

Cybercrime Victimization

PhD. student **Dora ARIFI**¹

Professor **Besa ARIFI**²

Abstract

Digitization has taken over the whole world and it's terrifying. The reason behind this is that the Internet offers many options for its users, some of which are very productive. Unfortunately, it also creates a space for hackers to operate freely and achieve their goals. As the number of internet users is increasing, cybercrime victimization is at the highest rate every day. Cybercrime is a new term that defines illegal activity that involves a network, computer, or network device. Cybercrime is a criminal offense committed against individuals or institutions. Anyone can be a victim of cybercrime. As a result, combating this type of crime presents a new challenge for law enforcement. It is crucial to understand the risks and consequences to take appropriate measures to protect the victims of such crimes. The paper is prepared based on other works to finally conclude that cybercrime is a worldwide problem, and no one is immune to it. We must raise awareness of the possible consequences and prevent future cyber victimization before it's too late.

Keywords: cybercrime, cyber legislation, victims, cyberstalking, cybersecurity.

JEL Classification: K14, K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/12>

Please cite this article as:

Arifi, Dora & Besa Arifi „Cybercrime Victimization”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkcic (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 193-204.

1. Introduction

The Internet is a very powerful tool because it can change everything in a single second. For some users, the Internet brings pleasure and helps in a positive way to carry out work. It is entertaining and provides knowledge for all who are interested. For some people, the Internet is scary, unknown, and dangerous. The Internet today is burdened with information from various fields, including our private ones, because we as Internet users therefore of social networks, with the creation of accounts, and distribution of photos, videos, news, and thoughts,

¹ Dora Arifi - South-East European University, North Macedonia, da24612@seeu.edu.mk.

² Besa Arifi - South-East European University, North Macedonia, b.arifi@seeu.edu.mk.

we give information or data automatically for which, although it is considered to be protected when it comes to bank numbers, given identification, again part of the information we provide, are exposed at any moment to the risk of misuse by various hackers. Social networks are digital platforms that offer different ways of socialization communication, games, work, sharing funny content, etc. People should be careful of what they post on social media. Users post too much, providing personal information and making it easier for hackers to operate. Information on various fields can be found everywhere on the Internet, on websites, forums, books, and online works as well as on social networks. One of the main mistakes in why people become victims of cybercrime is the lack of knowledge regarding the policies of digital platforms and not utilizing privacy settings. Since social accounts are constantly at risk, we try to find the most effective solutions to prevent hacking and combat such crime with new methods, increase the awareness of some about the importance of the information we provide, etc. People sometimes forget that they publish so much data, making it accessible to everyone they know and don't know. Social media users often communicate with strangers with whom they share personal events and details. The scariest part of communicating with people who don't really know each other in person is the fact that they may often hide their true personalities. Some people tend to present a character built on lies and deception. In this way, hackers can easily plan threats, manipulation, and stalking, and cause much damage to victims. Often hackers and other cyber criminals present themselves as polite, ambitious, interested in relationships, and investments, and people dealing with different non-governmental firms or organizations for health, animals, children, etc.

2. Cybercrime is taking over the world

To understand the perspective of the victims of cybercrime (as well as the victims of what Nicole A. Vincent calls *cyberwrongs*³) it is first necessary to understand the offences; how they occur, and how the internet may enable perpetrators to commit them. Again, the dynamism of the cybersphere makes this task daunting given the dizzying speeds at which platforms and usage patterns materialize and dematerialise.⁴ Cybercriminals use the rapid connectivity of the internet to exploit the vulnerabilities of the network.⁵

Most people are unaware of this exploit, which makes bad individuals feel safe committing crimes in the digital era⁶. Hackers use social networks to

³ Nicole A. Vincent, *Victims of cybercrime: definitions and challenges*, in Elena Martellozzo, Emma A. Jane (eds.), *Cybercrime and its victims*, Routledge, London, New York, 2017, p. 27-42.

⁴ *Ibid.*, p. 33.

