 constituent entities of the Russian Federation out of 85, which allows us to speak about a sufficient degree of representativeness. From the text of judicial acts, as a rule, the personal data of the victims are deleted. However, information about gender, behavior, relationships with the offender and the field of activity in which the illegal act occurred is left. These features were systematized and analyzed.

This study is focused on victims-individuals, therefore, in the course of selection for the analysis of acts, cases of encroachment on legal entities were excluded. The selection of cases for the study was made without taking into account the individual characteristics of victims and it was carried out in a continuous way, that is, the cases located in the reference system in a row were analyzed (if they corresponded to the parameters of the study). This allowed us to maintain the objectivity of the study and ensure sufficient representativeness.

In this study cybervictimization refers to the process of turning a potential victim into a real one, as well as the harm (result) from a crime committed using digital technologies (Mayorov, 2022). In Russia cybervictimization is associated with a variety of crimes: unauthorized access to computer information; use of malware; computer fraud; theft from bank accounts; illegal receipt of commercial or banking secrets and others. However, the present study is limited only to cases of unauthorized access to computer information, as they have not been studied as often and in such detail.

The purpose of this study is to identify the main individual characteristics that contribute to cybervictimization. To achieve the purpose the following tasks were set and solved: to analyze the judicial acts issued in connection with the commission of unauthorized access to computer

³⁶ A. V. Mayorov, 'Does Digitalization Affect Victimization in Today's Society?' (2022) *Victimology*, 9, 150.

³⁷ E. A. Rodina, 'General Social Prevention of Criminogenic Victimization of Internet Users' (2022) *Bulletin of the Saratov State Law Academy*, 146(3), 205.

³⁸ A. V. Gladkikh, 'Prevention Of Crimes in The Field of Computer Security. In Almanac Lecture' (2022) In *May Legal Readings on the Yenisei*, 40



information; to determine the gender of the victims; to determine the relationship with the offender and the area of activity in which the crime was committed; to analyze victim behavior that contributed to cybervictimization.

In particular, this paper attempts to answer the following research questions:

1. Is there a correlation between the probability of becoming a victim of unauthorized access to computer information and gender?
2. Does the relationship with the criminal affect cybervictimization?
3. Does the field of activity affect cybervictimization?
4. What victim behavior contributed to cybervictimization?

3. Results

In total, 300 judicial acts were analyzed, but the number of victims was 421, since several people sometimes suffered from a crime at once. The analysis of the acts showed that more often the victims are females (51.8%). In most cases there was no relationship between the criminal and the victim - in 82.4% the choice of the victim was random. However, it was found that in 7.1% of cases the criminal and the victims knew each other or were even on friendly terms. 4.8% of victims were intimate partners of the criminal (cohabitation or marriage).

In particular, according to the verdict of the city court in case No. 1-311/2019, it was established that the accused K. got access to the page on the VKontakte social network owned by the victim, who was his cohabitant. Using the victim's login and password stored in the mobile phone, K. entered her personal page on the VKontakte social network. Wanting to know about the correspondence between the victim and citizen Ch., the accused K. copied the correspondence and changed the access password, thereby blocking access to computer information to the legal user³⁹.

In 4.2% of cases the criminal and the victim were in a business relationship. So, according to the verdict of the district court in case No. 1-1069/2017, it was established that the victim S. did not fully pay off the accused L. for services in designing a website for a drug treatment center. L., using the link for password recovery available on the site, restored the access password, having received the opportunity to change and block access to the site. Then, without the consent of S., she changed the password for access to the site, thereby blocking access to the site, and placed an advertisement for a stretch ceiling company, instead of information about the drug treatment center⁴⁰.

Very rarely the criminal and the victim were related to each other (1.5%). For example, as it was found out by the city court in case No. 1-83/2018, the accused Yu., hired as the chief accountant, had access to the current account of the enterprise. Knowing the login and password of her daughter's account, the accused, by drawing up the payment order, transferred funds from her daughter's personal account to her account. Yu. used the received funds for her own needs⁴¹.

The percentage by types of areas of activity in which crimes were committed is as follows. Most often unauthorized access to computer information is carried out in connection with banking (50.1%), social networks (24.7%) and mobile communication (18%). All other areas of activity are much less common. So, in the sentences there were areas: online games (3.8%), online shopping (1.9%), transport (0.5%), advertising (0.5%) and judicial (0.5%). The indicators are more fully reflected in table 1.

