Handbook for development of cyber security culture in the educational system of North Macedonia

FOUNDATION ФОНДАЦИЈА
OPEN ОТВОРЕНО
SOCIETY ОПШТЕСТВО
MACEDONIA МАКЕДОНИЈА

Handbook for development of cyber security culture in the educational system of North Macedonia

Author: Ana Dionisieva

Analytica think tank

December 2023

CONTENTS

PURPOSE OF THE HANDBOOK

The Handbook is intended for a wide group of stakeholders in North Macedonia who work in the field of cyber security of students, prevention of cyber violence of students, digitalization and educational policies, to be informed about the multidimensional aspects of cyber security. The purpose of this Handbook is to provide teachers and young people in schools in North Macedonia with means and resources to improve their capacities in the field of cyber security and opposing cyber violence. Through various modules and activities, the Handbook aims to increase the knowledge and skills of the participants on the safe use of the Internet and other digital technologies. At the same time, it strives to develop effective school programs for the prevention of cyber-bullying and the creation of a safe school environment.

With the rapid development of information technology and social networks, information becomes more accessible, communication becomes easier, and people share many photos and videos, which may be misused in the future. According to the data of the State Statistics Office in North Macedonia[1], as of 2022, 86.6% of households had access to the Internet at home. According to the specification of the population by age category, young people aged 15 to 24 use the Internet 100%, and 100% of them use the Internet several times during the day. The most common Internet activities of young people are participation in social networks (creating a user profile, sending messages or other attachments on Facebook, Twitter, etc.) with 93.1% and using instant messages, i.e., exchange messages, for example, via Skype, Messenger, WhatsApp, Viber every day or almost every day with 95.5%. This is a significantly higher intensity of Internet use compared to other age groups. The high percentage of young Internet users carries the risk of being potential victims of digital threats. Social media is a global network through which a large amount of personal information is exchanged to interact with community members. On the one hand, this facilitates communication in today's modern times where information becomes freely available, but at the same time it creates a large space in which electronic data exchange takes place - cyberspace. In this space, electronic data can be misused.

1 INFORMATION SOCIETY - INFORMATION SOCIETY RELEASE - NEWS RELEASE Use of information and communication technologies in households and individuals, 2022, State Statistical Office, available at: chrome-extension://efaidnbmnnibpcajpcglclefindmkaj/https://www.stat.gov.mk/pdf/2022/8.1.22.36_mk.pdf/pdf/2022/8.1.22.36_mk.pdf

Social media has introduced new forms of behavior, with increased dynamics of sharing personal information, such as photos, videos, locations and others. These activities lead to an increased risk and threat to users of social networks. Through social media, text messages, apps or the internet, people can be exposed to cyberbullying in the form of sharing negative, harmful, false and malicious content. However, it is important to ask whether we have an adequate education system that actively supports safe internet use, especially in the context of personal content creation, social media use and media literacy among young users.

The Handbook therefore serves as a user-friendly, easy-to-read guide to key aspects of young people cyber securuty and cyberbullying prevention in schools with recommendations for future measures and policies. It aims to put the cyber security of young people on the agenda because it is one of the key issues currently facing young people from North Macedonia, and whose importance will further increase.

The Handbook was prepared as part of the project “Development of a culture of cyber security in the educational system of North Macedonia - Strengthening the capacity of young people and teachers for application of cyber security measures and the development of effective school programs for the prevention of cyber-violence”, realized by Analytica in the period from August 2023 to February 2024.

METHODOLOGY

The Handbook includes application of a research method, a focus group method from conducted training and a method of information synthesis. Initially, the research and analysis is based on the identification of students and teaching staff, with a focus on their understanding and application of cyber security measures.

In the research, research methods such as surveying were included, with a survey questionnaire of 25 questions, which were designed by analytical experts (computer scientist and school teacher). The research was conducted in three secondary schools in Skopje, with the participation of 313 respondents. The primary data obtained from the research refer to the existing situation in schools and serve as a basis for formulating recommendations and conclusions.

The questionnaire considers various aspects of digitalization, use of social media, cyber security as well as the personal experiences of young students with cyber bullying and dealing with it. Students were also asked to rate the involvement of schools, teaching staff and parents in dealing with cyberbullying and the measures taken by schools to increase the cyber security of students. The value of students' knowledge and participation is key to assessing the current state of cyber security in schools and making recommendations for future action. The results of the survey are not representative, but offer an in-depth understanding of students' experiences regarding cyber security and cyber bullying.

The secondary data in this Handbook are reports and other literature on cyber security in North Macedonia. The Handbook is also supported by statistical data, policy analysis and media sources.

ABOUT THE PROJECT

The project “Development of a culture of cyber security in the educational system of North Macedonia - Strengthening the capacity of young people and teachers for application of cyber security measures and the development of effective school programs for the prevention of cyber-violence” is financed by the Foundation “Open Society” Macedonia. The general goal of the project is to get to know young people with the benefits of digital transformation and increasing the use of cyber security measures among young people, which will increase their safe presence on the Internet and reduce the negative effects.

The Handbook is part of the project. Specific goals of the project are: identifying students and teaching staff from the digital transformation of society with a focus on educational programs and the degree of application of cyber security measures by young people, improving cooperation and knowledge transfer between civil society organizations, educational institutions and the institutions responsible for creating policies in the field of cyber security and the institutions responsible for sanctioning cyber crime, increasing the role of local civil society organizations in providing assistance and support to educational institutions and young people for better use of the potential of information and communication technologies.

The purpose of this research and hence the Handbook is to show the capacity of young people in dealing with different types of cyber attacks, the constructive use of the Internet and communication technologies, as well as to give recommendations for finding mechanisms that would contribute to strengthening the skills of students and teachers for safe use of the Internet through their education. The conclusions and recommendations of this research will have to influence the relevant institutions for further implementation of activities and measures. The project has been implemented in three secondary schools in the city of Skopje in order to implement activities that will strengthen the skills of young people through cyber security content.

LITERATURE REVIEW

With the spread of digital transformation, the academic and professional literature in the field of cyber security and youth violence is developing as a significant source of knowledge. The specific nature of the internet and digital platforms gives rise to many challenges and opportunities, and the research literature plays a key role in uncovering these aspects.

The research by world experts, such as the work of Livingstone and Görzig (2017)[2], focuses on various aspects of cyber security and youth violence. Case studies from Norway, Finland, and the Netherlands show that the Internet is often used for cyber-violence, and the literature suggests recommendations for improving the safety of young people in the digital environment.

In Europe, the research such as that of Kowalski et al. (2014)[3] attempt to identify the extent and nature of cyber violence among young people. They analyze the impact of social networks, forums and online games on young people and offer measures to develop prevention strategies.

In the Macedonian context, the findings of the report[4] "Baseline assessment for awareness raising and capacity building" highlight, among other things, that students' awareness of cyber-security threats should be further strengthened, considering that 40% of students consider themselves vulnerable while on internet, of which more than 13% had some kind of bad personal experience. This conveys important information about the state of cyber security in schools in North Macedonia.

2 Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective January 2012, DOI: 10.1332/policypress/9781847428837.003.0012, Publisher: Policy PressISBN: 1847428827

3 Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth Robin M Kowalski 1, Gary W Giumetti 2, Amber N Schroeder 3, Micah R Lattanner 4, Affiliations expand PMID: 24512111 DOI: 10.1037/a0035618

4 RESEARCH REPORT Baseline assessment for awareness raising and capacity building, CRPM

INTRODUCTION

The development of digital technology and unrestricted access to the Internet have increased the concern about the cyber security of young people in Cyberspace. From a young age, students are exposed to cyber attacks. Young people represent a very vulnerable category because they continuously use the cyber space with limited skills to deal with cyber threats and at the same time take protective measures.