⁵ Emily Ngo, *Social Media: The Unseen Risks of Cybercrimes*, A Thesis Presented to the Faculty of Anna Maria College, 2020, <https://annamaria.edu/wp-content/uploads/2021/06/Emily-Ngo-Fall-2020.pdf>, p. 2.

⁶ Tariq Rahim Soomro, Mumtaz Hussain, *Social Media-Related Cybercrimes and Techniques for Their Prevention*, Applied Computer Systems, Volume 24 (2019): Issue 1 (May 2019), p. 9-17.

plan and as a tool to commit crimes. First, they think about the target and how they will commit the crime, collecting personal information of the victims because social networks present a whole ocean that serves data for each person very easily and very quickly, for that reason, it is said that they commit crimes in real time. Due to this a cybercriminal can gather all the information and can sell up to \$630 million yearly⁷. Victims will no longer have personal data.⁸ It hides the users' identity as well as not being able to face repercussions immediately.⁹ Computer crime is a new type of crime and also a unique one that differs from traditional crimes. At present, the risk of cybercrime can visualize in the form of offences analogous to the physical world, such as cyberbullying and online harassment which are termed as *cyber-enabled* crimes, or through security risks that affect the computer itself, such as malware infections, ransomware infections, and theft and misuse of personal data which is called *cyber-dependent* crimes.¹⁰

3. Types of cybercrimes

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks.¹¹ Cybercrimes can be easily placed into two categories; violent and nonviolent cybercrimes. Most of the cybercrimes are nonviolent offenses, because interaction is without any physical contact.¹² According to the author Vishi Aggarwal, 'Non-violent computer crimes are cyber theft (identity theft, piracy), cyber fraud, cyber trespass, and destructive cybercrimes such as cyber vandalism, and viruses, etc., crimes which are while violent computer crimes are cyber terrorism, cyberstalking, pornography, and cyberbullying.' Nonviolent crimes affect the financial and mental aspect, while violent ones, apart from having a negative impact on the mental aspect, endanger the well-being and life of the victims. Different categories of individuals are attacked virtually in different ways, for example, women and children are mostly targeted through cyberstalking, cyber threats by leaking their pictures, and text messages, harassment, and misuse of data for pornography. Men are also threatened in various ways for financial gain, and elderly people fall prey to viruses that are controlled by hackers. Since older people are not

⁷ Bir, A., & Sodhi, S. (2020). *Social media law & cybercrime*, pp. 28, 29.

⁸ Emily Ngo, *op. cit.*, p. 3.

⁹ *Ibid.*, p. 4.

¹⁰ P. Naveen Prabhu, K. Niranjana, *A Study on Cyber Crime Victims*, International Journal of Research Publication and Reviews, Vol. (2) Issue (9), 2021, p. 89, <https://www.ijrpr.com/v2i9.php> last accessed 01.03.2024.

¹¹ V. Karamchand Gandhi, *An Overview Study on Cybercrimes in the Internet*, Journal of Information Engineering and Applications, Vol. 2, No. 1, 2012, p. 1.

¹² Shruti Vishi Aggarwal, *Cybercrime victims: A comprehensive study*, International Journal of Creative Research Thoughts, Volume 6, Issue 2, 2018 p 641 the document is available at: https://ijcrt.org/viewfull.php?&p_id=IJCRT1807078, last accessed 01.03.2024.

internet experts, they often fall for the lies of hackers since they try to provide help for repairing the damages when in fact, they start stealing personal data such as collecting passwords into accounts to get access most of the time to their bank accounts. Companies, organizations, and institutions are also good targets of computer crime because it involves large sums of money. Hackers can weave the most detailed and advanced plans to achieve their goals at any cost. Victims of cybercrime are generally harmed financially. The consequences caused are also mental aspects because pressure, threats, fear, and stress are present at the time of the cybercrime process. For example, in the female gender, in most cases, the psychological consequences and PTSD are caused because hackers misuse and publish messages, videos, and pictures of them to push them to surrender and adhere to the plan they have woven to arrive at material gain. Famous and wealthy people face different kinds of cyber threats because most of the time, hackers decide to intercept their phone calls as a part of the plan to gain more information for their financial purposes. The data published without the victim's consent can be misused for a longer time by anyone since it can be accessible to any of the internet users. Millions of people and hundreds of businesses and organizations are victims of computer crime every year. The most frequent computer crimes that are committed and victimize individuals are: Cyber stalking – is very common nowadays. Cybercriminals target victims by using different types of social media through threats and harassment. The aim of stalking is to cause stress and fear. The reasons for cyberstalking may be hatred, obsession, and revenge. Cyber stalking can take many forms, including:

