HANDBOOK FOR RECOGNIZING AND PREVENTING CYBER-VIOLENCE AND ACQUIRING SKILLS FOR APPLYING CYBER SECURITY MEASURES

Handbook for recognizing and preventing cyber-violence and acquiring skills for applying cyber security measures

Author: Giljman Osmani Musliji

Analytica think tank Skopje

December 2023

CONTENT

PURPOSE OF THE HANDBOOK

In today's digital age, the need for comprehensive cyber security education and effective strategies to prevent cyber violence has never been more crucial. The aim of this Handbook is to empower young people and teachers with the knowledge and skills necessary to safely navigate the digital and online world, understand cyber security measures and develop impactful school programs to prevent cyber-violence and ensure a safe cyber environment for students.

Specific objectives of the handbook:

Empowerment through Education: This Handbook will provide young people and teachers with a solid knowledge base on cyber security measures, online safety and the potential risks associated with cyber violence. Through active use of the Handbook, a culture of digital literacy and responsible online behavior will be fostered.

Skills development: This Handbook will equip users (teachers, school support services, students, parents and others) with practical skills to effectively implement cyber security measures, including password management, safe browsing habits and an understanding of privacy settings on different platforms. The handbook will enable teachers to integrate cyber security concepts into their curricula, ensuring students acquire the essential skills to safely navigate the digital landscape.

Cyberbullying prevention: This Handbook aims to raise awareness of the various forms of cyber violence, its impact on individuals and the wider community. Using the Handbook will provide resources and strategies for teachers to create and implement school programs that address cyber violence, fostering a safe and inclusive online environment.

Collaboration and support: Application of the Handbook will facilitate collaboration between teachers, parents and students to create a unified approach to cyber security and cyber violence prevention.

By achieving these goals, our Handbook aims to contribute to the development of a digitally resilient generation that can harness the benefits of technology while responsibly and ethically navigating potential pitfalls.

The handbook was prepared as part of the project *"Strengthening capacity of young people and teachers to apply cyber security measures and develop effective school programs to prevent cyber violence"*, implemented by think tank Analytica Skopje, in the period from September 2023 to February 2024.

METHODOLOGY FOR PREPARING OF THE HANDBOOK

This Handbook was developed using a multi-method methodology aimed at diagnosing primary data, experiences, perspectives and insights related to cyber security and cyber violence. The Handbook development process involved a combination of quantitative and qualitative research methods to provide a solid evidence-based foundation for the Handbook's content. The following methodologies were used:

1. Preliminary Research: An extensive review of existing cyber security and cyber violence prevention handbooks, educational materials, and relevant literature was conducted at the beginning of the development of the Handbook to identify gaps and areas for improvement. Secondary data sources were analyzed to gain insight into current trends, challenges and best practices in cyber security education and cyber violence prevention.

2. Survey methodology (research): In order to gather extensive knowledge from students, a structured survey was conducted on 507 students from five (5) schools from urban and rural areas. This quantitative approach enabled the systematic collection of data on students' digital habits, level of awareness and experiences with cyber violence. The results of the research provided a quantitative basis for understanding the prevailing trends and informing the content of the Handbook.

3. Focus groups: In order to delve deeper into the issue of cyber violence and cyber security, focus groups were conducted separately with both teachers and students, during the conducted trainings and workshops. These qualitative discussions allowed participants and teachers to share personal experiences, challenges and perspectives. The qualitative data obtained from the focus groups played a key role in shaping the content of the Handbook.

4. Data analysis: Collected data from the survey and qualitative findings from focus groups were subjected to analysis. Both quantitative and qualitative methods of analysis were employed to identify patterns, recurring topics and key findings. This rigorous analysis laid the foundation for synthesizing information and drawing meaningful conclusions that guided the development of the Handbook.

5. Handbook content development: Informed by research results and qualitative insights, the content of the Handbook was precisely crafted to address specific needs and issues identified in the research process. The integration of survey data and qualitative perspectives enabled a holistic approach to content development, ensuring that the Handbook responds to a wide range of user requirements.

ABOUT THE PROJECT

This Handbook was developed as part of the Project "Strengthening capacity of young people and teachers to apply cyber security measures and develop effective school programs to prevent cyber violence" and it was implemented by think tank Analytica Skopje, and financially supported by the Embassy of Canada in Serbia, North Macedonia and Montenegro. The project has a duration of 6 months, starting from September 2023 and ending in February 2024. The project includes a total of five schools, of which three secondary schools in the territory of the City of Skopje and two primary schools in the territory of the Municipality of Karposh.

The main goal of the project is to increase the use of cyber security measures among students and to create a network of trained teachers/educators who will disseminate the knowledge to other school communities.

Within the project, 7 activities are planned, namely:

- A.1. Investigation of knowledge among young people about cyber security
- A.2. Preparing of analysis with recommendations and measures to improve the situation with cyber security;
- A.3. Two-day training for teachers and representatives from civil society organizations and preparation of a proposed program for schools;
- A.4. Two-day training for peer educators;
- A.6. Workshops with young people and formation of peer education clubs;
- A.7. Designing and technical editing of a mobile application.
- A.8. Final conference to share project results and
- A.9. Social media campaign

With its implementation, the following results are expected to be achieved:

- R1. Conducted research and identified knowledge among young people about the challenges of the digital transformation process and digital security;
- R2. Designed and published a cyber security handbook intended for teaching staff, students and parents;
- R3. Increased cooperation of civil society organizations and relevant institutions with educational institutions and young people, as well as promotion of their role in creating a safer environment for young people;
- R.4. Trained 25 professors to implement innovative programs in schools in the field of youth cyber security;
- R5. 25 peer educators trained and 5 informal clubs formed in 5 schools from the target region;
- R.6. Campaign content (infographics, promotional press conference);
- R.7. Created a mobile application with an educational and informative character;

LITERATURE REVIEW

In an era dominated by digital technologies, educational institutions face the dual challenge of ensuring the safety of students and teachers in the virtual realm while reaping the benefits of technological advancements. This literature review explores the interrelated topics of cyber violence and cyber security, with a specific focus on students and teachers in educational settings.

The field of professional literature in the field of cyber violence and cyber-security of students and teachers has achieved significant contributions from prominent researchers and organizations. Researchers like R.A. Sabelle, J. W. Patchin and S. Hinduja[1], have played a key role in advancing our understanding of cyber violence, especially the books: Cyberbullying myths and realities, Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying, and Bullying, Cyberbullying, and Suicide.[2] Their joint efforts have resulted in numerous influential papers and books that delve into the complexities of online bullying and prevention strategies. These books provide a comprehensive examination of the cyber violence, exploring prevention measures and response strategies outside of traditional school settings. Also, these authors' research delves into the interdependence of violence, cyber violence, and its potential links to suicidal ideation.

The Pew Research Center[3], a well-respected institution, regularly publishes comprehensive reports on internet security, digital privacy and the prevalence of online harassment. The Teens and Technology[4] report focuses on technology use patterns among teenagers, shedding light on their online activities and the challenges they face. This report provides valuable insights into the evolving landscape of online threats facing children and educators.

In the area of children's online safety, the UNICEF Report[5] addresses the overall impact of the digital world on children, covering aspects of safety, well-being and development.

1 Computers in Human Behavior 29(6):2703-2711, Journal Review: Cyberbullying myths and realities, November 2013, authors R.A. Sabelle, J. W. Patchin and S. Hinduja.

2 Hinduja, S., & Patchin, J. W. (2018). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. Corwin Press.Hinduja, S., & Patchin, J. W. (2015). Bullying, Cyberbullying, and Suicide. Archives of Suicide Research.