Cyber violence, online fraud and cyber attacks have increased significantly due to the lack of awareness among young people and a mechanism is needed to protect against these negative influences. The level of awareness among users is still moderate. A significant measure that can be taken is the education of young people in schools. More precisely, young people should be educated on how to use the Internet safely and how to protect themselves.

A large amount of information and misinformation circulating in the cyber space are potential cyber threats for students. Schools need to provide teachers who will be trained and will promote a critical approach to cyber security. Also, through cooperation with parents and their education, safe using of the Internet will be promoted.

One of the biggest challenges schools are facing with is the lack of experts, finances and resources to implement cyber security in education. The speed of technological change requires greater technological skills among teachers in order to improve the education of young people.

The inclusion of cyber security topics in the annual programs will have a significant role in raising awareness among young people in order to reduce cyber incidents and attacks. To be safe on the Internet, appropriate setting of school activities regarding the online opportunities and risks, the harms and threats of the Internet is necessary, through education on the proper use of digital technologies and education on Internet security.

TYPES OF CYBER ATTACKS

The use of computers, tablets, the Internet and other technologies have become part of everyday life. Every day young people use different services for communication, such as Facebook, Snapchat, Viber, etc. Most of them are not aware of the risks that exist in their cyber security.

Almost 70% of children and adolescents worldwide were exposed to cyber risks in 2023. Cyber risks vary depending on age, also a large part of students are exposed to risky content, contact and bullying through the excessive use of technology.[5]

A cyber attack is defined as a hostile activity with the aim of stealing, exposing, disabling, destroying data through unauthorized access to a computer system or digital device. Cyber attacks are usually aimed at individuals, companies and institutions using internet, mobile and computer technologies.

Platforms such as social networks, websites, e-mails are commonly used to carry out cyber attacks. Hackers also use artificial intelligence to disguise malicious code that is programmed to run later and create malware programs that can be adjusted accordingly during an attack. Young people are a vulnerable category exposed to various types of attacks.

Cyber attacks can be used and carried out in several ways. The goal is to gain unrestricted access to certain user information.

- The most common cyber attacks on young people are:
- Cyber grooming
- Phishing
- Cyber bullying
- Social Engineering
- Online Gaming
- Ransomware

5 Almost 70% of children & adolescents have been exposed to cyber risks:Security magazine, available at www.securitymagazine.com/articles/100099-almost-70-of-children-and-adolescents-have-been-exposed-to-cyber-risks

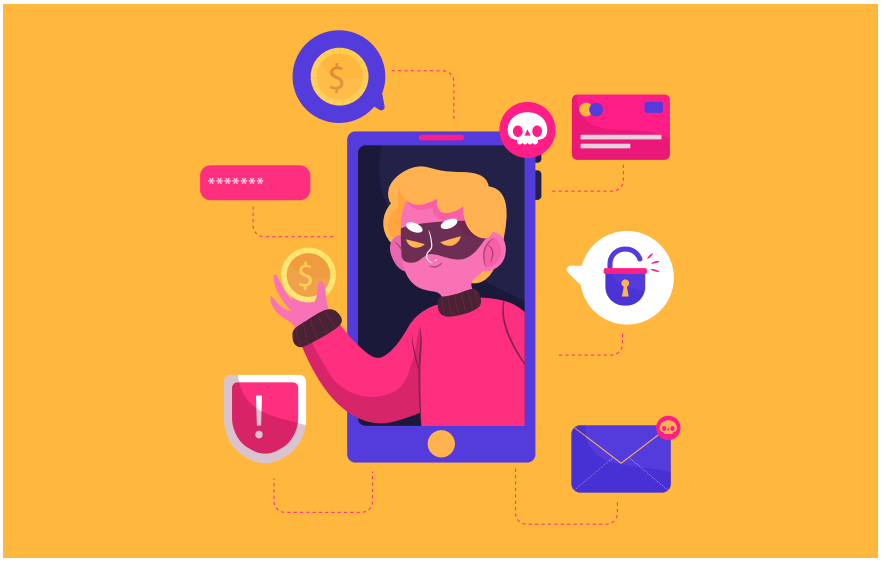
Cyber grooming

Cyber grooming is one of the most growing threats that children and adolescents face. In this process, a cyber groomer tries to gain trust among young people aiming to establish an emotional connection through social networks in order to carry out sexual harassment or exploitation. The main goals of cyber grooming are: obtaining personal data (often explicit images, videos and conversations) in order to threaten and blackmail the individual.[6]

By creating a fake account, a cyber groomer poses as a child who communicates through social networks, email, chat rooms and instant messages.

The biggest target group for cyber groomerot are adolescents, because during that period a large part of them face physical changes. The curiosity of young people increases their online activity and makes them vulnerable to cyber grooming. The process of cyber grooming itself can have a negative effect on the victim and remain long-term. In addition to the student feeling insulted and betrayed, the victim feels that he deservedly was abused, which leads to low self-esteem and self-blame.

Raising awareness as well as legal measures to prevent this type of attack is crucial. This type of attack is a gateway for further exploitation of children.



https://www. freepik.com/free-vector/hacker-activity-illustrated-concept_8088561.htm#page=9&query=cyber%20grooming&position=21&from_view=search&track=ais&uuid=5fd5f6ee-7839-45ca-b515-b068d8bf963c

6 What is cyber grooming?HackerNoon, available at:www.hackernoon.com/what-is-cyber-grooming

Phishing

Most cyber attacks start with phishing emails. Phishing is a type of social engineering in which cybercriminals will trick the victim into giving them sensitive information or installing malware.[7]

Phishing is based on malicious software, which is a standard way of illegally acquiring sensitive data. Among young people, many contacts with phishing are made through social networks and smartphones.

Although technical security measures are getting better, phishing remains one of the cheapest and easiest ways for cybercriminals to gain access to sensitive and personal information. If users click on a link, their security may be compromised and they may become victims of identity theft. With one click, users can also compromise their personal information, logins such as usernames and passwords, and financial information such as credit card numbers.

Attackers often achieve this with a malicious email that appears to be from a trusted source, but sometimes they use other methods as well. There are several reasons why "phishers" want to gain illegitimate access to a youth's account on Facebook or another network, and these are:[8]

- Spreading malware
- Opening unsecure hyperlinks
- Spam
- Collecting information and data from closest people

Phishing scams – publishing is vulnerable too. What you need to know - Science & research news | Frontiers (frontiersin.org)

7 What Is Phishing? A Brief Guide to Recognizing and Combating Phishing Attacks, www.comptia.org/content/articles/what-is-phishing

8 Phishing Attacks Targeting Young Adults: December 15, 2017 by Daniel Brecht, available at: www.resources. infosecinstitute.com/topics/phishing/phishing-attacks-targeting-young-adults/

Cyber bullying

Cyberbullying is one of the most common cyber threats that young people face. Cyberbullying happens online or by the use of mobile phones. This type of cyberattack involves threatening or abusive words sent or posted on the Internet to or about a person. Cyberbullying occurs through various forms:[9]

- Posting or sending embarrassing threats via text messages
- Encouraging continued harassment
- Sending or posting negative, bad or embarrassing photos (which are either real or photoshopped)
- Stealing a username and password or a mobile phone, in order to later impersonate the individual in order to damage his reputation
- Recording phone conversations secretly and then posting them online

The consequences of cyberbullying among young people are collective. They can affect their mental, physical and psychological health with daily manifestations.