- harassment, embarrassment and humiliation of the victim;
- emptying bank accounts or other economic controls such as ruining the victim's credit score;
- harassing family, friends and employers to isolate the victim.¹³

Often the perpetrators are impossible to identify because they present themselves as anonymously by changing their identity on social networks and their IP address, making it impossible to find the location of the action. Hacking and Cracking – every act committed towards breaking into a computer and/or network is hacking.¹⁴ Hackers use their legal tools to commit crimes. On the contrary, crackers do not possess such tools, but by using someone else's tools, they damage the system and as a consequence, the victim. In many pieces of literature, crackers are known as 'bad people' because they undertake criminal actions for personal and financial reasons. On the other side, hackers are often hired by companies to control and change the company's systems and programs. Cyber pornography – it means the publication of erotic materials of victims on social networks, i.e. on the Internet. Many websites exhibit pornographic pictures, photos,

¹³ V. Karamchand Gandhi, *op. cit.*, p 1.

¹⁴ Kejal Chintan Vadza, *Cyber Crime & its Categories*, Indian Journal of Applied Research, Volume 3, Issue 5, 2011, p. 130, DOI:10.15373/2249555X/MAY2013/39.

writing, etc. Such materials can be produced quickly and cheaply through morphing or through sexual exploitation of women and children.¹⁵ Identity theft – impersonating to be someone else on the internet or creating a fake identity and then acquiring information from an individual is known as identity theft. Through identity fraud, purchases and transactions are carried out without the knowledge of the victim, leading him to great financial losses. Identity theft is carried out by hacking into the computers of individuals or organizations, using fake emails, using hacking to collect the necessary data, etc. Cyber trafficking – the impact of technology on trafficking of human beings is of particular concern during two stages of the trafficking process: recruitment and exploitation¹⁶. Plagiarism – the act of taking another person’s work without permission and using the same as ours. Plagiarism is punishable. Various systems detect works borrowed without permission. The more internet users there are, the more widespread this crime will be. The Oxford English Dictionary Online (OED Online) defines plagiarism as ‘the action or practice of plagiarizing; the wrongful appropriation or purloining, and publication as one’s own, of the ideas, or the expression of the ideas (literary, artistic, musical, mechanical, etc.) of another.’¹⁷ In order to avoid plagiarism, authors must give credit in any instance in which they use another author’s idea, opinion or theory; any facts, statistics, graphs or drawings; any pieces of information that are not common knowledge; quotations of another person’s actual spoken or written words; and paraphrased versions of another person’s spoken or written words.¹⁸ According to a cybersecurity report of 2022, it is said that “27% of Millennials and 34% of Gen Zers have lost their money or data due to harmful cyber activity, such as phishing, yet many of them fail to report the incidents or seek out cybersecurity training it”.¹⁹

¹⁵ Dr. Grace Varghese, *A sociological study of different types of cybercrime*, International Journal of Social Science and Humanities Research, Vol. 4, Issue 4, 2016, p. 603, the document is available at <https://www.researchpublish.com/papers/a-sociological-study-of-different-types-of-cyber-crime> last accessed 01.03.2024.

¹⁶ Dr. Paolo Campana, *Online and technology-facilitated trafficking in human beings. Summary and recommendations*, Council of Europe, 2022, p. 7, the document is available at <https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10c>, last accessed 01.03.2024.

¹⁷ Patience Simmonds, *Internet Resources: Plagiarism and cyber-plagiarism: A guide to selected resources on the Web*, ACRL College & Research Libraries News, Vol. 64 No. 6, 2023 the documents is available online at: https://crln.acrl.org/index.php/crl_news/article/view/20607/25112 last accessed 10.03.2024.