3 The State of Online Harassment, January 2021, Pew Research Center, available at: https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

4 "Teens and Technology 2013", ,Pew Research Center

5 "Children in a Digital World" (2017), UNICEF

Organizations such as the European Union Cyber Security Agency (ENISA) and the UK's National Cyber Security Center (NCSC) have a key role to play in the field of cyber security. The ENISA report focuses on promoting cyber hygiene practices among children to improve their online safety.[6] The NCSC[7] report specifically examines teachers' cyber awareness and practices, offering insight into their perspectives and challenges. It also offers guidance on ensuring the cyber safety of children and young individuals.

Academic journals such as The Journal of School Violence[8] often feature studies related to cyber violence and school violence. These sources collectively form a rich body of knowledge, providing educators, policymakers, and parents with valuable insights and tools to address the challenges posed by cyber violence and strengthen cyber security in educational settings.

In the Macedonian context, the Agency for Electronic Communications MKD-CIRT, from the research carried out in 2019, prepared a brochure entitled "Cyber Security at Home, Guide for Parents, Educators and Children", where, among other things, they point out that Internet users in the country are the most concerned about the dangers of identity theft, hacking of social media accounts and online shopping scams. According to the same survey, parents believe that the most important measures that should be taken to protect children on the Internet are conversation and education of children, parents' familiarity with children's activities on the Internet, as well as limiting the time children spend on the Internet.[9]

The above sources and literature convey important information about the worrying state of cyber security and cyber violence.

6 Cyber Hygiene for children" (2018): ENISA
7 "Cyber Aware Teacher Survey Report" (2020), NCSC
8 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ojp.gov/pdffiles1/ojjdp/grants/217918.pdf
9 https://mkd-cirt.mk/wp-content/uploads/2021/03/VtoraBroshuraPrint.pdf

INTRODUCTION

We live in a time where much of our lives, personal and professional, are exposed to the digital world of the Internet. We do our daily tasks online, like our banking, shopping, bill paying, social planning, and even parts of our work in the digital world.

Although the benefits of using the Internet are enormous, we must be cautious about the dangers that the digital world hides. The most common dangers are: the behavior of children on the Internet, inappropriate and untrustworthy content, making contact with cyberbullies and people who aim to abuse the contacts, legal and financial dangers, unauthorized access and use of our personal data, etc.

Due to this and the excessive exposure of children and adults in the digital world, and the fact that the Internet is used in many places through the availability of multiple devices: at home, at school, with friends, it is necessary to develop an approach that will include multiple stakeholders for the proper use of the Internet, including school staff, parents/guardians and students, i.e. young people. Therefore, in the following, we will refer to the dangers hidden by the Internet and its use, as well as the role of various stakeholders in protecting young people and students from these dangers.[10]

Source: https://www.fenews.co.uk/resources/why-social-media-is-effective-for-business/

10 Priracnik-za-spravuvanje-so-kiber-nasilstvo-mk.pdf

For both students and teachers, the threats that circulate in cyber space are the excessive amount of information that is not known whether it is correct or incorrect and it is also not known how reliable the source of that information itself is. Hence, it is necessary for schools to provide a team of professional teachers who will be trained and promote methods and ways of prevention and coping in the chaotic cyber space, and the threats they are exposed to, such as cyber violence and cyber security.

Also, through cooperation with parents and their education, safe use of the Internet will be promoted.

Source: https://www.freepik.com/premium-vector/teamwork-collaboration-banner-with-colored-line-icons-team-goal-inspiration-career-typography-infographics-concept-team-work-isolated-vector-illustration_20412457.htm

CONCEPT OF PEER VIOLENCE

"The 20th century will be remembered as a century marked by violence. It burdens us with a legacy of mass destruction, violence inflicted on a scale never seen or possible before in human history. We owe our children a life free from violence and fear. To ensure this, we must be relentless in our efforts not only to achieve peace... but also to address the roots of violence. Only then will we transform the legacy of the last century from a crushing burden into a lesson for caution" - Nelson Mandela, Foreword to the World Health Organization's World Report on Violence and Health, 2002.[11]

The World Health Organization's World Report on Violence and Health (WRVH) defines violence as: "The intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community that either results in or is likely to result in injury, death, psychological harm, maldevelopment or deprivation".[12]

Peer violent behaviors, whether virtual or face-to-face, have a negative impact not only on the victims, on the witnesses, but also on the perpetrators themselves. Peer violence, i.e., bullying, is a form of aggressive behavior over a long period of time and is repeated directed at the same person. In other words, it can be defined as: deliberate, conscious negative behavior with the intention of hurting a person or a specific group, with the intention of causing intimidation, humiliation or damage to reputation. The bully always has more power than the victim, a behavior that cannot be justified by anything.

Peer violence is not: a one-time incident that, nor is it a friendly argument, argument or disagreement, accidental or accidental infliction of pain, friendly teasing or misunderstanding, violent resolution of a clash of attitudes between friends of the same strength.

11 Foreword to the World Health Organization's World Report on Violence and Health, 2002
12 https://worldbeyondwar.org/mk/types-of-violence/

Types of peer violence:

- Verbal/non-verbal – name-calling, mocking, belittling, insults, threatening looks, grimaces, ridicule, unwanted touching of a sexual nature, stalking, blackmailing;
- Physical – hitting, pushing, knocking down, stealing and destroying objects;
- Social – gossiping, avoiding, ignoring, isolating, spreading lies and rumours, exclusion;
- Electronic (cyberbullying) - sending, posting or sharing negative, harmful, false or malicious content about someone else using electronic devices.

CYBER VIOLENCE

Although the benefits of using the Internet are enormous, we must be cautious about the dangers that the digital world hides. The most common dangers are: the behavior of children on the Internet, inappropriate and untrustworthy content, making contact with cyberbullies and people who aim to abuse the contacts, legal and financial dangers, unauthorized access and use of our personal data, etc.

As a result of the above reasons and threats, we are aware that each of us can easily become a target of attacks and a victim of violence in the cyber space.

Cyber violence occurs through digital devices such as mobile phones, computers and tablets. Cyber violence can take place via SMS, text messages and applications or online on social media, forums or games where people can view, participate or share content. This violence includes sending, posting or sharing negative, harmful, false or malicious content about someone else. Sometimes cyber violence crosses the line into illegal or criminal behavior.

TYPES OF CYBER VIOLENCE

Cyber pursuing

This type of online peer violence is when the victim is constantly followed through social networks and is sent all kinds of messages or snap/story reactions in the form of threats, insults or lies. Then, certain photos of the victim are downloaded, digitally altered using appropriate applications and used to further humiliate or threaten. Most of the children who commit peer violence use this form, because they feel untouchable and think that there are no real consequences if the violence is done digitally. Therefore, it is very important to make children aware that once they publish something on the Internet, it is impossible to control it. Even things that are deleted can exist in many electronic copies elsewhere and reappear.

Cyber stalking

This type of cyberbullying is when someone uses technology to repeatedly harass, intimidate and threaten someone. Cyberstalkers may follow their victims and try to meet them. Many cases of cyberstalking involve adults (pedophiles) finding teenagers to have sex with them.

Anonymous and false representation

Many schools have problems with such "gossip" groups through the social network Instagram, Facebook, TikTok and the like. Typically, a student will form a group that they name after the school they attend and then attract hundreds of students as members who leave anonymous messages. These messages can be extremely distasteful and insult and belittle children in a shockingly cruel way. To make things even more real and insulting, some of the students take screenshots and share them with the victim who is the object of the taunting, which further inflames the matter.

Often times, the student/victim of this kind of bullying uses prejudice to guess who might be writing the bad things around them and often that child will also start a similar campaign on social media to get revenge. In this way, the victim also becomes a bully, so that negative circle takes on an even deeper dimension.

Disclosure, fraud, impersonation and blackmail

Disclosure means the intentional and public sharing of sensitive, private or embarrassing information about a particular child to other children or to different groups. Children often know how to confide in or send certain

important data or images to other children, and then screenshots/videos are made of them to be forwarded to completely third parties.

This is where another form of cyber violence known as deception comes into play, according to which the child bully "befriends" with the victim in order to extract certain things and information, which will later be used to escalate peer violence.