Table 1. Features of characteristics of victims of unauthorized access to computer information

Gender	
Male - 203 people (48.2%)	Female - 218 people (51.8%)
Relationship between the criminal and the victim	
No relationship (accidental victim)	347 people (82.4%)
Friends/acquaintances	30 people (7.1%)
Intimate partners (cohabitants/marriage)	20 people (4.8%)
Business	18 people (4.2%)
Relatives	6 people (1.5%)
The area in which the crime occurred	
Banking	211 cases (50.1%)
Social networks	104 cases (24.7%)
Mobile communication	76 cases (18%)

³⁹ Case 1-311 [2019] Novy Urengoy City Court of the Yamalo-Nenets Autonomous Okrug (Russian Federation)

⁴⁰ Case 1-1069 [2017] Central District Court of Chita (Russian Federation)

⁴¹ Case 1-83 [2018] Belebeevsky City Court of the Republic of Bashkortostan (Russian Federation)



Online games	16 cases (3.8%)
Online shopping	8 cases (1.9%)
Transport	2 cases (0.5%)
Advertising	2 cases (0.5%)
Judicial	2 cases (0.5%)

The study of descriptions of the behavior of the victim in the texts of judicial acts made it possible to establish a number of features and patterns. In most cases unauthorized access to computer information was carried out through phishing mailings (35.6%). In other words, the victim followed the link sent in the message, which allowed one way or another to gain access to the information stored on his/her device. For example, as it was established by the verdict of the city court in case No. 1-897 / 2018, the victim, misled by the content of the text of the SMS message about the intention to buy property from her, followed the link indicated in the message. As a result, a malicious computer program was installed on her mobile phone, which provided the accused P. with the possibility of unauthorized access, blocking and copying computer information⁴².

At the same time, the behavior of a large part of the victims cannot be called negative (25.1%). In fact, they behaved neutrally and did not have any opportunity to oppose the intruder. Usually, neutral behavior is associated with cases in which the criminal used his/her official position. Thus, according to the verdict of the district court in case No. 1-299/2018, the accused F. was a specialist in the sales office of a mobile operator. Being at her workplace in a mobile phone shop, against the will of the subscriber, in order to transfer information to a third party, she entered the personal account of subscriber G. in the subscriber base management system. To do this, she used the computer provided to her and confidential password information. F. copied and printed information about the telephone connections of the subscriber number used by G., and provided on paper the details of telephone and other connections to an outside person⁴³.

Almost a fifth (18%) of individuals became victims because they used a weak password or did not change it for a long time, and also used the same password for different accounts. From time to time, organizations allow database leaks, so careless use of passwords contributes to unauthorized access to computer information. In particular, the district court in case No. 1-268/2017 found that the accused Ch. in order to steal other people's money acquired access logins and their corresponding passwords on the Internet, allowing unhindered access to the pages of users of the VKontakte social network. Then Ch. got access to the victim's electronic page and changed the identification data, blocking the access to the latter. From the electronic page of the victim Ch. sent messages to other users with a request to lend money. Under the influence of fraud users made a transfer in the total amount of 5,000 rubles⁴⁴.

16.8% of victims gave login and password from their accounts under the influence of deception or installed malicious software on their devices. It should be noted that in some cases the victims allowed several variants of illegal behavior at once, so they can be classified into several categories. For example, as it was established by the district court in case No. 1-886/2019, the accused S. found a previously unknown B., whom he fraudulently, under the pretext of helping to find a lost mobile device, convinced to install malicious software on his mobile device. The software allowed remote access to the victim's mobile device. As a result, S. got access to the personal account of the banking application. Further, S. deliberately generated and sent three orders to the branch of the bank to transfer funds in the total amount of 1660 rubles from the bank account of the victim to his own account⁴⁵.

7.1% of the victims voluntarily provided the criminal with the login and password from the account, without being under the influence of deception. Thus, the district court in case 1-323/2017 found that the accused P. had information about the login and password from the accounts of the victim, since they cohabited and were in a trusting relationship. P., without the consent of the victim, illegally accessed her electronic mailbox. Then, from the indicated e-mail box, he followed the links

⁴² Case 1-897 [2018] Shakhty City Court of Rostov Region (Russian Federation)

⁴³ Case 1-299 [2018] Akhtubinsky District Court of the Astrakhan Region (Russian Federation)

⁴⁴ Case 1-268 [2017] Leninsky District Court of Cheboksary (Russian Federation)

⁴⁵ Case 1-886 [2019] Leninsky District Court of Tyumen (Russian Federation)

to the victim's page on the social network. On the website P. made changes in the "personal data" section, indicating obscene content⁴⁶.