Cyberbullying Information for Parents | How You Can Help | Kids Helpline

9 Cyberbullying behind fronteers:Deviant Behaviors and Intercultural Factors in Digital Communications: Gulia Mura www.academia.edu/1298055/Cyberbullying_behind_fronteers_deviant_behaviours_and_intecultural_factors_in_digital_communication

Social engineering

For young people, many online services are interesting, unknowingly using them they become vulnerable to online risks. The desire to make new friends, sharing personal information with others makes them an easy target for online attacks from social engineering.

Social engineering is used to mislead or manipulate targets in order to obtain information or access to their computers. Cybercriminals use social media access to hide their true identities and motives and pose as trusted individuals. This is done by tricking the user into clicking on a malicious link or by gaining physical access to the computer by fraud.[10]

Young people are not always aware of the risks of downloading or downloading files from unknown sources. The more information we share, the greater the chance of being a victim of social engineering.

https://cheapsslsecurity.com/blog/social-engineering-attacks-and-prevention-methods/

10 Handbook of Cyber Threats: Identifying and Combating Risks for Public and Private Sector Users and Citizens:AleksandarBratic, October2022, Geneva Centre, For Security Sector Governance available at: www.dcaf.ch/sites/default/files/publications/documents/GuidebookCyberThreats_MK_web_Jan2023.pdf

Online gaming

Online gaming is entertainment for young people. One of the ways to connect and interact with others. Many of them play games whether on game consoles, computers or mobile devices. The gaming community is getting bigger and by thatthe online scams, cyberbullying and the sharing of inappropriate content are increasing.[11]

Online games pose a safety risk to children and young people. Some of the risks are:

- Exposure to inappropriate content that may be missed by parental control and data filtering software
- Exposure to problematic content such as violence, sexual content or inappropriate behavior by other players
- Cyberbullying and harassment through online games or chat room messages that can be anonymous and targeted
- Internet luring. Individuals are known to be malicious and often use popular multiplayer games to connect with children/youth in order to start a chat or video through the game
- With the range of games available online and the ability to play with other players globally it can be interesting but also risky. Therefore, it is necessary for young people to know how to protect themselves in certain situations.

https: //www. internetsafetystatistics.com/risks-online-gaming/

11 Cyber security issues in online games: RESEARCH ARTICLE | APRIL 18 2017: IP Conf. Proc. 1955, 040015 (2018) Chen Zhao

Ransomware

Ransomware is a type of malicious code that encrypts data on a victim's computer and demands a monetary ransom to decrypt it. The popularity of this type of malicious programs has increased since the end of 2013 due to the emergence of cryptocurrencies that made it easier to pay the ransom, i.e., it made it more difficult to track the attackers. Ransomware works by encrypting the victim's data. The victim will only be able to decrypt the data if they get access to the used encryption key, which is owned by the attacker. After paying the ransom, the attacker has to provide the victim with the key, which is often not the case, so it's questionable whether it even makes sense to pay the ransom. Ransomware is usually spread through Trojan horses that, after installation, perform encryption and print messages in locked data and instructions to users to pay the ransom.

Some types of ransomware lock the computer by displaying a blackmail message. The other way is file encryption. In exchange for decrypting the data, payment of money is required.

https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021

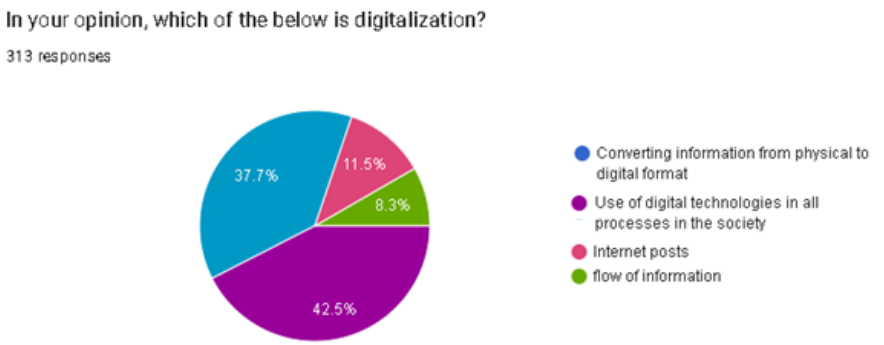
RESEARCH RESULTS

The research data refer to the current situation in schools and their role in educating young people about Safe use of the Internet. This research analyzes the digital transformation, the application of cyber security methods and mechanisms among young people by identifying the different types of cyber attacks, ways to protect against cyber attacks, the awareness of young people about the dangers of cyber attacks.

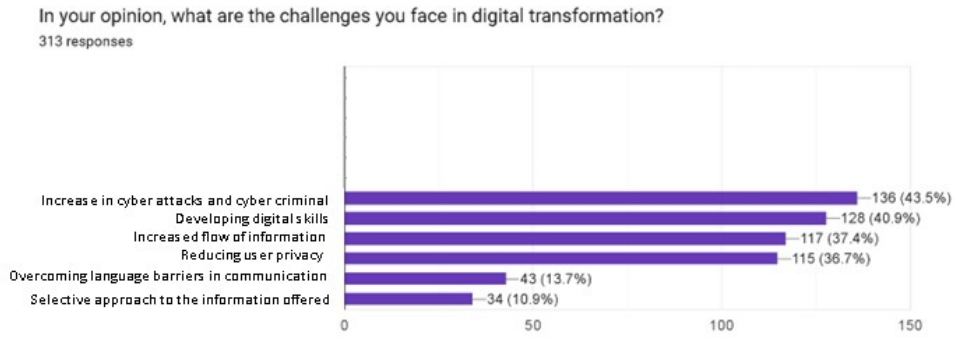
The research covered a total of 313 respondents from secondary schools SUGS "Nikola Karev", SUGS "GeorgiDimitirov" and SUGS "Shaip Yusuf". The instrument that was applied for the research is a survey questionnaire with 25 questions designed by an analytical expert.

The survey was conducted in the period of August 2023, on a representative sample of 313 respondents, students of secondary schools in the city of Skopje.

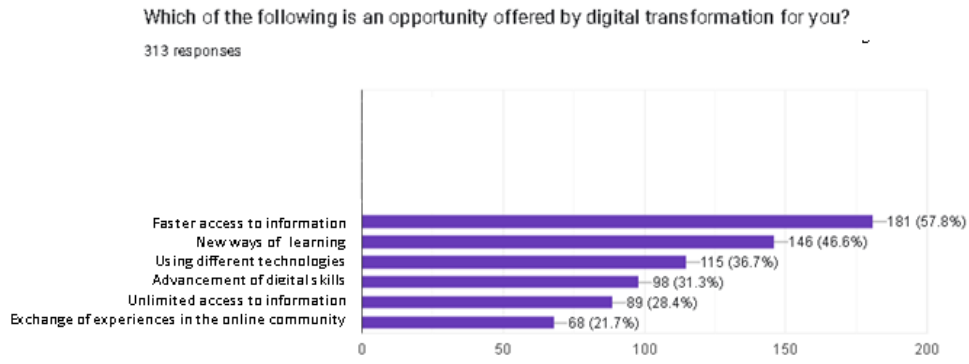
The survey is the starting point for the current application of mechanisms and methods for implementing cyber security among young people in secondary schools, how they experience the digital transformation, whether they can detect a cyber attack, how they deal with cyber attacks and how informed they are about the dangers that exist in the cyber space, are the questions that we needed to get an answer to.