On the other hand, impersonation, or frapping, is when a child logs into another child's user account and begins a campaign of posting and sharing inappropriate content to all friends and followers. It could be embarrassing statements, insults, or some links that have inappropriate content.

As one of the worst and most evil forms of cyber violence is online blackmail where, for example, compromising photos of the victim are used and humiliating services are demanded from the same; if the child does not agree to do what is asked of him, the bully threatens to send the photos to x people, in order to defame and humiliate him in front of everyone he knows.

Harrasment

Harassment involves repeatedly sending malicious, abusive or threatening messages to an individual or group online. This can be done to victims publicly or privately.

Trolling

Trolling is a deliberate act, intended to provoke a response or reaction, through the use of some type of inflammatory statement - such as the use of insults or hate speech - in an online forum. Trolling is often done out of the troll's pleasure in upsetting others.

Denigration

This type of cyberbullying happens when someone posts rumors and gossip about someone online. Cyberbullies use disparagement in order to destroy the victim's relationships and reputation.

Exclusion

Exclusion is the creation of groups or events on digital platforms or communication platforms and excluding someone from them. This can also happen by not tagging someone in a photo or inviting them to an event, as well as excluding someone from an online conversation.

There are many reasons why students may engage in these behaviors, including boredom, revenge, anger, and to elicit reactions from their victims.

Additionally, the very anonymous nature of the internet makes it easy for people to bully others online, especially if they are social outcasts themselves who lack the courage to do so face-to-face.

Possible reasons for violence

- Excessive exposure to violence (through TV, video games, the general socio-cultural context in which we live)
- The lowered threshold of tolerance, and open and covert violence, as well as violent communication among young people, become a way of living and communicating.
- A large part of us are not even aware that what is happening around us is actually violence, as well as teachers and professional services hardly or do not recognize peer violence at all, both virtual or classic, and do not react promptly and appropriately to preventing it.

WHAT IS INTERNET PRIVACY

Do you ever wonder who collects our personal information and how? What information do they need, what do they do with our data, who do they share our secrets with, and do we even have privacy in the virtual world we are exposed to every day?

Our privacy is important because it gives us the space we need to develop as human beings. Privacy gives us the freedom to behave, to read, learn and express without worrying about who can see or hear, it means not feeling judged for our behaviours. It gives us the opportunity to give our trust to others so that we can shop, socialize, be intimate with each other and form the virtual connections that keep our communities strong, our democracy functioning, and our lives enriched. If we do not have that privacy, we cannot function properly as a society or as individuals.

Internet privacy includes the right to personal information regarding the storage, use, provision to third parties and display of personal information over the Internet. Internet privacy is a subset of data privacy. Privacy concerns have been around since the beginning of computer networking.[13]

Digital literacy is one of the eight key competencies in compulsory education, and the acquisition of digital media literacy skills can be considered an integral part of the child's right to quality education, privacy protection and protection from violence and abuse. It is the responsibility of adults to provide adequate protection and support for children to enjoy their rights in the digital world. Safe and constructive use of digital devices and the Internet implies having appropriate skills for digital literacy: searching and critically evaluating information from the Internet, communication through digital tools, creating digital content, safe behavior on the Internet and solving problems in the digital environment. The digital world is real, inseparable from the experiences gained outside it. Digital communication is real, even though it takes place virtually.

All the rules that apply to communication in everyday life also apply to communication in the virtual world. Just as we don't want to reveal our personal information to everyone we meet on the street, it would be logical not to do so online either. Just as we don't insult or hurt people live, we shouldn't do it through digital devices or communication tools either.

13 Vodich_za_sajber_bezbednost_PRINT%20(1).pdf

Source: https://www.google.com/url?sa=i&url=https%3A%2F%2Fbetterproposals.io%2Fblog%2Fproposal-terms-and-conditions%2F&psig=AOvVaw0D9C3CMQm6x_92VEJBdLJb&ust=1700920643686000&source=images&cd=vfe&opi=89978449&ved=0CBQQjhxqFwoTCODqrKrl3IIDFQAAAAAdAAAAABAE

The right to privacy and protection of personal data is one of the basic human rights recognized in the most important international documents, such as: the United Nations Convention on the Rights of the Child (Article 16), the Universal Declaration of Human Rights (Article 12), the European Convention on human rights (Article 8) and other.

Personal data are all those data that refer to a person, based on which it can be identified:[14]

- name and surname of the person;
- postal address;
- e-mail address;
- photography;
- IP address;
- location where the person is located;
- data from the health card;
- data collected in the online environment through cookies;
- data used to profile the user (economic situation, personal interests, behavior, consumer habits, movement, etc.).

Children and young people are concerned about what personal data will come into the possession of parents and friends, but not about the fact that they share the same data publicly and are often unaware that it can be misused. It is very important to raise awareness among young people about what personal data is not appropriate to share with other people and in the digital space, in which situations and why. It is especially important when we talk about the content that children and young people share online, because the moment we post something online, we tend to lose control over the content we post.

14 Vodich_za_sajber_bezbednost_PRINT%20(1).pdf

Users leave their personal data on the Internet:

- knowingly, for example, when buying some products, downloading content from the Internet, publishing photos, opening profiles on a social network;
- unconsciously, for example, through cookies, fingerprint, location data, IP address of the device from which the internet is accessed, etc.[15]

15 Priracnik-za-spravuvanje-so-kiber-nasilstvo-mk.pdf

COMMUNICATION ON THE INTERNET AND CONSEQUENCES OF CYBER VIOLENCE

Research shows that moderate use of digital technology positively contributes to children's development, while non-use and excessive use have a negative impact. Parents, with their habits in using digital technology, greatly shape its use by the child. Regular monitoring and freedom to discuss children's activities on digital devices are more effective in reducing cyber violence than simply limiting time or access to certain content.[16]

Banning the use of the Internet is not a highly recommended measure, because in this way children are deprived of the numerous opportunities provided by the Internet, especially considering that the Internet is a powerful information-cognitive tool and an opportunity to acquire skills that are crucial for successful functioning in the digital space.

The recommendation for adults is that their main focus should not be on the time the child spends in front of the screen, but on the quality of that time, ie., on the content of the activities used. Young people should be supported not to use the Internet exclusively for entertainment, but also for other meaningful and useful activities (acquiring different skills, finding useful information, school assignments, etc.).

The virtual world is not immune to violence, but "cyber violence" is becoming a form that young people are facing more and more often. For them, it is much "easier" to write a malicious comment than to say it to someone's face, or to click the "like" button on any violent post, instead of personally supporting the bully as they are bullying the victim.

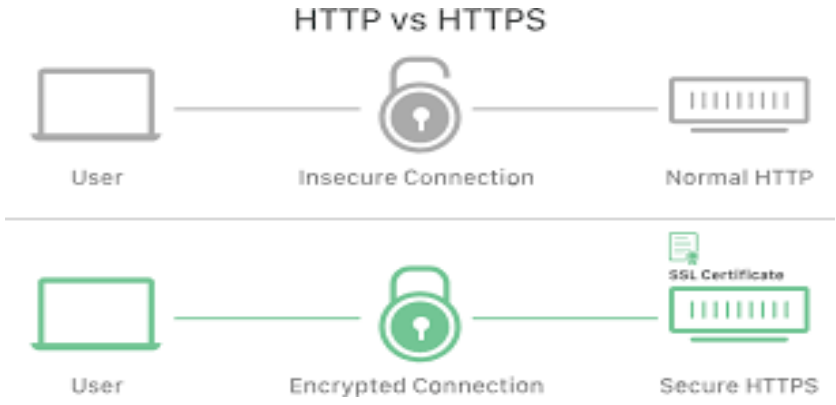
16 (Blum-Ross & Livingstone, 2016)

WEB BROWSERS AND SECURITY

We, in our daily life, working on a computer or some other digital device, visit a large number of websites, which offer us countless services necessary for us and for our personal development and facilitation in the performance of our daily responsibilities. Used services, such as reading news, searching for information, social networks, listening to music, downloading necessary information and documents, and more, have become an inevitable part of our way of life.