2.8% of the victims left the device turned on with the login and password entered for the account. The criminal used this opportunity to realize intentions. Thus, the district court in case 1-421/2018 found that the accused L., being in the apartment of the victim K. and using his laptop, opened the browser tab where the e-mail, the login and password were entered. L. linked the e-mail to her subscriber number. After that using the password recovery system, L. changed the password for entering the indicated e-mail box and deleted the security question⁴⁷.

2.8% of the victims behaved immorally or unlawfully with the criminal, which caused the latter to intend to take revenge with the help of unauthorized access to computer information. Thus, the district court in case 1-212/18 found that the accused M. provided services to the victim in the field of IT technologies, for which he received a reward. At the end of the year M. provided another service, but did not receive a reward, in connection with which he repeatedly demanded payment of the amount of money. Having received a refusal to pay, M. accessed information and deleted from the computer information created by the victim in order to carry out activities related to transport services⁴⁸.

In some cases the behavior of the victim fell into several categories at once. So, some of the victims simultaneously reported the password to the account and behaved immorally with the criminal. In other cases they followed a phishing link and installed malicious software. In more detail the percentage of behaviors of the victims is shown in Table 2.

Table 2. The behavior of victims of unauthorized access to computer information revealed in court decisions

Type of behavior of the victim	Percentage of acts of courts in which this behavior was*
Following a phishing link	35.6%
Neutral behavior (not conducive to committing a crime)	25.1%
Using a weak password / using a password for a long time / using the same password for different accounts	18%
Giving login and password to a third party under the influence of fraud / installation of malicious software under the influence of fraud	16.8%
Voluntary and deliberately providing login and password to a third party	7.1%
Leaving the switched on device with the entered login and password off hand	2.8%
Illegal or immoral behavior	2.8%
* The same victim could carry out several types of behavior at once when one crime was committed	

5. Discussion

The results of the study show that the gender of the victim does not have a significant impact on victimization associated with unauthorized access to computer information. The reason seems to be that this crime is remote and technocentric, and in most cases the victim is chosen at random. The findings are consistent with the opinion that gender is a low predictor of cybervictimization⁴⁹. At the same time, it is necessary to agree that gender can still influence victimization depending on the type of the committed crime⁵⁰.

As the analysis of judicial acts showed, the relationship with the criminal can have an impact on victimization, although not in most cases. This issue is not enough discussed in the scientific literature. As it is noted by Ho and Luong, previous research was mainly focused on parent-child


⁴⁶ Case 1-323 [2017] Gagarynsky District Court of Sevastopol (Russian Federation)

⁴⁷ Case 1-421 [2018] Leninsky District Court of Barnaul, Altai Krai (Russian Federation)

⁴⁸ Case 1-212 [2018] Soviet District Court of Kazan (Russian Federation)

⁴⁹ Odunze, above

⁵⁰ Whitty – Buchanan, above.



relationships⁵¹. Other types of relationships are practically not studied, if this is stated in the context of the study of unauthorized access to computer information. At the same time, the analysis of the acts of the courts showed that 17.6% of the victims were not accidental. On the contrary, they were in some kind of relationship with the criminal (relative, business or other). In traditional crime it is known that relationships can have a strong impact on victimization⁵². Cybercrime does not tend to be so dependent on this characteristic, but it is clear that victims must consider the possibility of a relative, partner or business partner committing the crime. One study correctly notes that the majority of cyberattacks carried out by intimate partners were technically simple. The most commonly used was guessing the password or possessing the password from the accounts⁵³. We consider it possible to agree with the opinion of Polyakov and Shiryaev that a separate group of victims should be singled out, who have victim personality traits⁵⁴. Unlike random victims, such victims can actively provoke the commission of a computer crime against themselves. As an example, they may be people who publicly speak negatively about "hackers".