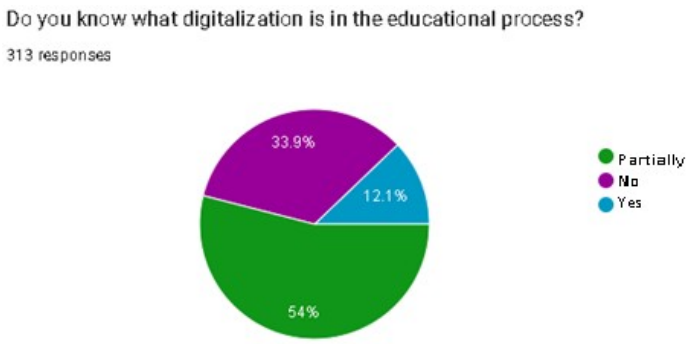
To the question What is digitalization? - 42.5% of young people declared that for them digitalization represents the use of digital technologies in all processes of society, 37.7% perceive digitalization as the transformation of information from a physical format into a digital format, while 11.5% consider that the Internet posts is digitalization. Digital technologies have provided many opportunities for the inclusion of the population in all spheres of digitalization of society. Hence, we can conclude that young people understand digitalization because a large part of them are involved in its processes in shaping the digital era.



The analysis of the research showed that 136 of the respondents consider that the biggest challenge for them in the digital transformation is frequent cyber attacks. Immediately behind them is the opportunity to develop digital skills among young people, the increased flow of information and the reduction of privacy. New technologies contribute to the continuous emergence of new vulnerabilities, and thus new threats to privacy, confidential materials and the availability of services. From what we can see, the biggest challenge for them is cyber attacks. It is obvious that more security is needed and finding ways to deal with the challenges.

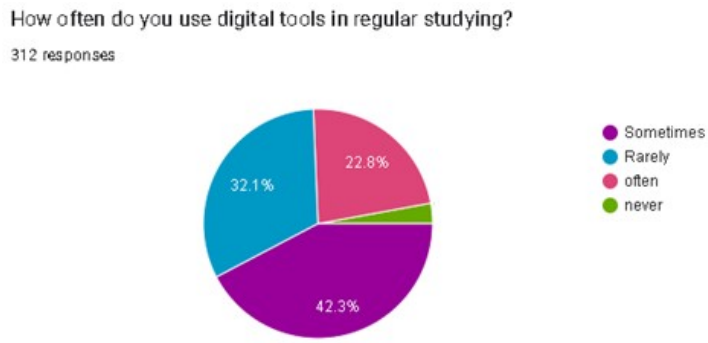


Of the many opportunities offered by digital transformation, 181 respondents chose quick access to information, 146 new ways of learning, 115 decided to use different technologies, while only 68 respondents chose the opportunity to exchange experiences in online communities. The Internet is a public global space used by billions of people with a wide range of information and hence we can see the greater number of respondents who perceive digitalization for creating, sharing and finding information. Digitalization removes all geographical barriers, encouraging global learning. New learning methods through online platforms, online workshops are opportunities used by young people in order to acquire some new digital skills.



54% of the total number of respondents partially know what digitalization is in the educational process, while 33.9% do not know about digitalization in the educational process.

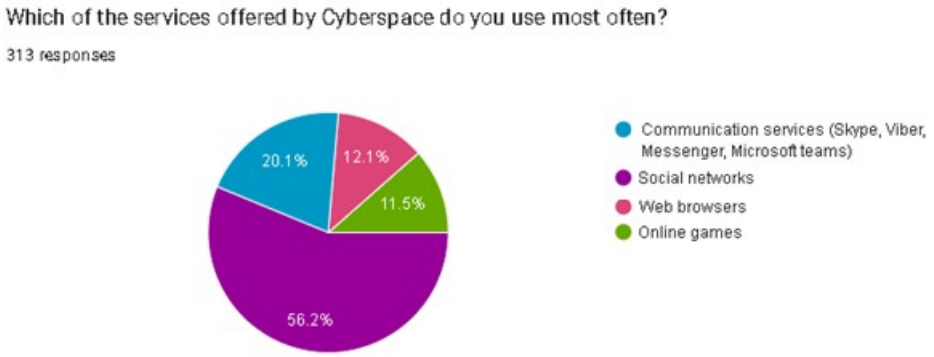
One of the biggest challenges facing today's education is its digitalization. Digitalization does not only include the use of computers and the Internet, but also finding the right information, filtering and processing it. From this finding, we can notice that there is a large percentage of students who do not know what digitalization is in the educational process, thus we can say that each of the students has a different technological ability, which depends on its implementation in the digital process.



To the question: How often do you use digital tools in regular studying? - 42.3% of students declared that they sometimes use digital tools, 32.1% rarely use digital tools.

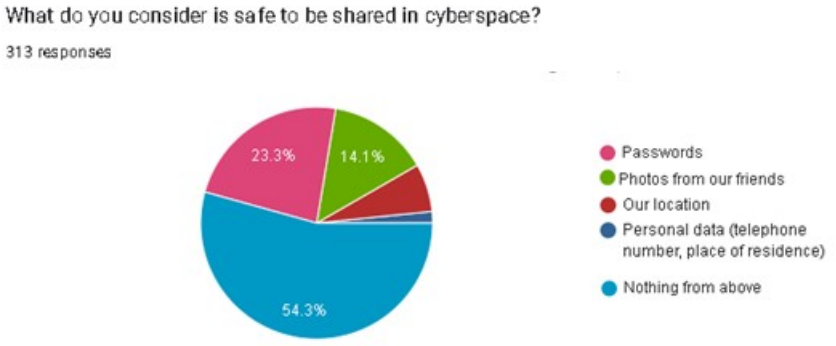
Given this we can conclude that it is necessary to provide students with access to digital learning, with which increased knowledge and skills are expected both in the field of the subjects they are studying and in the field of information technologies and cyber security when using the tools. Digital content should be multimedia, i.e., contain text, animation, sound and presentation. Digital learning content should be available in schools during classes and be present outside of classes in students' homes.

This finding may demonstrate that digital tools are used less often during studying. One of the factors may be the small number of digital devices that the school has or insufficient representation of e-content in the curricula.