¹⁸ Nm Lehobye, *Plagiarism: Misconduct awareness on novice research within the cyberworld*, Potchefstroom Electronic Law Journal (PER/PELJ), Volume 13 No. 3, 2010 p. 496.

¹⁹ Paige Gerald, *Cybersecurity report finds cybercrime victims are often Millennials and Gen Zers*, Information Security, 2022, the document is available online at: <https://it.rutgers.edu/2022/10/17/cybersecurity-report-finds-cybercrime-victims-are-often-millennials-and-gen-zers/> last accessed 10.03.2024.

4. How do cybercriminals operate?

Cybercriminals also exploit the natural desires of humans to trust others to send unsolicited electronic mail to unsuspecting victims as though they originated from legitimate sources.²⁰ Because victims of cybercrime are an invisible constituency, they are often overlooked by policy-makers and those who assist victims of traditional criminal offenses. Yet the harms are substantial and deserve greater attention.²¹ Most of the time fraudsters and hackers try to gain the victim's trust to achieve their goals. They work hard for weeks or months until they betray the victim and get the money. For most cybercrimes, no physical contact takes place between perpetrator and victim, and in the case of online banking fraud, victims are often compensated for financial damage. Because victimization impact cannot be measured based on physical injury and not always on actual financial damage, the impact of cybercrime seems to be underestimated, or cybercrime is even considered a victimless crime.²² Concerns over online anonymity, privacy, and security are valid. It is difficult to determine who exactly is the person online or how protected a person's data is over the internet²³. Cybercriminals use the rapid connectivity of the internet to exploit the vulnerabilities of the network. Most people are unaware of this exploit, which makes bad individuals feel safe committing crimes in the digital era²⁴. Cybercriminals most of the time use methods to scare victims and cause panic and fears in order to make them guess and not think rationally or make a scam believable by making the victim think they are doing the right thing. Cybercrime perpetrators can operate alone, as a group, or even as a criminal organization. Today there are such organizations that actually function like any other organization. Some criminals use their skills and knowledge to damage computer equipment, and software or block programs by publishing photos and other illegal information. Cybercriminals use phishing and phishing to achieve their goals. They also use different methods to change databases on many websites without authorization. They manipulate data or gain information such as passwords, trade secrets, credit card numbers, and other sensitive personal and government information. To further reduce the chances of detection, and prosecution, cybercriminals often choose to operate in countries with

²⁰ Obinna J. Eze, John Thompson Okpa, Chukwuemeka Dominic Onyejebu and Benjamin Okorie Ajah, *Cybercrime: Victims' Shock Absorption Mechanisms*. From the edited volume Eduard Babulak Malware – Detection and Defense, 2022, the document is available online at: <https://www.intechopen.com/chapters/83682> last accessed 12.03.2024.

²¹ Victims of cybercrime Workshop, Council of Europe p. 1 the documents is available online at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803075c3> last accessed 11.03.2024.

²² Jildau Borwell, Jurjen Jansen and Wouter Stol, *Comparing the victimization impact of cybercrime and traditional crime: literature review and future research directions*, Journal Digital Social Research, Vol. 3, No. 3, 2021, p. 96.

²³ Emily Ngo, *op. cit.*, p. 1.

²⁴ Tariq Rahim Soomro, Mumtaz Hussain, *op. cit.*, p. 9.

weak or nonexistent cybercrime laws.²⁵ As more people engage in an ever-increasing variety of online activities and more businesses conduct their affairs online, it is predictable that there would be a rise in cybercrime.²⁶