As it can be seen from the study, the main areas of the activity in which the crime occurred are: banking (50.1%) and social networks (24.7%). The dominance of banking is not surprising since most cybercriminals are focused on making financial gain⁵⁵. Social networks also help them do this. Our findings are in agreement with previous studies that found social media to be a good ground for cybercriminals because most internet users spend their time on social media and post personal (and sensitive) information⁵⁶. Thus, companies which provide services in these areas and users should pay special attention to security due to the high risk of crimes.

The areas of online shopping and online games, to our surprise, did not show high risks of victimization. It seems that the reason lies in the fact that other methods are more often used to commit crimes in these areas. For example, fraud is common, when useless goods are sent. That is, for illegal profit making, it is not required to hack accounts. On the other hand, it can be assumed that organizations in these areas are aware of possible risks and are making every effort to ensure safety of users.

The results of this study also show that behaviors that contribute to victimization predominate among victims. Only 25.1% behaved neutrally, that is, they did not provoke the criminal and did not facilitate the commission of the crime. These persons, as a rule, would not be able to take measures to counter hacking, since it was carried out by employees of service organizations (banks, mobile operators, etc.). Yet the risk of becoming a victim is not the same for all categories of citizens. It was proven that individual and domestic factors, online behavior and preventive behavior influence victimization. In other words, the risk of victimization is different, and users have the opportunity to protect themselves⁵⁷.

The high number of clicking phishing links and weak or long-used passwords confirms the fact that users continue to ignore the possible risks. This is consistent with the results of previous studies. Thus, the scientists found out that due to the level of self-control of the victim, online victimization can be predicted. It follows that advanced users have more options to avoid risky behavior: opening random links, downloading media from unsafe sources, and others⁵⁸. The foregoing allows us to fully agree with the opinion of Odunze that prevention should be the focus, since most cybercrime occurs as a result of ignoring the risks associated with online interaction. Measures to reduce the possibility of becoming a victim can be carried out both by the state and service organizations, and by users. Considering that the majority of hacks, according to our data, occur in banking, it is necessary to recommend that banks implement additional systems for checking suspicious activity from customer

⁵¹ Ho – Luong, above.

⁵² E. A. Chiesa et al. 'Intimate partner violence victimization and parenting: A systematic review' (2018) *Child abuse & neglect*, 80, 298.

⁵³ D. Freed et al. "A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology' (2018) In Proceedings of the 2018 CHI conference on human factors in computing systems, 12.

⁵⁴ Polyakov –Shiryaev, above.

⁵⁵ Miró-Llinares et al., above.

⁵⁶ Milani et al., above.

⁵⁷ Bergmann et al., above.

⁵⁸ Reynolds et al. 'Opportunity and self-control: Do they predict multiple forms of online victimization?' (2019) *American Journal of Criminal Justice*, 44, 80.



accounts. In addition, banks should implement regular password change reminders and prevent weak passwords from being set. The widespread introduction of double verification, in which the login to the account occurs not only as a result of entering a password, but also with additional confirmation codes, is justified. It should be added that banking, social networks and mobile communications are extremely profitable areas of activity. It would be right if a significant part of these revenues was used to promote additional security for users. At the same time, users themselves should familiarize themselves with online threats when performing banking transactions and take appropriate security measures.

Oduze points out that cooperation between government agencies and Internet companies is necessary. Individual hacking threats are more difficult to counter than when they are combined. We believe that the state should support commercial and non-commercial organizations that contribute to the prevention of computer crimes. It is worth considering both tangible forms of encouraging such activities (tax mitigation, grants) and intangible ones (advertising the organization, encouraging activities).

At the same time, in some cases the user allows such victim behavior that technical measures on the part of the state and service organizations are practically unable to prevent the crime. These are situations in which the victim gives the password voluntarily or leaves the device turned on with the entered login and password, or commits immoral acts towards the criminal. This problem has been relevant since the beginning of global digitalization and it remains relevant, despite the widespread use of computer technology. Taking into account the fact that educational institutions pay very little attention to security in the Internet space, we consider it necessary to include the basic aspects of safe behavior in the curriculum. At the same time, classes should be both elderly and the young participants. Moreover, as it was noted, an increase in the number of users does not at all mean an increase in their literacy.

CONCLUSION

The study made it possible to formulate several important conclusions. The gender of the victim of unauthorized access to computer information does not have a significant impact on victimization and can hardly be used in predicting. In most of the reviewed cases the criminal and the victim did not know each other. However, 17.6% of the victims were not accidental, which means that their relationship directly influenced victimization.