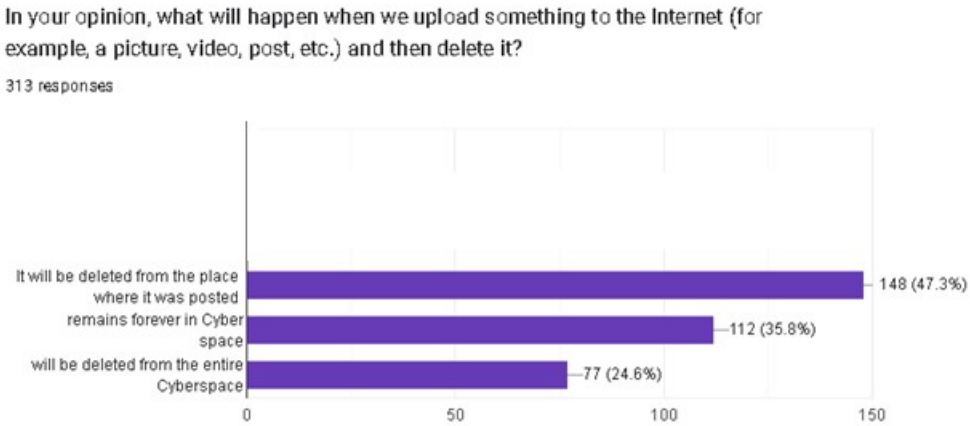


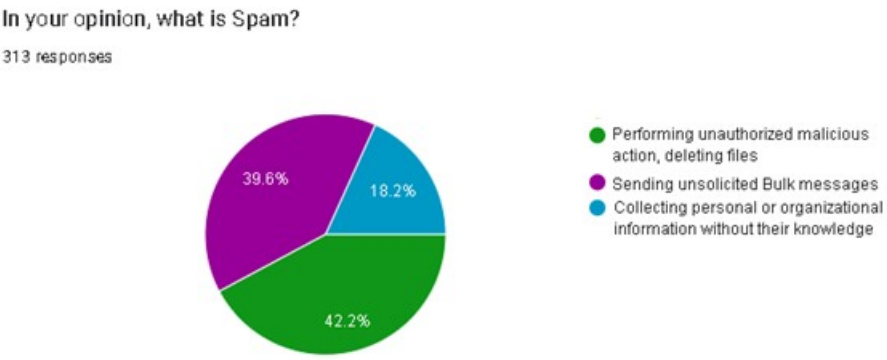
To the question, Which of the services offered by Cyberspace do you use most often? - 56.2% declared that they use social networks. A large part of the young population are users of social networks Tic Tok, Instagram, SnapChat and Facebook. Clearly, they are inherently vulnerable to cyber threats. This finding shows that social networks have easy and open access for users. Much of these platforms share private and confidential information. Young people often consider social networks as fun, giving them the opportunity to communicate, exchange pictures, videos and news. The results show that almost a large part of young people get information through social networks and internet portals. The social life of young people has been transferred to social networks and takes place online.

We can also say that young people are not aware of the risks that social networks have such as: cyberbullying, sharing private data, exposing inappropriate content.

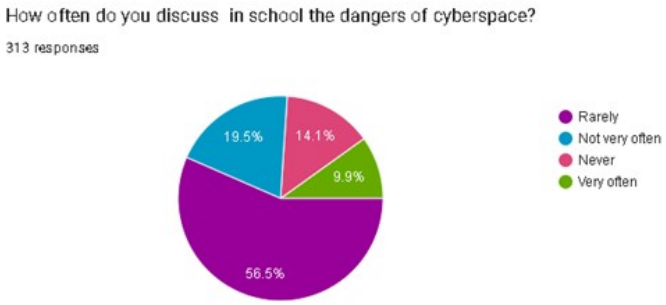


When asked What is safe to share on the Internet? - 54% answered that sharing personal data, location, photos of friends, passwords is not safe, but also 23.3% of the respondents consider that sharing passwords, photos of friends on the Internet is safe. A large number of young people publish photos of themselves and their friends on social networks. They expose themselves to the potential risk of a cyber attack. The fact that 23.3% of young people declare that they can share their passwords without any risk is worrying.

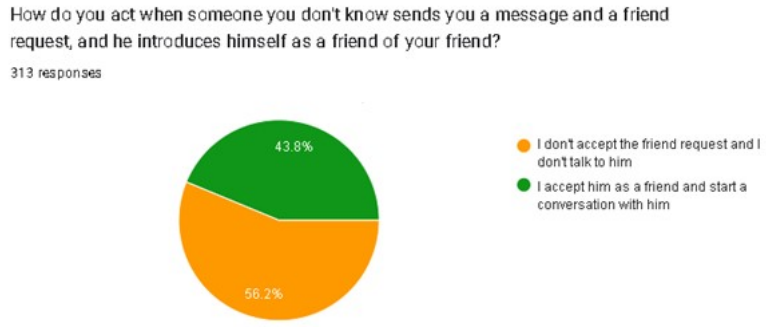


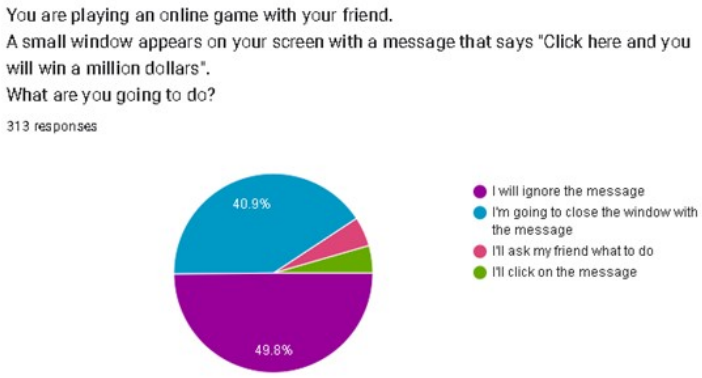


The results of this question show that 39.6% of respondents have real knowledge about the actions of spam messages. Spam emails only become dangerous depending on how you handle them. The use of smart phones is everyday life for young people, so it is necessary to know what happens if they open a spam email. One of the dangers is the content contained in the spam emails, which is used for intimidation. Also, malware that can cause damage to devices. Therefore, it is necessary to know that every spam message can be flagged, then deleted and certain mechanisms can be set to protect mobile devices.

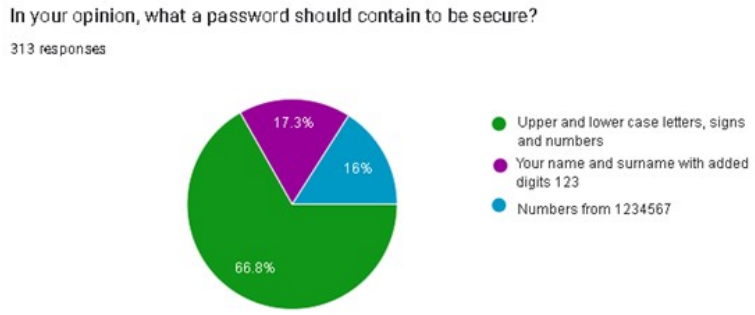


Answers to the question: How often do you discuss the dangers of the Cyberspace? show that 56.5% rarely discuss Cyber security in schools, 19.5% not very often and only a small percentage 9.9% often discuss the dangers in Cyberspace. There is a great need to conduct security awareness training in schools as well as to strengthen data protection on various devices. Students, teachers need access to the learning tools necessary to understand, detect and avoid the cyber threats they may encounter on a daily basis.Recent years show that education experienced record cyber attacks making it the most vulnerable category at risk from malware.

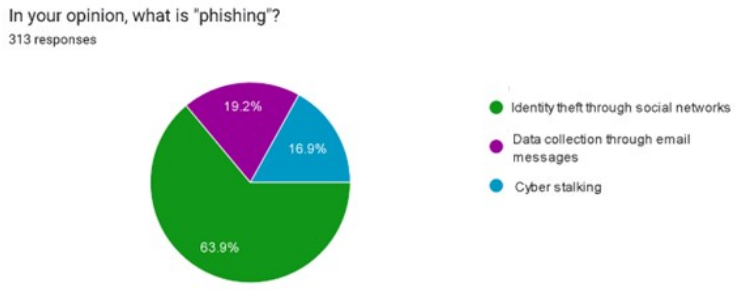




One of the frequent cyber attacks is the collection of data through small pop up windows that deceive users with a monetary reward. 49.8% of respondents ignore the message while 40.9% close the window that appears. Ignoring the message is not the safest way to protect yourself. It's safest to close it entirely through the browser, rather than just hitting the ad close button. Reducing the appearance of such windows can be deleted through the search history.