It should be kept in mind that every website uses a communication protocol, and it is very important to know which websites use a secure protocol and which websites are safe to visit.

HTTP is a protocol that enables communication between different systems. It is commonly used to transfer data from a web server to a browser in order to allow users to browse web pages. However, with the regular HTTP protocol, the information flowing from the server to the browser is not encrypted, which means it can be easily stolen, while the HTTPS protocols fix this by using an SSL certificate, which helps create a secure encrypted connection between server and browser, thus protecting potentially sensitive information from theft as it is transferred between the server and browser. HTTPS is especially important for web pages where we enter user accounts, passwords and credit cards.[17]



Извор: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.cloudflare.com%2Flearning%2Fssl%2Fwhy-is-http-not-secure%2F&psig=AOvVaw2Q3ZH8SbLB_T5O7S7ojLVg&ust=1700921098450000&source=images&cd=vfe&opi=89978449&ved=0CBQQjhxqFwoTCJDc4oTn3IIDFQAAAAAdAAAAABAE

17 Vodich_za_sajber_bezbednost_PRINT%20(1).pdf

TYPES OF CYBER ATTACKS

A cyber attack or cyber security threat is a malicious activity designed by malicious people, so-called hackers, to steal or damage your data or disrupt the system of an individual or an entire organization.

Several types of cyber attacks are known, namely:

- Social engineering
- Phishing attacks (phishing - fishing)
- Downloading data in passing (Drive by downloads)
- Man-in-the-Middle Attacks (MITM Attacks)
- Attacks with thrown USB devices
- Malware - malicious software

To acquire the skills to protect yourself and your systems, you first need to be familiar with and learn about these different types of cyber threats and the different ways to stay safe in cyber space.

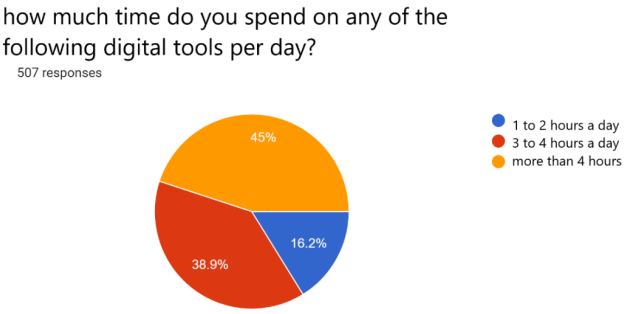
RESEARCH RESULTS

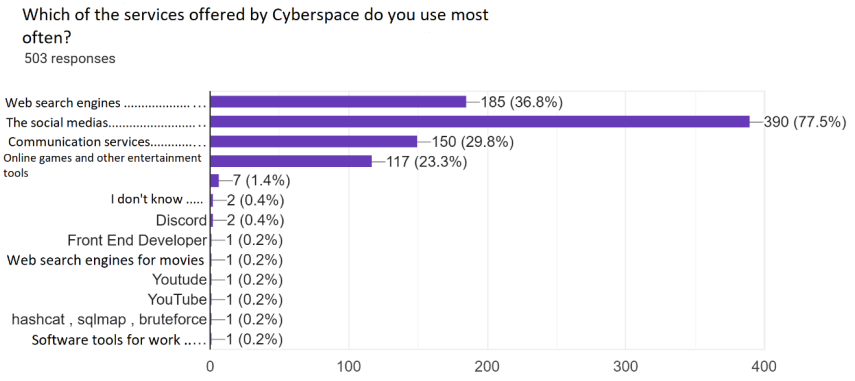
This research aims to analyze and insight on the current situation in the identification, prevention of cyber violence and cyber attacks, and how much students are familiar with the risks that the digital world hides and how much they know and apply the methods of protection and privacy in the cyber space that they use.

The survey was conducted in September 2023, on a representative sample of 507 respondents, students from three secondary schools in the City of Skopje and two primary schools from the Municipality of Karposh (urban and rural areas).

The survey questionnaire is the basis of our research, because our starting point is the existing state of students' awareness and how informed they are. How much do they know about cyber violence and how do they deal with it, what is the situation in their school, what is the role of existing protocols for dealing with violence, what is the role of teachers and parents in dealing with violence, what types of cyber attacks are familiar to them, and what mechanisms they use to prevent and defend against cyber attacks, how they protect personal information and how safe they feel in cyber space are the questions we got answers to using this method.

The instrument that was applied for the research is a survey online questionnaire with 20 questions, which are combined of different types of questions, in order to get as clear picture as possible about the actual situation of cyber violence and cyber security, ie. the student is given the opportunity to choose one or more answers from the offered options or to give his own personal answer from his experience.

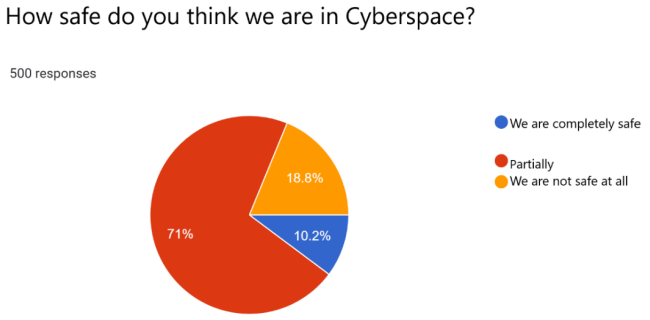




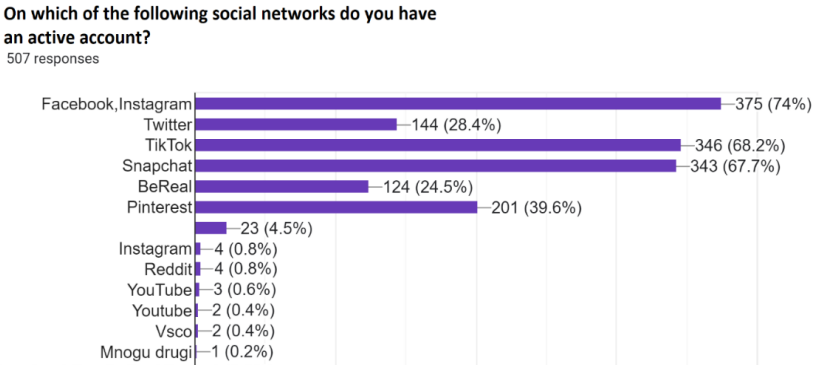
Taking into account the answers to the first two questions, you get a clear picture of the time spent on the Internet and what exactly that time is invested in. Out of 507 responses from students, approximately 84% answered that they spend more than 3 hours and more than 4 hours on the Internet (digital world) and 77.5% of students spend that time on social networks.

According to this result, young children's time is wasted unknowingly and unproductively, and if we take into account that hardly any of the young people admit that they actually spend a very large part of their time on these "activities", then it can be said that young people really too much of their time are actually influenced by the contents of social networks, which has a great impact on the formation of their views and opinions.

Since social networks are also a kind of socialization – if everyone uses a certain social network, there is a fear that they will miss something if they do not use it for a certain period.

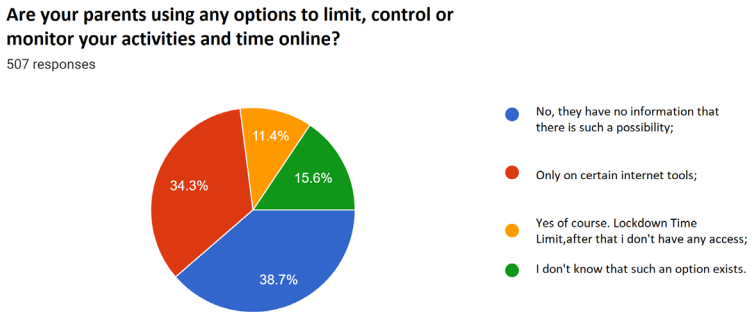


The graph itself shows the awareness of how safe children feel in cyber space. 71% of the students declared that they feel partially safe, which means that they have uncertainty and lack of information about security in the digital world. 18.8% of respondents declared that they feel completely safe in cyber space, while 10.2% declared that they do not feel safe at all.