5. Challenges of cybercrime

In many ways, it is unsurprising that cybercrime has increased in recent years. As technology becomes more sophisticated, so do cybercriminals, and cybercriminals now target individuals, businesses, healthcare facilities, educational institutions, and governments.²⁷ Although an increased number of studies on the impact of crime on victims have been conducted, most of the work in this field focusses on traditional crimes such as violent crime, theft and criminal destruction, rather than cybercrime.²⁸ Some experts believe that cybercrime is nothing more than ordinary crime committed by high-tech computers where computer is either a tool or target or both and other expert view that cybercrime is a new category of crime requiring a comprehensive new legal framework to address a unique nature of emerging technologies and the unique set of challenges that traditional crime does not deal with such jurisdiction, international cooperation, intent and the difficulty of identifying a perpetrator²⁹. The challenges of the digital age and for the investigation of electronic crime or cybercrime or computer crime are numerous and diverse, and include:

Bridging multi-jurisdictional boundaries; Retaining and preserving evidence; Acquiring appropriate powers decoding encryption Proving Identity Knowing where to look for evidence Tackling the tools of crime and developing tools to counter crime Rethinking the costs and priorities of investigations responding to crime in real time coordinating investigative activities improving training at all levels of the organization developing strategic partnerships and alliances Improving the reporting of electronic crime Enhancing the exchange of information and intelligence Acquiring. Developing and retaining specialist staff; and avoiding “tech lag” (or getting access to cutting-edge technology).³⁰

Considering the importance of the internet in today’s world, experiencing a crime online might cause severe psychological issues in the individual (from

²⁵ Kate Brush, Michael Cobb, *Cybercrime, TechTarget*, 2021, revised 2024, the document is available online at: <https://www.techtarget.com/searchsecurity/definition/cybercrime> last accessed 14.03.2024.

²⁶ James Hawdon, *Cybercrime: Victimization, Perpetration and Techniques*, American Journal of Criminal Justice, 2021, vol. 46, <https://doi.org/10.1007/s12103-021-09652-7>, p. 838.

²⁷ *Ibid*, p. 837–838.

²⁸ Jildau Borwell, Jurjen Jansen, Wouter Stol, *op. cit.*, pp. 86–87.

²⁹ Neelesh Jain, Vibhash Shrivastava, *Cybercrime changing everything – an empirical study*, International Journal of Computer Application, Issue 4, Volume 1, 2014, p. 77, the document is available at https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY last accessed 01.03.2024.

³⁰ *Ibid*, p. 82.

loss of trust to symptoms of post-traumatic stress disorder – PTSD – or suicide), as it potentially would after an offline crime.³¹ Cybercrime seems to challenge the principles upon which our conventional understandings of criminal harm and justice are based, because it results in the globalization of crime, new forms of victimization, extensive data trails, and changes in the organization of criminal activities.³² A restorative orientation is both more consistent with the policy objectives of ‘putting the victims’ first’ and meeting victims’ needs and, given the challenges of policing global cybercrime and the low levels of investigatory and prosecutorial success, a more meaningful response to these crime types.³³ Finally, given the stigma associated with both being victimised and victims’ self-identification with states of ‘vulnerability’ more generally, while a vulnerability framework may be useful to understand and respond to victimisation in its wider context, framing the victim response as one that builds resilience may be more effective at reaching victims.³⁴

6. Cybercrime impact on victims

Cybercrime’s victims are very common nowadays. Examples of the unique cybercrime victimization elements are the scale on which victims can be approached, the technology that is part of the offense and its anonymity, intangibility, and remoteness.³⁵ Cybercrime generally leaves negative consequences for the victim like any other crime, but the damage is much longer. Any material published without the victim’s consent remains on the Internet for a long time. Anyone can access, misuse, and publish the victim’s photographs, videos, and other personal materials. The victims do not face fear, stress, and depression from this criminal activity but also must deal with the ‘victim blaming’ phase, where society blames the victim for the activity and deserves consequences. There are many cases where photos, videos, and other data are published to the victims, destroying their careers, family, marriage, and so on. Such a crime can happen through sending an email, call, advertisement, etc. It is crucial to take preventive measures and notice unusual activities on time. For example, we are logged out from our social media unexpectedly or cannot complete a bank transaction. In

³¹ Louisa von der Ahe, *Mental Wellbeing and Cybercrime: The Psychological Impact of Cybercrime on Victims*, University of Twente, 2022, p. 4, the document is available at <https://essay.utwente.nl/91014>, last accessed 01.03.2024.