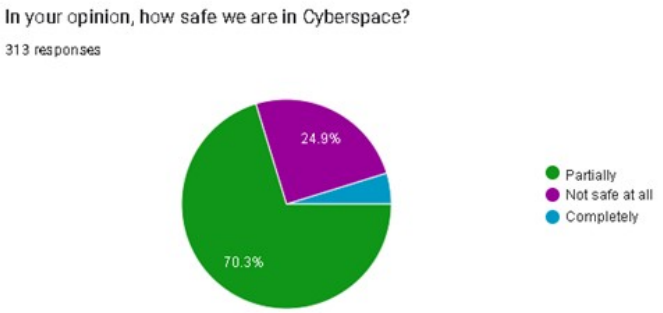


The era of the Internet has presented many risks to people from which we are still not ready to protect ourselves. 16% of the students, when asked what is a secure password for them, answered that the numbers from 1234567 represent a secure password for them. The general rule is to avoid this choice. With this way of creating a password, we become an easy target for hackers. Thus, 17.3% stated that when creating the password, they use the first and last name and numbers 123. We need to avoid such words, we need to add punctuation marks, numbers that can be substituted for letters. One of the rules is not to use the same password for different accounts. Changing passwords more often increases protection against cyber attacks.



63.9% of students declared that phishing is identity theft through social networks. The main purpose of phishing is to collect user data through email messages. Here we can only see that 19.2% partially know the meaning and function of phishing as one of the most frequent Malware attacks. Advanced development of digital skills among young people is needed to be able to recognize phishing.

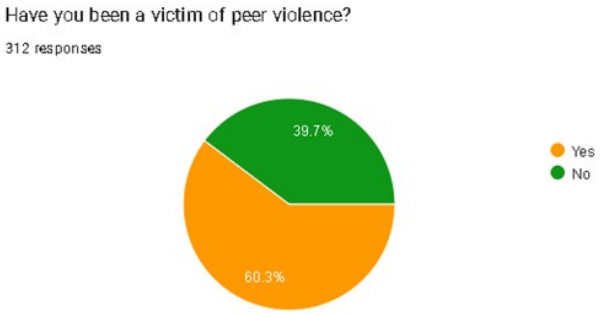
According to the question of whether educational workshops on the safe use of cyberspace are held in the school, 44.4% declared that workshops on the topic of cyber security are rarely held, while 18.2% of students declared that they had never attended a cyber security workshop in their school. In correlation with the second question, a large number of students declare that they need further education on Cyber Security because they consider they do not have enough knowledge about protection against hacker attacks and breach of personal data. The most popular applications used among young people are Facebook, SnapChat, Instagram to contact their friends but also to inform themselves through various news. One of the problems that appears is the authenticity of the information. To what extent young people are digitally literate and educated to protect themselves from fake news. The implementation of Cyber security in schools is of great importance.



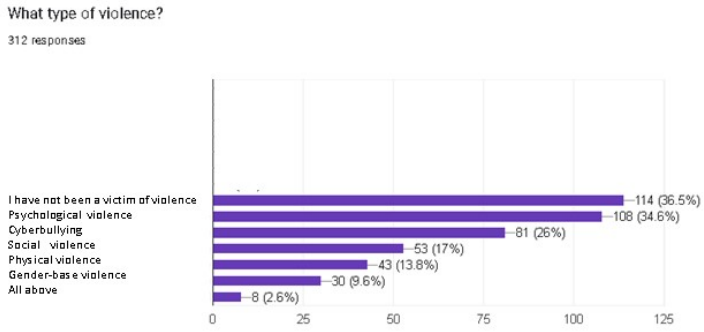
The Internet is the largest and inexhaustible source of information in the history of human civilization, which has contributed to the complete digitalization of the daily functioning of the human.[12] It is impossible to determine the size of the Internet at any given moment, because it is constantly increasing and thus cyber attacks are increasing. The data obtained from the survey indicate that 70.3% of the respondents consider the Internet to be partially secure, while 24.9% of the respondents consider that cyber space is completely unsecure for their data, photos and privacy. This finding shows that students still consider that they are partially familiar with cyber security as a term, but not with the techniques, methods and mechanisms for protection againsthacker attacks.

Also, a large part of the respondents do not feel secure on the Internet at all because they are aware of the dangers that are spreading, they know that their data, pictures can be easily found on different web sites.

12 Alatkazabezbednostizashtitana decata.pdf (ugd.edu.mk)

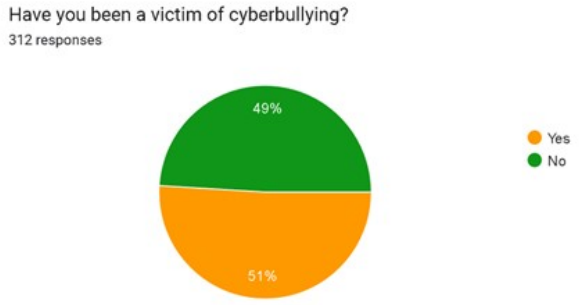


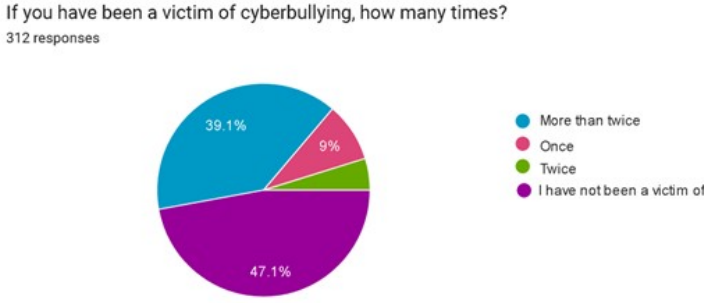
One of the biggest challenges facing schools is peer violence. From the 60% who answered that they were a victim of peer violence, we can say that in schools where this type of violence among students occurs most often, there is a large increase. Peer violence is continuous and can be direct or indirect in order to prove dominance and power in society. Indirect violence can occur in the form of cyber violence by spreading misinformation, hidden profile pictures that will harm the individual. Violence between peers can also be physical, psychological violence, social gender-based violence.



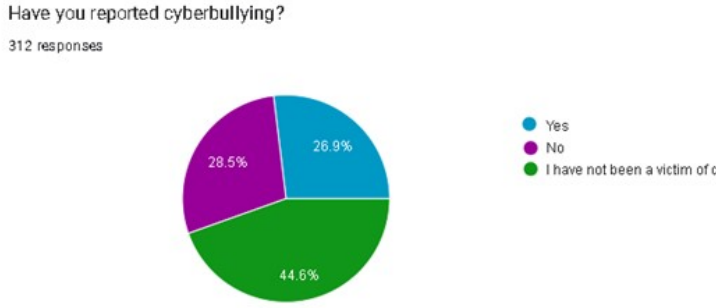
This finding shows that the dominant type of violence that exists among students is psychological violence, since almost 34% of respondents answered that this type of violence is dominant in the school where they are educated. Right behind it are electronic violence and social violence, which are in second and third place. It is worrying that for several years, programs created and supported by the ministries and educational policy-making institutions have been implemented in schools, which aim to contribute to dealing with physical and psychological violence, and yet even in the 21st century, these forms of violence remain dominant.

It is clear that electronic violence is a type of violence that is gaining momentum and is increasingly affecting students and teachers. On the other hand, there is insufficient awareness and skill to deal with it among the students and among the teaching staff. We recon that education is needed for the positive use of technology, which will create safe and effective practices, and is key in the prevention of misuse of technology.