The most risky are the areas of banking, social networks and mobile communications. Each of them is associated with working with personal data of users and generating large amounts of income, which attracts criminals. Apparently, this trend will continue in the near future, therefore, additional efforts should be focused on crime prevention in these areas.

Victim behavior is very typical for victims of unauthorized access to computer information, which most often manifests itself in following phishing links and careless actions with account passwords. However, this means that users have the possibility to defend themselves against crime. The reasons for such behavior may lie in the lack of computer literacy or neglect of the relevant rules of behavior, which should be taken into account by those implementing preventive measures.


In our opinion, the state should support commercial and non-commercial organizations that contribute to the prevention of computer crime, with the help of tangible and intangible forms of encouragement: tax mitigation, grants, advertising of the organization, and promotion of activities. At the same time, the main efforts should be focused on technical solutions and teaching the basics of safe behavior in the Internet space.

This study obviously does not cover all aspects of victimization and all characteristics of victims of unauthorized access to computer information. Nevertheless, the representative sample made it possible to study certain risks and offer recommendations for their neutralization. Further research using other methodologies may provide a more accurate and in-depth analysis of the behavior of victims of unauthorized access to computer information. It is believed it would be appropriate to study effectiveness of teaching basics of safe behavior in the Internet space and artificial intelligence systems designed to analyze suspicious activity in social networks. In addition, more cross-national comparative research on cybercrime victimization is needed. It would be useful to assess the correlation between the results of this study and those made in other countries. This will allow a better understanding of differences between victims and victimization, as well as development of the most effective cybercrime prevention measures.



REFERENCES

- [1] H. Trittin-Ulbrich et al. 'Exploring the dark and unexpected sides of digitalization: Toward a critical agenda' (2021) *Organization*, 28, 8-25.
- [2] B. Sturc et al. 'The Specifics and Patterns of Cybercrime in the Field of Payment Processing' (2022). *International Journal of Criminology and Sociology*, 9, 2021-2030
- [3] F. Miró-Llinares et al. 'Understanding target suitability in cyberspace: An international comparison of cyber victimization processes' (2020) *International Journal of Cyber Criminology*, 14, 139-155.
- [4] E. R. Leukfeldt et al. 'Exploring the needs of victims of cyber-dependent and cyber-enabled crimes' (2020) *Victims & Offenders*, 15, 60-77.
- [5] R. Milani et al. 'Exposure to cyber victimization: Results from a Swiss survey' (2022) *Deviant Behavior*, 43, 228-240.
- [6] M. Jiang, M. 'Cybersecurity policies in China'. In L. Belli (ed.) *CyberBRICS* (Springer: Cham, 2021), 183-226.
- [7] V. I. Gladkikh - I. N. Mosechkin, 'Problems of improving criminal law measures of counteracting crimes in the sphere of computer information' (2021) *Russian Journal of Criminology*, 15, 229-237.
- [8] J. Chigada - R. Madzinga, 'Cyberattacks and threats during COVID-19: A systematic literature review' (2021) *South African Journal of Information Management*, 23, 1-11.
- [9] K. Jaishankar, 'Cyber victimology: a new sub-discipline of the twenty-first century victimology'. In J. Joseph (ed.) *An International Perspective on Contemporary Developments in Victimology* (Springer: Cham, 2020), 3-19.
- [10] M. Näsi et al. 'Cybercrime victimization among young people: a multi-nation study' (2015) *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16, 203-210.
- [11] K. S. Choi, 'Computer crime victimization and integrated theory: An empirical assessment' (2008) *International Journal of Cyber Criminology*, 2, 308-333.
- [12] F. T. Ngo - R. Paternoster, 'Cybercrime victimization: An examination of individual and situational level factors' (2011). *International Journal of Cyber Criminology*, 5, 773-793.
- [13] T. Smith - N. Stamatakis, 'Cyber-victimization trends in Trinidad & Tobago: the results of an empirical research' (2021) *International Journal of Cybersecurity Intelligence & Cybercrime*, 4, 46-63.
- [14] H. T. N. Ho - H. T. Luong, 'Research trends in cybercrime victimization during 2010-2020: a bibliometric analysis' (2022). *SN Social Sciences*, 2, 1-32.
- [15] M. T. Whitty - T. Buchanan, 'The online romance scam: A serious cybercrime' (2012) *CyberPsychology, Behavior, and Social Networking*, 15, 181-183.
- [16] N. Akdemir, *Contextual vulnerabilities approach to understand victimization in cyberspace* (Kriter: Istanbul, 2021).
- [17] M. C. Bergmann et al. 'Cyber-dependent crime victimization: the same risk for everyone?' (2018). *Cyberpsychology, Behavior, and Social Networking*, 21, 84-90.
- [18] M. Junger et al. 'Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe' (2017) In *2017 international conference on cyber situational awareness, data analytics and assessment (Cyber SA)*, 1-8.
- [19] T. J. Holt - A. M. Bossler, 'Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization' (2009) *Deviant Behavior*, 30, 1-25.
- [20] C. Krasnay - P. B. Hámornik, 'Analysis of cyberattack patterns by user behavior analytics' (2018) *AARMS-Academic and Applied Research in Military and Public Management Science*, 17, 101-114.
- [21] D. Odunze, 'Cyber victimization by hackers: A criminological analysis' (2018) *Public Policy and Administration*, 8-15.
- [22] L. Ali et al. 'The effects of cyber threats on customer's behaviour in e-Banking services' (2017) *International Journal of e-Education, e-Business, e-Management and e-Learning*, 7, 70-78.
- [23] M. Dodel - G. Mesch, 'Cyber-victimization preventive behavior: A health belief model approach' (2017) *Computers in Human behavior*, 68, 359-367.
- [24] D. V. Zhmurov - R. N. Klyuchko, 'Cyber-Victimology as A New Reality of The Technotronic Society (Gender Research)' (2020) *Baikal Research Journal*, 11, 19-31.
- [25] V. V. Polyakov - A.V. Shiryaev, 'Forensic aspects of the identity of victims of cybercrime' (2018) In *Criminal procedure and forensic readings in Altai*, 164-172
- [26] N. Khomenko, 'On the Victimization of Cybercrime Victims' (2021) *Victimology*, 8, 143-148.
- [27] N. M. Alexandrina, 'Victimological characteristics of computer crimes committed against legal entities' (2019) *Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 45, 223-227.
- [28] V. Mayorov, 'Does Digitalization Affect Victimization in Today's Society?' (2022) *Victimology*, 9, 148-156.