³² Jildau Borwell, Jurjen Jansen and Wouter Stol, *op. cit.*, p 88.

³³ Sara Correia, *Cybercrime victims: victim policy through a vulnerability lens*, Cyber Threats Research Centre, Swansea University, 2021, p. 15 the document is available at: Correia, Sara, *Cybercrime Victims: Victim Policy through a Vulnerability Lens* (August 2, 2021). Available at SSRN: <https://ssrn.com/abstract=3897927> or <http://dx.doi.org/10.2139/ssrn.3897927> last accessed 01.03.2024.

³⁴ *Ibid*, p. 15.

³⁵ Jildau Borwell, Jurjen Jansen, and Wouter Stol, *The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory*, Sage Journals Volume 40, Issue 4, 2021, p. 3. <https://doi.org/10.1177/0894439320983828>.

such a way, when we feel that someone else controls our social networks or bank accounts, they understand that we have fallen victim to hackers and cybercrime. In the first moments, victims face panic and inexplicable fear because the fate of accounts and money is unknown. In some ways, a cyber-attack can feel like the digital equivalent of being robbed, with a corresponding wave of anxiety and dread.³⁶ Depending on the cybercrime, victimization may require law enforcement, medical, or psychiatric assistance because victims may become suicidal, depressed, nervous, anxious, fearful, or afraid.³⁷ Victimization can happen more than once. If the victim does not take certain protective measures, he may again fall victim to the same or different cyber-attacks. Electronic devices such as laptops used away from secure internet connections are vulnerable to external threats, since fraudsters sometimes offer free Wi-Fi connections or interfere with legitimate Wi-Fi connections to steal the personal information of individuals at airports or shopping malls.³⁸ Social media tools, a platform that is very open to manipulation and crime, also cause trust issues, especially due to the potential of creating fake profiles, fictitious and suspicious identities. When the texts, images, animated images, etc. shared without paying attention to the language used on social media platforms are used in an uncontrolled manner and spread to large masses, it creates a huge data cloud and causes content density.³⁹ Social networks when used in an uncontrolled or illegal manner bring problems and increase the predispositions for cyber victimization.⁴⁰ In an interview conducted (01.03.2024) with an 18-year-old female victim for the matter of the research, we see what trauma victims of computer crime experience and how much society should support them.

Q: What type of cybercrime have you been victimized by? When did it happen?

A: Hacking and publishing my photos. It happened a year ago.

Q: How did you feel in those moments?

A: My friends notified me about the photos published. They were very

³⁶ Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass, 2022 the documents is available online at: <https://blog.lastpass.com/posts/2022/08/the-psychological-impact-of-cyber-attacks> last accessed 15.03.2024.

³⁷ Claudia San Miguel, Kristina Morales, and Marcus Antonius Ynalvez, *Online Victimization, Social Media Utilization, and Cyber Crime Prevention Measures*, *Asia-Pacific Social Science Review* 20(4), p. 124, the document is available at https://rio.tamtu.edu/soc_sci_facpubs/7/, last accessed 15.03.2024.

³⁸ N. Akdemir, *Exploring the Human Factor in Cyber-enabled and Cyber-dependent Crime Victimization: A Lifestyle Routine Activities Approach*, Durham Research Online, 2020, p. 13, the document is available at <https://durham-repository.worktribe.com/output/1299418/exploring-the-human-factor-in-cyber-enabled-and-cyber-dependent-crime-victimisation-a-lifestyle-routine-activities-approach>, doi: <https://doi.org/10.1108/intr-10-2019-0400> last accessed 15.03.2024.

³⁹ Murat Eddogdu, Murat Kocuyigit, *The Correlation between Social Media Use and Cyber Victimization: Research on Generation Z in Turkey*, *Connectist: Istanbul University Journal of Communication Sciences*, Istanbul 2021, p. 3.

⁴⁰ *Ibid*, pp. 3-4.

personal, sent from my side on chats. I felt terrible. I cried. I was afraid of people. I isolated myself from everyone for a long time.