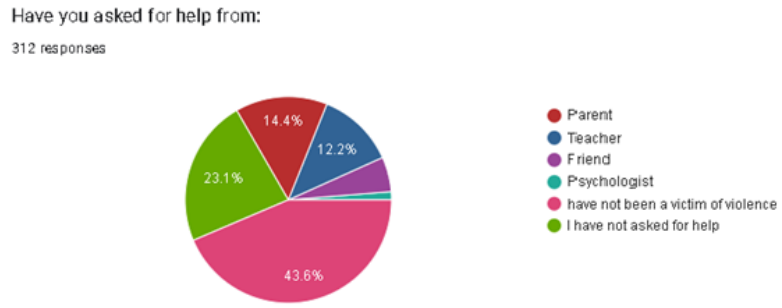




Given these two findings, we can say that the percentage of students who were victims of cyber violence is high, but it is also worrying that 39.1% were victims of cyber bullying more than twice. What kind of changes manifest the children who have been victims of violence, whether teaching staff, professional services and parents could detect these occurrences of violence, what adults have undertaken to deal with violence and provide help and support to students, are issues that should be dealt with in the near future, so that all factors can be involved and change the current situation with violence in secondary schools.

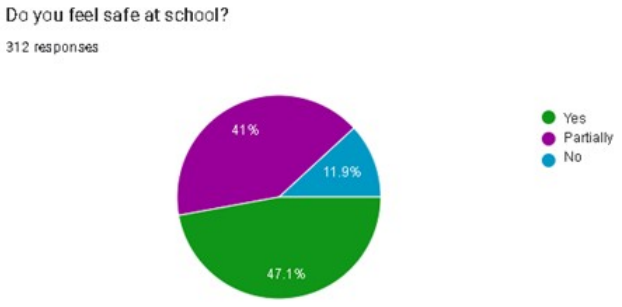


Having the answers to this question, 28.5% of the respondents who were victims of cyber violence did not report it, which indicates that there is still a fear among the victims to report. Young people do not seek help for cyberbullying for many of the same reasons they do not seek support after being bullied in the real world. From the answers given to this question, we can single out the following reasons: They feel embarrassed. They don't want to be seen as snitches and lose even more social status. They fear retaliation. They feel it is their responsibility to deal with it. Hence, there is a need for incitement and encouragement to report the cyber bully as cyber bullying does not stop at schools it continues beyond them.



The answers to this question provide one very important information, which is that 43.6% of students will ask for help and support from their parents to solve the cyber violence they experience, while 23.1% did not ask for help, which is worrying. Another reason that young people are reluctant to seek help from adults about their cyberbullying experiences may be that young people tend to consider that cyberbullying is not a serious problem and therefore they do not need help.

One possible reason why young people do not tell teachers about cyberbullying may be because they do not feel that their school has the resources to deal with cyberbullying. These results suggest that additional training may be needed for teachers to identify effective ways to address cyberbullying in the school environment.



This finding shows that 41% of respondents partially feel safe at school, 11.9% do not feel safe and 47.1% are safe during their stay at school. Schools are educational institutions where children spend a large part of their time and build all their values. It is extremely important that students feel safe, secure and happy at school. It is very important that the school, teaching staff and professional services have a clear policy of zero tolerance of violence and a clear perception of what this means, not only on paper, but how we live and implement it in the way life is organized in the school. It is also important to create a school environment where everyone feels safe, secure and has a sense of belonging. Belonging is especially important for young people. Schools should be places where the integrity and humanity of every child and teacher will be uncompromisingly respected and where there will be measures, training and monitoring for this.

RECOMMENDATIONS FOR IMPROVING CYBER SECURUTY IN SCHOOLS

The problem with cyber threats is alarming in education due to the volume of data that is managed, lack of resources, education of teachers, professional staff as well as reduced awareness of students about Cyber security. The high volume of attacks has determined that schools need to increase measures to protect data from cyber attacks.

Cooperation with institutions such as the Ministry of Education and the Ministry of Internal Affairs from the Cybercrime sector is of utmost importance, because only in this way can the most sustainable solution be found that would prevent and minimize cyber attacks.

Cyber security must be an integral part of the annual curricula of every educational institution. Students and teachers need access to the learning tools necessary to understand, detect and avoid the cyber threats they may encounter every day.

The research showed us that a large number of students were the victims of a cyber attack, but it also proves to us that the students do not have enough digital skills and mechanisms for Cyber Security. In the conducted survey, the results showed that educational workshops on the topic of cyber security are rarely conducted in schools. Hence the need to increase students' awareness of finding cyber mechanisms that will protect them from the risks of the Internet.

In order to improve the situation with the schools, it is necessary to involve teachers, students, the professional service and the institutions.

The following is necessary:

- Informing the teachers, students and professional staff about the latest security risks in order to react promptly
- Finding sustainable anti-virus and anti-malware software solutions to protect school computer systems and block any type of malware
- Regular software updates and maintenance to eliminate any ransomware risk vulnerabilities
- Informing the teachers and students about phishing attacks and their recognition
- Introduction of Cyber security topic content in the curricula
- Trainings intended for students and teachers dedicated to cyber security, the meaning of cyber threats and their prevention
- Organizing workshops in which students, teachers and parents will participate to familiarize themselves with the rules for using Cyberspace.
- Formation of school teams for cyber security composed of trained teachers, students and professional service.
- School teams to prepare and implement a training program to develop mechanisms to prevent a cyber attack
- Developing a cyber culture in schools in order to prevent potential attacks
- Education of the students and parents with the possible legal measures for action against cyber violence and at the same time familiarize the students and parents with the specific articles of the Criminal Code, according to which they are given the opportunity to act
- Proceedings according to the Criminal Code Article 251-Damage and unauthorized access to the computer system, Article 151-a Creating and entering a computer virus and Article 151-b Computer fraud.

USEFYL CYBER SECURITY TIPS

Cyber Security

Cyber security aims to protect us from any malicious digital cyber-attacks. Cyber security can be implemented in schools as well as in all institutions against cyber attacks that are caused through publicly available internet connection, phishing emails, suspicious links, documents or downloadable applications.

The Internet has become our everyday life. In the education, the Internet is extremely important and is also constantly growing. Immediately after the pandemic, children relied only on the Internet to learn. The Internet inevitably became of immense importance. We all feel the need for internet in all spheres of life. In the field of education, the Internet is extremely important and is also constantly growing.

In our educational system, the dependence on the Internet is huge, which makes it necessary to have cyber security against phishing attacks, malware, cyber bullying and other attacks.

The reasons for which such attacks occur are:

- Lack of technical skills and knowledge
- Low awareness among young people about cyber security
- Increased use of the Internet

Protection from cyber grooming

With the growth of social networking platforms, online games and instant messaging apps, chuldren can chat with anyone – friends or strangers – from all over the world. This can benefit many by making them feel less isolated, but for some it can leave them vulnerable to cyber grooming.[13]

Online grooming is when people use fake information and profiles to befriend people online, usually for sexual purposes. This type of attack usually occurs through social media. Children are much more likely to trust information that people share with them without questioning its legitimacy. An online grommer can take the time to learn about their victim, go through their online profiles, find out their likes and dislikes from those profiles in order to find out information about their victim.

There are mechanisms to protect against this type of attack, one of them is the education of young people about cyber security.

Tips for preventing this type of attack:

- Do not install software, games and applications from an unknown source
- Do not accept friendship from an unknown person because it is highly probable that Cyber grommer has created a fake profile in order to chat with its victims
- Setting privacy settings on social networks (posts visible only to friends)
- Avoid talking to people who ask questions about your sexual experiences
- To avoid turning on the web camera when chatting with strangers
- Don't go to meet a person you met only online. Always take a friend or older person with you.
- Do not share photos with strangers

13 Online grooming: what it is and how to protect your child | Internet Matters

Protection from phishing attacks

One of the ways to protect ourselves from these attacks is to know how to detect them. There are several ways of detecting these types of attacks. Email phishing has specific characteristics that can be recognized, among which are:

- Attachments or links
- Spelling mistakes Bad grammar
- Unnecessary urgency to immediately verify your email address or other personal information

https://www.internetsecurity.tips/the-dangers-of-phishing-scams-prevention-and-protection-tips/

Measures to protect against email-phishing are:

Never open alarm messages. Reputable companies will not ask for personally identifiable information or account details via email. This includes your bank, any company you work with.