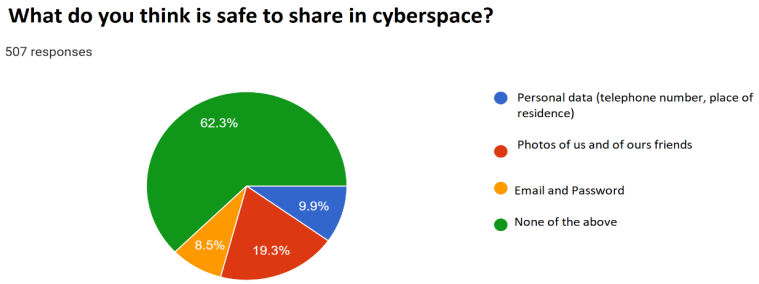
To the question: "On which social networks do children have an active account", the students had several options to choose from as an answer, and according to the answers we can conclude that Facebook and Instagram (74%), TikTok (68.2%) and Snapchat (67.7%), are the most used social networks by our children.

A large part of young people register, create profiles on social networks very young, between the ages of twelve and fourteen. When talking about the positive effect, the reasons are of course the facilitation of communication for certain children, the easier availability of information, the possibility to highlight creativity, to share ideas with others, etc.[18]



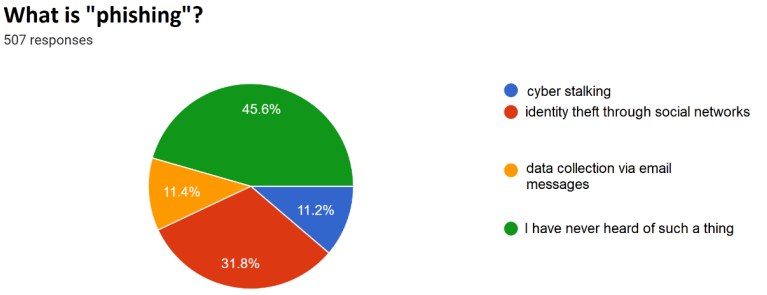
The main role for the safe use of the Internet is played by the parents themselves and the children's close surroundings, but according to the real situation, as a conclusion from the responses of the respondents, 38.7% declared that most of the parents are not aware and educated about the way they can influence the cyber security of their children, which security measures they can set and through which tools. While 34.3% stated that they have a ban by their parents only on certain tools, 15.6% of the respondents do not even know that there is an option with which parents can control their children's activities on the Internet.

18 https://goce.mk/zhivotot-na-soczi%D1%98alnite-mrezhi-i-zhivotot-izgubeni-vo-prevodot/



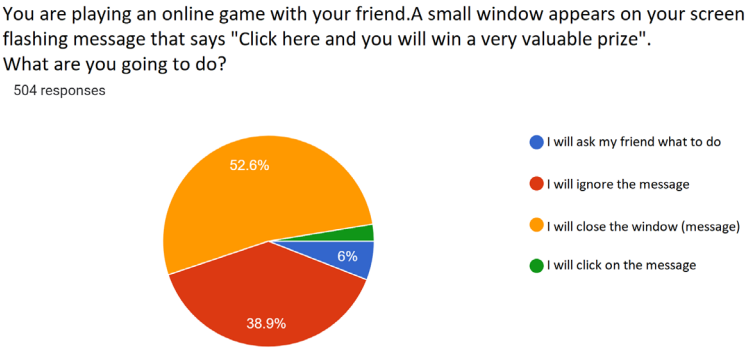
The results of the above question about sharing show that children are aware of the rules of cyber security in sharing important elements of our everyday life, where 62.3% of respondents declared that none of the options offered should be shared online. The other respondents have different views on what should not be shared on the internet. But despite such awareness, a question arises, why do we still want to share statuses, pictures or other things on social networks?

Researchers believe that happiness is the main motivator for sharing on social networks. Emotions that are accumulated and related to happiness are the most common when it comes to the most successful viral content on the networks. Google's Abigail Posner describes happiness sharing as an "energy exchange." According to her, when we watch or create content that brings us to life, we forward it to others to give them some of the energy and liveliness. Every gift contains the spirit of the giver.[19]

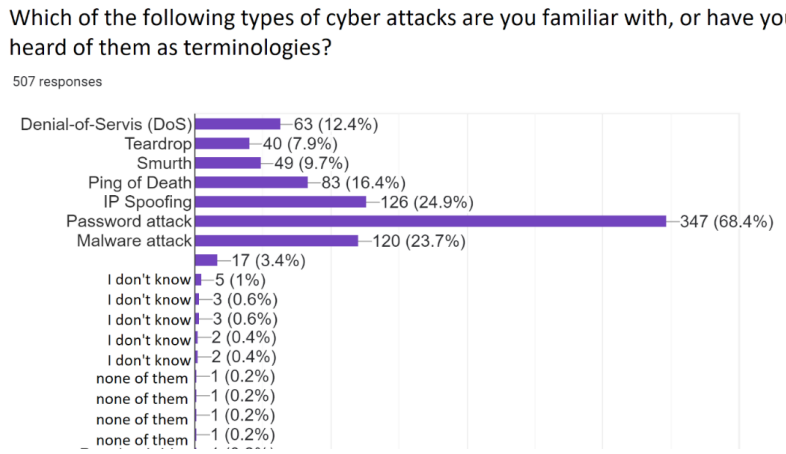


When asked "What is phishing?", 45.6% declared that they had not heard of such terminology, and only 11.4% gave the correct answer. According to this, we can conclude that children need additional education (formal or informal), which will help them learn more about the types of cyber attacks, how to recognize and protect against them.

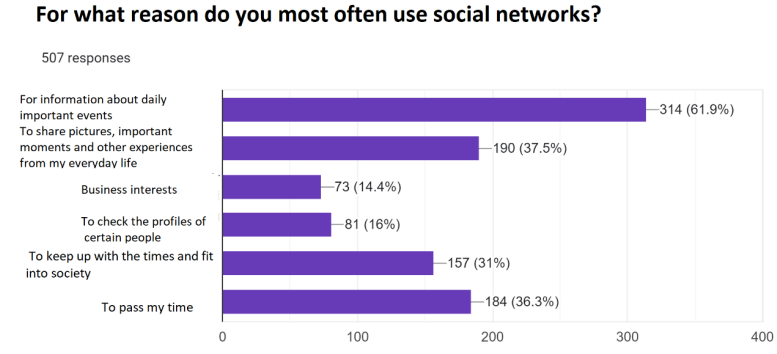
19 https://sovremenitehnologii.mk/socijalni-mrezi/



In similar cases, when a message unexpectedly appears on the screen, it is best to ignore it. All other procedures will lead to the activation of a certain virus. However, 52.6% of the respondents declared that it is best to close the window, which means that they automatically expose themselves to a risk that they are not even aware of. And 38.9% of respondents are aware of how to act in such a situation or a challenge.



If we go back to the results of the answers to the second question, about what children use the most from cybers pace, we found more answers that they it is the social networks. Well, that's why children are most familiar with the passwordattack, because they have personally faced it. 68.4% of the students answered that they are familiar with this type of attack, while other types of attacks are less known to the respondents.