- 
- [29] E. A. Rodina, 'General Social Prevention of Criminogenic Victimization of Internet Users' (2022) *Bulletin of the Saratov State Law Academy*, 146(3), 197-206.
- [30] V. Gladkikh, 'Prevention Of Crimes in The Field of Computer Security. In Almanac Lecture' (2022) *In May Legal Readings on the Yenisei*, 39-42.
- [31] Case 1-311 [2019] *Novy Urengoy City Court of the Yamalo-Nenets Autonomous Okrug (Russian Federation)*
- [32] Case 1-1069 [2017] *Central District Court of Chita (Russian Federation)*
- [33] Case 1-83 [2018] *Belebeevsky City Court of the Republic of Bashkortostan (Russian Federation)*
- [34] Case 1-897 [2018] *Shakhty City Court of Rostov Region (Russian Federation)*
- [35] Case 1-299 [2018] *Akhtubinsky District Court of the Astrakhan Region (Russian Federation)*
- [36] Case 1-268 [2017] *Leninsky District Court of Cheboksary (Russian Federation)*
- [37] Case 1-886 [2019] *Leninsky District Court of Tyumen (Russian Federation)*
- [38] Case 1-323 [2017] *Gagarinsky District Court of Sevastopol (Russian Federation)*
- [39] Case 1-421 [2018] *Leninsky District Court of Barnaul, Altai Krai (Russian Federation)*
- [40] Case 1-212 [2018] *Soviet District Court of Kazan (Russian Federation)*
- [41] E. A. Chiesa et al. 'Intimate partner violence victimization and parenting: A systematic review' (2018) *Child abuse & neglect*, 80, 285-300.
- [42] D. Freed et al. "A Stalker's Paradise" *How Intimate Partner Abusers Exploit Technology*' (2018) *In Proceedings of the 2018 CHI conference on human factors in computing systems*, 1-13.
- [43] Reynolds et al. 'Opportunity and self-control: Do they predict multiple forms of online victimization?' (2019) *American Journal of Criminal Justice*, 44, 63-82.