If you ever receive an email requesting any account information, delete it immediately and then call the company to verify that your account is in order. Do not open attachments in these suspicious or strange emails - especially Word, Excel, PowerPoint or PDF attachments. Avoid repeatedly clicking on hyperlinks in e-mails, as they may install malware.

Be careful when receiving messages from third parties; never click on URLs in the original message. Instead, visit the site directly by entering the correct URL to verify the request.

Maintain the software and operating system. Windows operating systems are often the target of phishing and other malicious attacks, so make sure you're secure and up-to-date.

Protection from cyber bullying

While there is no a complete way to prevent children from being a part of cyberbullying, there are things we can do together to reduce the likelihood of being a target. This includes implementing security mechanisms as well as ongoing conversations about cyberbullying. It is also important to educate young people about how to use social media safely and responsibly and what to do if they are being bullied online.

Some of the mechanisms to protect against cyberbullying are:

Protecting accounts and devices When it comes to preventing cyberbullying, it's important to use passwords for everything. Passwords are one of the most effective ways to protect accounts and devices. It should be emphasized to children that they should never share their passwords with anyone, including their best friend.

Using privacy tools and settings No matter what children do online, we need to familiarize them with the safety tools of all social networks. Almost every social media platform, including Instagram, Twitter, SnapChat and TikTok have privacy settings.

Manage location sharing Some smartphones allow users to share their location with friends. This means that if they share their location with people, these people will always know where they are. Also, some photographers have geo tags that determine the location of individuals. It is very important to know that such photos should not be shared online.

Log out when using public devices

One of the most important rules is to log out of public computers or laptops at school or in the library, from any account. This includes signing out of email, social media accounts, their school account. Closing the tab is not enough. If someone gets on the computer right after it's done, they may still be able to get into your account. And once they have access, they can take control of that account by changing passwords. Once you lose access to your account, it can be difficult and time-consuming to regain control. Refuse to respond to cyber bullies.

Protection from social engineering

The best way to prevent social engineering attacks is to know how to spot them. Once you're already caught in a social engineer's web, it can be difficult to break free. You don't need to be a tech expert to practice good social engineering prevention.

Change your spam email settings

One of the easiest ways to protect yourself from social engineering attacks is to adjust your email settings. You can strengthen your spam filters and prevent social engineering scam emails from slipping into your inbox. You can also add email addresses of people and organizations you know to be legitimate directly to your digital contact lists - anyone who claims to be them in the future but uses a different address is most likely a social engineer.

Explore the source

If you receive an email, text or phone call from an unknown source, enter them into a search engine and see what comes up. If it's part of a known social engineering attack, the sender may have been flagged before. Even if the sender looks legitimate, check anyway, as the email address or phone number may turn out to be just a little different from the real source - and may be linked to an unsafe website. If a web search isn't successful, another way to successfully prevent an attack is to directly contact the organization that claims to have contacted you.

Update your antivirus/antimalware software

Check if automatic updates are turned on. Periodically check if updates are applied and scan your system for possible infections.

Protection from online gaming

Online gaming is fun, but to increase the safety, it is vital to practice cyber security. Here are some protection mechanisms you should follow:

Use strong passwords.

One of the simplest ways to protect yourself is to use a strong password. Keeping track of numerous passwords can be difficult - so using a password manager can help.

Set up multi-factor authentication

If the game offers you two or more factor authentication, enable it. This adds another step to the login process, such as sending a code to your phone number or email address. Two or more factor authentication provides extra security to your game account - some games even offer in-game rewards to players who enable it.

Protect your personal data

Do not include identifying information in your gaming usernames - such as your name, date of birth or location - and avoid sharing personal information on gaming forums. When using your gaming headset, be careful about what personal information you say out loud.

Download only from authenticated sources

Keep your computer and yourself secured by avoiding downloads from illegal sources. Whether it's games or scam codes, downloading from unofficial or pirated sources risks introducing viruses or game malware to your computer.

Keep your software up to date

Make sure you keep your devices and software up to date. Updated software will ensure you benefit from the latest security patches to address cyber vulnerabilities.

Install and use a VPN when playing games

If you play games on a desktop computer, hiding your location is important to protect your identity. When you use a virtual private network, or VPN, your computer can appear to be somewhere else in the world, preventing attackers from finding your location.

Protection from ransomware

Ransomware is a type of malware that can infect a computer and take data from an individual who will keep it until the "ransom" is paid. These types of attacks are dangerous for schools. If they download data, there is a high risk of making it public. There are several ways to protect against ransomware infection.

Data backup

Placing the data on an external drive and online cloud in order to reduce the risk.

In case of a ransomware attack, the user can delete the computer and reinstall the backup files.

Update all systems and software

Always keep your operating system, web browser, antivirus and any other software you use updated to the latest version available. Malware, viruses, and ransomware are constantly evolving with new variants that can bypass your old security features, so you'll want to make sure everything is patched and up to date.[14]

Install antivirus software and a Firewall

Comprehensive antivirus and anti-malware software are the most common ways to defend against ransomware. They can scan, detect and respond to cyber threats. However, you will also need to configure your firewall as antivirus software only works internally and can only detect the attack once it is already in the system. Firewalls are often the first line of defense against any incoming, external attacks. It can protect against both software and hardware attacks.

14 How to Protect Yourself from Ransomware (kaspersky.com)

BIBLIOGRAPHY AND LINKS

1. INFORMATION SOCIETY - INFORMATION SOCIETY RELEASE - NEWS RELEASE Use of information and communication technologies in households and individuals, 2022, State Statistical Office, available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.stat.gov.mk/pdf/2022/8.1.22.36_mk.pdf
2. Prof. D-rGordanaLazetic, D.-N. P-r. (2020). Tool for safety and protection of children from violence in the digital world. Skopje.
3. Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth, Robin M Kowalski 1, Gary W Giumetti 2, Amber N Schroeder 3, Micah R Lattanner 4, Affiliations expand, PMID: 24512111 DOI: 10.1037/a0035618
4. Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective, January 2012, DOI: 10.1332/policypress/9781847428837.003.0012, Publisher: Policy PressISBN: 1847428827
5. RESEARCH REPORT Baseline assessment for awareness raising and capacity building, CRPM
6. Protect your child from online grooming. (2023).
7. Ransomware protection: How to keep your data safe in 2023. (2023).
8. Free Vector | Free vector hacker activity illustrated concept (freepik.com)
9. Cyberbullying Information for Parents | How You Can Help | Kids Helpline
10. The Risks of Online Gaming and How to Prevent Cybercrime (internetsafetystatistics.com)
11. Ransomware attacks nearly doubled in 2021 | Security Magazine

Authors: This Handbook was prepared by Ana Dionisieva, researcher at Analytica think tank.

This Handbook was prepared within the framework of the project "Development of a culture of cyber security in the educational system of North Macedonia - Strengthening the capacity of young people and teachers for the application of measures for cyber security and the development of effective school programs for the prevention of cyber-violence", which is implemented by Analytica - Skopje, with the financial support of the Open Society Foundation - Macedonia. The content of this Handbook is the sole responsibility of Analytica Skopje and in no way can be considered to reflect the views of the Open Society Foundation - Macedonia.