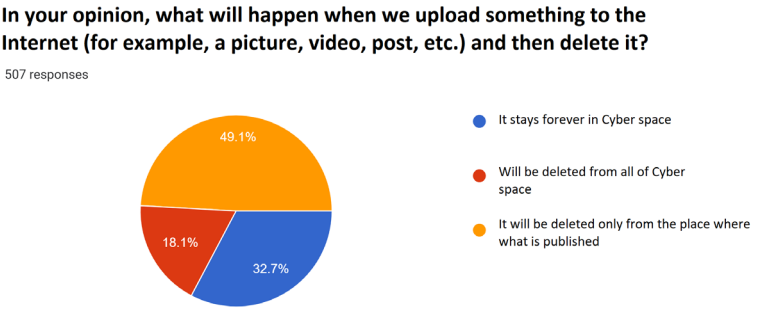
The balance between life on social networks and reality is becoming more and more difficult, because the power of Instagram, Facebook, Twitter, Tik Tok is great, addiction is easily created (like any other addiction), and the possibility for young people to "separate" from real life and to think that what they see on social media is actually what they should aspire to is a big one.

The three most prominent reasons for using social networks are:

- for getting informed (61.9%),
- for sharing (37.5%),
- for no reason, just to pass the time (36.3%).

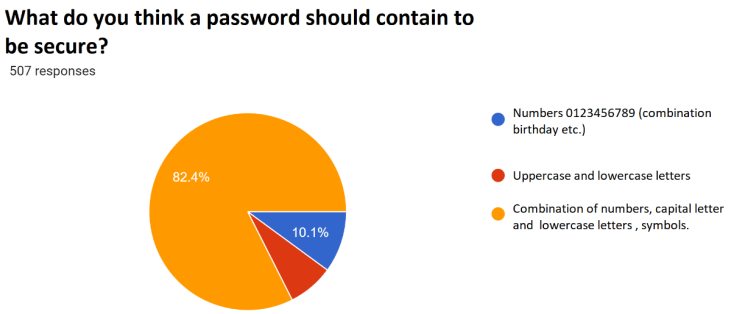
The virtual world creates pressure on young people in the real world by giving them a false image of the lifestyle, clothing, social behavior, unrealistic information, etc.

The virtual world creates pressure on young people in the real world by giving them a false image of the lifestyle, clothing, social behavior, unrealistic information, etc.



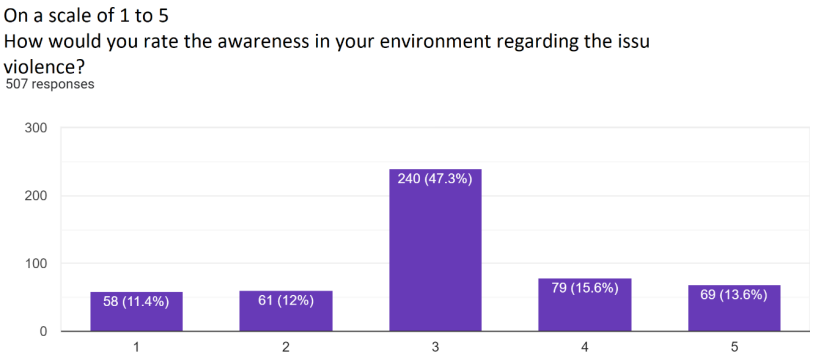
All our activities on the Internet can be used, and already are used for some purposes. According to the answers received, 49.1% of the students are aware that once they posted on the Internet, even if they want to delete it immediately, they will not succeed, because it remains forever in cyber space. 32.7% of respondents believe that what they posted on the internet (in cyber space) will be deleted by itself from the place where it was published, and 18.1% of students believe that it will be completely deleted from cyber space after some time.

So we need to be very careful what we share in the digital space.

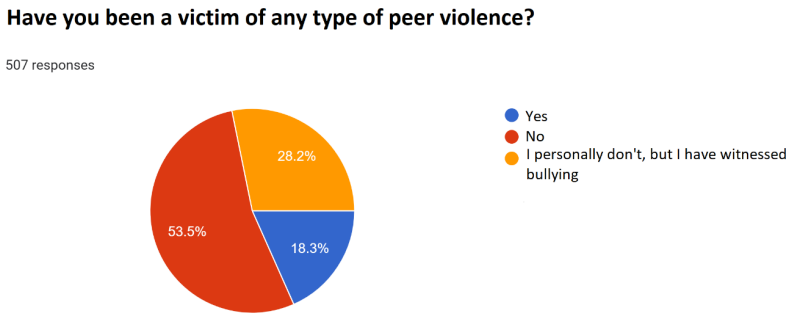


Setting passwords for using various applications in the digital space is a very important security measure. Hence, according to the answers of the students, 82.4% of them are familiar with the importance of the password combination and how it should be composed.

If you use as complex passwords as possible, especially when it comes to social networks and e-mail, this way you protect your data, so it is safe. When we say, "slightly more complex passwords," we mean using a long combination of upper and lower case letters, numbers, and characters. According to the answers given, the students are familiar and aware of the complexity of passwords as a measure to prevent a possible attack.

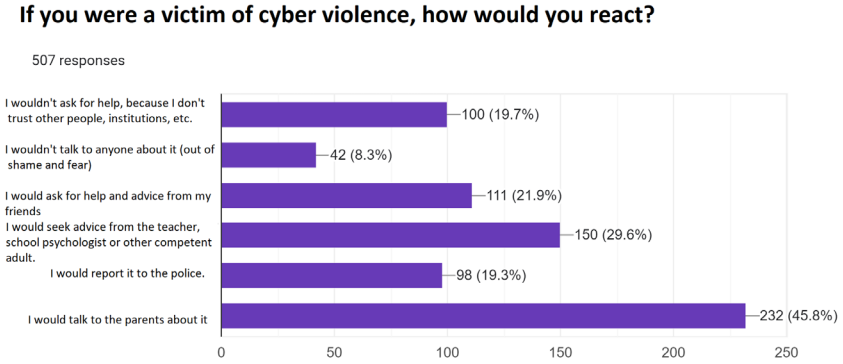


From the answers to the above question, we can see that 70.7% of the surveyed students believe that the awareness in society and their environment regarding cyber violence is low and average. The answers of the students point to the fact that there is an urgent need for improvements in the direction of raising awareness among all social actors about the importance and sensitivity of cyber violence and that a lot of work needs to be done to ensure a safer climate and a sense of security in cyber space.



53.5% of students declared that they were not victims of peer violence. At the same time, 28.2% of students answered that they witnessed peer violence, and only 18.3% of them declared that they were victims of peer violence.

These students' response results open up more directions for considering the possible causes. Namely, the Analytica think tank's research from 2022 showed that as many as 62.7% of students confirmed that the violence is often or constantly present in the school environment.[20] At the same time, 37.4%[21] of students answered that electronic violence is the most prevalent in their environment, after physical and psychological violence. These results point to the fact that the wide spread of violence may have led to the extent that a large part of the students are not aware that their specific behavior is a form of violence and hence it becomes everyday and "normal" behavior. Thus, there is a danger that it will become an accepted social and societal norm. In addition, the high exposure of young people to violence (through TV, video games, the general socio-cultural context in which they live) further contributes to the "unconscious" violent behavior of children. This means that the threshold of tolerance has been lowered and open and covert violence, as well as violent communication, unfortunately becomes a way of living and communicating between children.

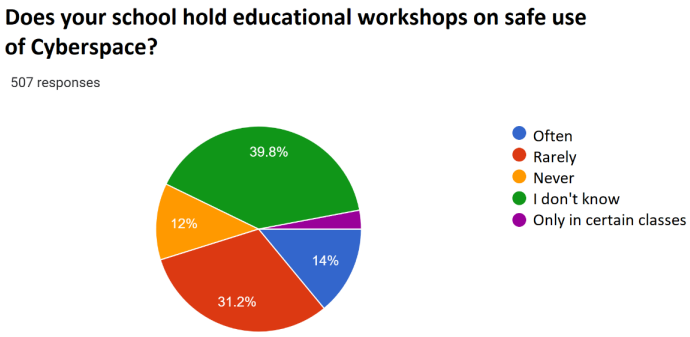


The fact that 28% of students stated that they would not seek any help if they were a victim of cyber violence is worrying. However, on the other hand, the fact that 72% of the students declared that they would seek help from a professional service, the class teacher or the parents themselves is positive. This indicates that still the open communication between parents and children, or teachers (classroom teacher) and children is a positive sign or a key solution in dealing with any type of peer violence. At the same time, this shows us that the teacher-children-parents relationship is really important and therefore work should be done to strengthen it in order to encourage all students to ask for help if they are faced with any kind of violence.