Q: What happened to your photos?

A: My social account was closed. My friends reported the account. Hackers posted everything on my account. Since then, I haven't noticed any criminal activity. I don't know if someone from my friend's list has the photos yet. It is scary.

7. Conclusion

Cybercrime is a widespread crime. Cyber-attacks are getting more advanced. Governments must take effective measures to prevent and slow down the cybercrime consequences by raising awareness, developing strategies, and improving current laws for combating cybercrime. In addition, organizing training for officers and other cybersecurity workers will be a preventive measure.

Maybe we will never be victims of cybercrime, but that doesn't mean we aren't in danger. Hackers are everywhere around us. Every moment by using their 'weapons' they can operate and cause damage. Therefore, I specifically mentioned the need to increase awareness because most people do not know the types of cybercrime except the 'hacking' type and are not informed about the basic preventive measures that they should take to protect themselves from victimization, such as using strong passwords, check secure websites, install and update anti-viruses, never open spam e-mails, never share personal information in suspicious sites, we need to secure our home network, always use a secure internet connection, never save passwords in the browsers, keep most of the personal information private on social media, make backups on data, etc. It is very important to educate children and teenagers since mostly they can easily fall victim to such crimes since they can be manipulated in many ways by cyber criminals.

Bibliography

1. Aggarwal, Shruti Vishi, *Cybercrime victims: A comprehensive study*, International Journal of Creative Research Thoughts, Volume 6, Issue 2, 2018, the document is available at: https://ijcrt.org/viewfull.php?&p_id=IJCRT1807078, last accessed 01.03.2024.
2. Ahe, Louisa von der, *Mental Wellbeing and Cybercrime: The Psychological Impact of Cybercrime on Victims*, University of Twente, 2022, the document is available at <https://essay.utwente.nl/91014>, last accessed 01.03.2024.
3. Akdemir, N., *Exploring the Human Factor in Cyber-enabled and Cyber-dependent Crime Victimization: A Lifestyle Routine Activities Approach*, Durham Research Online, 2020, the document is available at <https://durham-repository.worktribe.com/output/1299418/exploring-the-human-factor-in-cyber-enabled-and-cyber-dependent-crime-victimisation-a-lifestyle-routine-activities-approach>, doi: <https://doi.org/10.1108/intr-10-2019-0400> last accessed 15.03.2024.