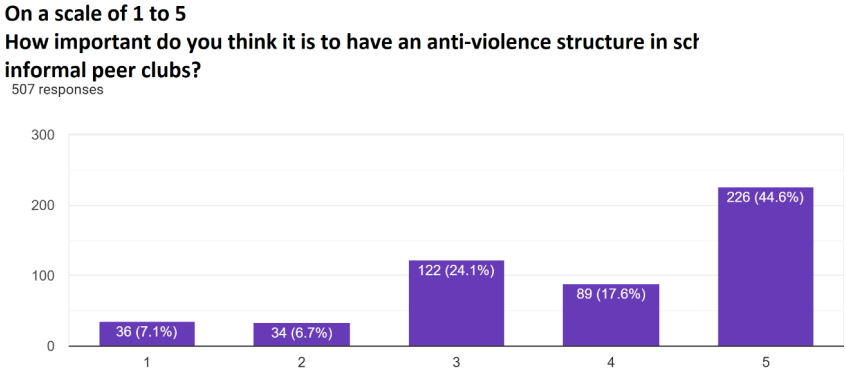
20 Handbook for developing a culture of peace and prevention of violence as basic values in the educational system in the republic of north macedonia, Maja Hristovska and Vesna Trajkovska-Sterjov Analytica Think Tank, January 2022. Available at: chrome-extension://efaidnbmnnibpcajpcglclefindmkaj/ https:// /www.analyticamk.org/images/2021/12/12/Prevencija_Nasilstvo_MK.pdf

21 The Analytica think tank's research aimed to identify forms of violence in schools. At the same time, 37.4% of the students answered that electronic violence is the most present in their environment, after physical and psychological violence. (Handbook for developing a culture of peace and prevention of violence as basic values in the educational system in the Republic of North Macedonia, Maja Hristovska and Vesna Trajkovska-Sterjov Analytica Think Tank, January 2022)

"Parents must be curious, but not judge the child. It often happens that the child is worried that the parent will deny it access to the device if it talks honestly about the problems it is facing, so you need to reassure the child that you will not take away its mobile phone if it is facing such a problem" - Doctor Paul Wegle of the American Academy of Child and Adolescent Psychology.[22]



43.2% of students answered that educational workshops on cyber security are not held in their schools or that it happens very rarely. The results of this question are worrying, as 39.8% of the respondents answered that they do not know if cyber security workshops are held. Considering that with the advancement of technology and the expansion of digitalization, we face a series of challenges and specific dangers, however, very small work is done on digital education, both formal and informal.



To this question, the students had the opportunity to evaluate the need for informal peer clubs, on a scale of 1-5 (1 indicates the lowest score and 5 indicates the highest score). A very important fact shared by students is that 62.2% of them consider it important to have informal peer clubs in their schools through which cyber security education will be carried out in order to improve the school climate and deal with violence. Only 13.8% of the respondents believe that there is no need for the existence of informal clubs for peer education in their schools.

22 https://www.crnobelo.com/zivot/semejstvo/95707-zoshto-decata-zhrtvi-na-sajber-buling-krijat-od-roditelite-deka-se-zlostavuvani-4-znaci-deka-deteto-trpi-maltretiranje

Hence it is clear that students should be offered the opportunity and conditions for an informal way of education, regular training in the field of informal education, space and content for their effective organization and activation in the direction of improving the environment in which they live and work. .

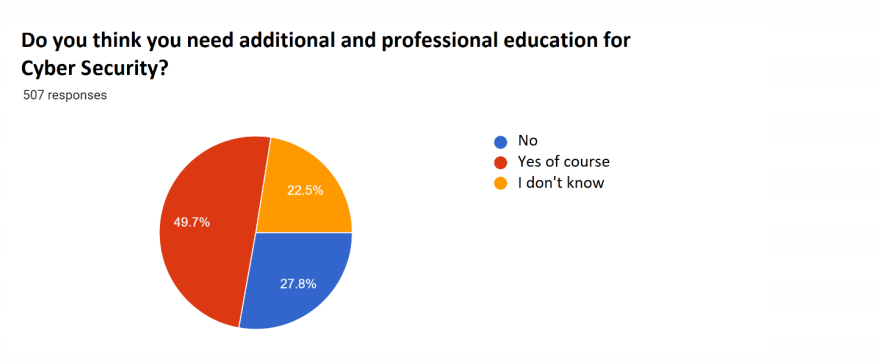
Through informal education, young people enrich their knowledge and develop skills that help them in the educational process, as well as in exercising their civil rights. The skills of critical thinking, effective communication and teamwork that they acquire through non-formal education are of crucial importance for their participation in democratic processes.

To the open question - "What is the difference between http and https?", respondents gave their thoughts and answers. In the attachment, we quote only a few of the answers:

1. Whenever we type an internet address, we can notice how before the "www" there is either the http or the https part. This may not have caught your attention right away, but sometimes the text is HTTP and sometimes it's HTTPS, so what's the difference? If you look closely, you'll notice that HTTPS has a padlock icon next to it, which means access is restricted or encrypted."
2. "There is no difference"
3. "I think https is more secure"
4. "I don't know"
5. "https provides data protection while http does not"
6. "I don't know, but I want to know"
7. "When HTTP is used, all data that is sent is unprotected, while HTTPS allows secure, encrypted communication that protects against misuse"
8. "https-means there is a page and we can open it, but http-I don't know"
9. "A different way of collecting data"
10. "I really don't know what the difference is"
11. "I don't know, but I think I see https more often on websites, which means I think it's more secure than http."

If we look at and analyze all the answers to this open question to which the students gave their answers, we can conclude that most of the students do not know the difference between HTTP and HTTPS. And this is certainly an expected result. Furthermore, if we analyze the answers of those stu-

dents who answered other than “don’t know” we can see that the answers differ in terms of understanding and awareness of the differences between HTTP and HTTPS. Certainly, a number of students correctly identify the differences while others express uncertainty or lack of knowledge. Responses indicating a perception of HTTPS as a more secure variant are consistent with the common understanding of the security features associated with HTTPS. The presence of responses from students who express a desire to learn suggests the possibility of additional education on this topic. Overall, the analysis of this open-ended question indicates a diverse range of perceptions and levels of knowledge among respondents.



From the received answers to the question about “the need for additional education for cyber security”, it can be concluded that, in general, there is a need for education, the results of the respondents confirm this, where 49.7% stated positively about the need for additional education for cyber security, 22.5% of respondents declared themselves neutral about this issue, while 27.8% think that there is no need for this type of additional education.

First of all, the children themselves should be given knowledge about what act is considered cyber violence and cyber attack, how to recognize it, how to deal with it and where to report it. But at the same time, we would emphasize the need for further education of teachers and professional services in schools to deal with this problem, especially the need to introduce new effective measures and cooperation with competent institutions and parents and intersectoral cooperation.

RECOMMENDATIONS FOR PREVENTION OF CYBER VIOLENCE AND DEVELOPMENT OF CYBER SECURITY IN THE EDUCATIONAL ENVIRONMENT

Nowadays, with the development of technology and the digital revolution, the use of the Internet begins at an early age, depending on who uses the services offered by the digital space and for what reason.

According to the obtained results of the questions from the questionnaire, it is clear that Internet services and social networks are an inevitable part of children's lives and everyday life. The digital space is a reality that, as much as it facilitates communication, it helps us stay in touch with friends, family, share information, have fun through games and various other internet services for our needs, not knowing that sometimes it can be very dangerous, with possibilities of causing unwanted consequences.