4. Bir, A., & Sodhi, S. (2020). *Social media law & cybercrime*.
5. Borwell, Jildau, Jurjen Jansen & Wouter Stol, *Comparing the victimization impact of cybercrime and traditional crime: literature review and future research directions*, Journal Digital Social Research, Vol. 3, No. 3, 2021.
6. Borwell, Jildau, Jurjen Jansen & Wouter Stol, *The Psychological and Financial Impact of Cybercrime Victimization: A Novel. Application of the Shattered Assumptions Theory*, Sage Journals Volume 40, Issue 4, 2021, <https://doi.org/10.1177/0894439320983828>.
7. Brush, Kate & Michael Cobb, *Cybercrime, TechTarget*, 2021, revised 2024, the document is available online at: <https://www.techtarget.com/searchsecurity/definition/cybercrime>, last accessed 14.03.2024.
8. Campana, Paolo, *Online and technology-facilitated trafficking in human beings. Summary and recommendations*, Council of Europe, 2022, the document is available at <https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10c>, last accessed 01.03.2024.
9. Correia, Sara, *Cybercrime victims: victim policy through a vulnerability lens*, Cyber Threats Research Centre, Swansea University, 2021, the document is available at: Correia, Sara, *Cybercrime Victims: Victim Policy through a Vulnerability Lens* (August 2, 2021). Available at SSRN: <https://ssrn.com/abstract=3897927> or <http://dx.doi.org/10.2139/ssrn.3897927> last accessed 01.03. 2024.
10. Eddogdu, Murat & Murat Kocyyigit, *The Correlation between Social Media Use and Cyber Victimization: Research on Generation Z in Turkey*, Connectist: Istanbul University Journal of Communication Sciences, Istanbul 2021.
11. Eze, Obinna J., John Thompson Okpa, Chukwuemeka Dominic Onyegbu & Benjamin Okorie Ajah, *Cybercrime: Victims' Shock Absorption Mechanisms*. From the edited volume Eduard Babulak Malware – Detection and Defense, 2022, the document is available online at: <https://www.intechopen.com/chapters/83682>, last accessed 12.03.2024.
12. Gandhi, V. Karamchand, *An Overview Study on Cybercrimes in the Internet*, Journal of Information Engineering and Applications, Vol. 2, No. 1, 2012.
13. Gerald, Paige, *Cybersecurity report finds cybercrime victims are often Millennials and Gen Zers*, Information Security, 2022, the document is available online at: <https://it.rutgers.edu/2022/10/17/cybersecurity-report-finds-cybercrime-victims-are-often-millennials-and-gen-zers/>, last accessed 10.03.2024.
14. Hawdon, James, *Cybercrime: Victimization, Perpetration and Techniques*, American Journal of Criminal Justice, 2021, vol. 46, <https://doi.org/10.1007/s12103-021-09652-7>.
15. Jain, Neelesh & Vibhash Shrivastava, *Cybercrime changing everything – an empirical study*, International Journal of Computer Application, Issue 4, Volume 1, 2014, the document is available at https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY last accessed 01.03.2024.
16. Lehobye, Nm, *Plagiarism: Misconduct awareness on novice research within the cyberworld*, Potchefstroom Electronic Law Journal (PER/PELJ), Volume 13, No. 3, 2010.
17. Miguel, Claudia San, Kristina Morales & Marcus Antonius Ynalvez, *Online Victimization, Social Media Utilization, and Cyber Crime Prevention Measures*, Asia-Pacific Social Science Review 20(4), the document is available at <https://>

- rio.tamtu.edu/soc_sci_facpubs/7/, last accessed 15.03.2024.
18. Ngo, Emily, *Social Media: The Unseen Risks of Cybercrimes*, A Thesis Presented to the Faculty of Anna Maria College, 2020, <https://annamaria.edu/wp-content/uploads/2021/06/Emily-Ngo-Fall-2020.pdf>.
 19. Prabhu, P. Naveen & K. Niranjana, *A Study on Cyber Crime Victims*, International Journal of Research Publication and Reviews, Vol. (2) Issue (9), 2021, <https://www.ijrpr.com/v2i9.php> last accessed 01.03.2024.
 20. Simmonds, Patience, *Internet Resources: Plagiarism and cyber-plagiarism: A guide to selected resources on the Web*, ACRL College & Research Libraries News, Vol. 64 No. 6, 2023 the documents is available online at: https://crln.acrl.org/index.php/crl_news/article/view/20607/25112 last accessed 10.03.2024.
 21. Soomro, Tariq Rahim & Mumtaz Hussain, *Social Media-Related Cybercrimes and Techniques for Their Prevention*, Applied Computer Systems, Volume 24: Issue 1 (May 2019), p. 9-17.
 22. Steel, Amber, *The Psychological Impact of Cyber Attacks*, LastPass, 2022 the documents is available online at: <https://blog.lastpass.com/posts/2022/08/the-psychological-impact-of-cyber-attacks> last accessed 15.03.2024.
 23. Vadza, Kejal Chintan, *Cyber Crime & its Categories*, Indian Journal of Applied Research, Volume 3, Issue 5, 2011, DOI:10.15373/2249555X/MAY20 13/39.
 24. Varghese, Grace, *A sociological study of different types of cybercrime*, International Journal of Social Science and Humanities Research, Vol. 4, Issue 4, 2016, the document is available at <https://www.researchpublish.com/papers/a-sociological-study-of-different-types-of-cyber-crime> last accessed 01. 03.2024.
 25. Vincent, Nicole A., *Victims of cybercrime: definitions and challenges*, in Elena Martellozzo, Emma A. Jane (eds.), *Cybercrime and its victims*, Routledge, London, New York, 2017, p. 27-42.