That's why the question of how safe cyber space is, which in addition to its positive effects, as internet services, also offers social networks that influence people, especially young people, who are the most frequent users of them and to a certain extent "addicts" of social networks (the students themselves declared that most of them spend more than 4 hours on the Internet and without any important reason).

If left unchecked, the effects of cyber violence and social media using addiction itself can lead to extreme stress and depression, and student victims can become prone to negative uncontrolled behaviors as a result of their experiences. But in order to be able to develop the person in the course of the new digital expressions, it is still necessary to know the way to protect the safety in the digital space, because there is a lack of information about it, not only among children, but among parents and schools, as the results of our research show.

For this purpose, we single out several recommendations that will facilitate daily research and use of the Internet:

"Young people are the ones who know the cyber space better, they feel it as theirs, and therefore peer education and solidarity are key to dealing with online violence" - this is one of the main conclusions from the discussion on the topic: "Cyber violence - safety" and self-censorship" [23]

- Considering the above conclusion, it is very important and necessary to develop awareness among children and young people that in the virtual world there are rules, obligations, requirements, limits, that responsibility and caution are as important as in the real world. Our children are sitting next to us at home or at school, but they are still exposed to risks in a virtual world full of strangers and challenges like never before. Children and young people are more technically skilled and knowledgeable than us, but they need the experience of adults to be protected and responsible in the virtual world, to have the various benefits of the digital age and to be able to adequately face the many challenges that lie ahead. That is why it is necessary to educate students and, of course, further education of adults about the awareness of risks in cyber space.
- Since children who have experienced cyber violence more easily turn to their peers for help, it is necessary to conduct peer education at school, organize teams of peer educators or online counseling for young people who have been victims of cyber violence.
- The school should also provide strategies, techniques and ways to report any kind of violence, namely: setting up mailboxes in the school premises where children witnesses can anonymously report cases of violence, setting up a link to a website where that children will have access to report violence, etc.
- Students should be properly informed and educated not to be participants or passive observers in the act of peer violence (witnesses to a cyber attack). It is necessary to encourage students in such situations to turn for help and support to adults, close trusted people, professional officers and teachers in the school.
- One of the ways to prevent or deal with cyber violence or a cyber attack is to establish a stronger relationship between parents/guardians and the school, through more frequent and efficient activities and work with students, which will achieve a timely mobilization that will have a preventive effect, i.e., organizing informal workshops or some kind of campaign aimed at informing parents about the challenges and risks of cyber space.
- Also, in the school premises it is desirable to display printed posters with some "standard" measures for protection and security in the cyber space.
- Realization of additional trainings to acquire the skills needed by teachers and professional services to be able to apply different approaches that would improve the climate and communication in the classes during the lessons.

23 "Cyber violence - security and self-censorship", which was held in the Committee social club, organized by the Helsinki Committee for Human Rights

PRACTICAL TIPS FOR SECURITY IN THE DIGITAL SPACE

- You should be very careful with your personal information and digital identity;
- Create and use more complex passwords (combination of uppercase letter, lowercase letter, number and characters);
- Think twice and check links before clicking;
- Make sure you use secure WI-FI networks;
- Use a VPN;
- Remember to use sites that start with https//;
- Turn off your Bluetooth if you don't need it;
- Use antivirus and antimalware software and update them more often;
- Make backup copies of your data (Backup);
- Be careful what content you share - avoid posting personal and confidential information, such as: email address, phone number, home address, card numbers, PINs, passwords, etc.
- Avoid filling out forms asking for your personal information, as they are often supported by malicious users who can misuse your information;
- Use the option to limit the display of the content you watch or post, so that it is visible only to trusted friends on social networks.

PRACTICAL RECOMMENDATIONS AND ADVICE FOR PARENTS ON CYBER SPACE SECURITY

How should you behave with your child to limit the risks in the cyber space and to be aware of any abuse or cyber attack, we have listed some useful recommendations and tips for you parents.

- Talk together with the children and explain your rules and expectations if you provide your child with a digital device.
- Agree on what is acceptable to post and send and for the child to consult with you as a parent.
- For older children, it is preferable to use real-life examples from the news that illustrate the risks, dangers and legal issues.
- If you want your child to trust you and share things with you, whether they are unpleasant or not, and even beyond your ethical principles, you should be ready to listen and support it, without judging it.
- Make sure that your children do not accept unknown users as "friends".
- Check more often how your child interacts with technology: does it do it in a way that changes its behavior when you enter the room? Does it turn off the computer, etc?
- Maintain the highest privacy settings across all devices and platforms.
- Check those settings regularly as they sometimes reset themselves when platforms make updates or change their terms of use.
- Teach your children to think seriously before posting or sharing anything online.
- Make sure that your child knows that it can always come and talk to you about everything that is happening, that you as a parent will not judge it.

Report a crime to the police or the Public Prosecutor's Office.

A criminal offense can be reported to the nearest police station, by calling 192 or to the Computer Crime Department at the Ministry of Internal Affairs, by e-mail at cybercrime@moi.gov.mk or on the "Red Button" page.

BIBLIOGRAPHY:

1. Computers in Human Behavior 29(6):2703-2711, Journal Review: Cyber-bullying myths and realities, November 2013, authors R.A. Sabelle, J. W. Patchin and S. Hinduja
2. Hinduja, S., & Patchin, J. W. (2018). Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. Corwin Press.Hinduja, S., & Patchin, J. W. (2015). Bullying, Cyberbullying, and Suicide. Archives of Suicide Research
3. The State of Online Harassment, January 2021, Pew Research Center, available at: https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/
4. "Teens and Technology 2013", ,Pew Research Center
5. "Children in a Digital World" (2017), UNICEF
6. Statistical report, 2022, available at: https://www.stat.gov.mk/pdf/2022/8.1.22.36_mk.pdf

   https://mladieu.mk/wp-content/uploads/2022/10/Priracnik-za-spravuvanje-so-kiber-nasilstvo-mk.pdf
7. Cyber hygiene for children " (2018): ENISA
8. "Cyber Aware Teacher Survey Report" (2020), NCSC
9. https://www.ojp.gov/pdffiles1/ojjdp/grants/217918.pdf
10. https://mkd-cirt.mk/wp-content/uploads/2021/03/VtoraBroshuraPrint.pdf
11. Handbook for dealing with cyber violence, Priracnik-za-spravuvanje-so-kiber-nasilstvo-mk.pdf
12. https://akademik.mk/sajber-nasilstvoto-e-prodolzhenie-na-nasilstvo-to-vo-fizichkiot-prostor/
13. https://medium.edu.mk/aktiviraj-se/socijalni-mrezi-mladite-zarobeni-vo-lazniot-svet-na-influenserite/
14. https://goce.mk/zhivotot-na-soczi%D1%98alnite-mrezhi-i-zhivotot-izgubeni-vo-prevodot/

15. file:///C:/Users/Elsa/Downloads/Vodich_za_sajber_bezbednost_PRINT%20(1).pdf

16. https://www.dcaf.ch/sites/default/files/publications/documents/GuidebookCyberThreats_MK_web_Jan2023.pdf

17. https://alobushavko.mk/mk/parents/110-soveti-za-digitalno-roditelstvo

18. https://worldbeyondwar.org/mk/types-of-violence/

Authors: This Handbook was prepared by GilJman Osmani Musliji, a researcher from the think tank Analytica Skopje.

This Handbook was produced within the framework of the project "Strengthening capacity of young people and teachers to apply cyber security measures and develop effective school programs to prevent cyberbullying", which is implemented by Analytica Skopje, with the financial support of the Embassy of Canada in Serbia, Montenegro and North Macedonia. The contents of this Handbook are the sole responsibility of Analytica Skopje and in no way can be considered to reflect the views of the Embassy of Canada in Serbia, North Macedonia and Montenegro.