

RESEARCH

ON METHODS OF PREVENTION AMONG YOUNG PEOPLE AS USERS OF SOCIAL NETWORKS



This project is financially supported by the Erasmus+ Program and the Association bears full responsibility for the content of this document, and under no circumstances can it be taken as an official position of the EU and the NA

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Title

“Research on methods of prevention among young people as users of social networks”

Text Copyright ©

Authors:

Mila Georgieva
Petya Sabeva
Shadi Mahmud
Valentina Sabeva
Milena Tsanova
Vladimir Kitanovski
Petra Hauser
Karolina Marzec-Balinow

About the authors:

Association "Follow Me", Dobrich, Bulgaria:

- Associate Professor Mila Georgieva, Ph.D., Department of Health Economics and Management, Faculty of Public Health, Medical University of Varna;
- Petya Sabeva – Healthcare manager;
- Shadi Mahmud – Chairman of Association “Follow me”, Bulgaria,
- Valentina Sabeva- Youth worker
- Milena Tsanova - Youth worker;

University “Mother Teresa” in Skopje, North Macedonia:

- Associate Professor Vladimir Kitanovski, Faculty of Technological Sciences, Mother Teresa University, Skopje;

Academy for political education and measures to promote democracy, Austria:

- Petra Hauser, Director;

Association “URBAN FORUM”, Poland:

- Karolina Marzec-Balinow, Director.

Copyright © Publisher:

Follow me Association, Dobrich, Bulgaria, 2024, ISBN 978-619-92834-2-4(print edition) ISBN 978-619-92834-3-1 (e-book, PDF)

The current “Research on methods of prevention among young people as users of social networks” has been developed under the project "Prevention of youth risky viral trends" with number 2022-1-BG-01-KA220-YOU-000085174, Erasmus+ and as such product it is distributed for free. You can copy, download or print content for your personal use, and you can include excerpts from this book in your own documents, publications, presentations, blogs, websites and teaching materials, provided that suitable acknowledgement of the authors and publisher as source and copyright owners is given. All requests for public or commercial use and translation rights should be submitted to follow.me.association@gmail.com.

Please, cite this publication as:

Georgieva, M., Sabeva, P., Mahmud, S., Sabeva V., Tsanova, M., Kitanovski, V., Hauser, P., & Marzec-Balinow, K. (2024). *Research on methods of prevention among young people as users of social networks*. "Prevention of youth risky viral trends" project with number 2022-1-BG-01-KA220-YOU-000085174, Erasmus+. Dobrich, Bulgaria: Follow me Association.

CONTENTS

ABOUT THE PROJECT	5
I. INTRODUCTION	8
II. METHODOLOGY	10
1. PURPOSE OF THE STUDY	10
2. TASKS	10
3. METHODS	10
4. SCOPE AND TARGET GROUP OF THE STUDY	12
5. TERMINOLOGICAL CLARIFICATION	13
III. METHODS FOR PREVENTION OF SOCIAL MEDIA THREATS – THEORETICAL PERSPECTIVE	14
A. PARTNERING COUNTRIES	14
1. BULGARIA	15
2. NORTH MACEDONIA	31
3. POLAND	43
4. AUSTRIA	51
B. WORLDWIDE	59
C. INTERNATIONAL	98
IV. METHODS FOR PREVENTION OF SOCIAL MEDIA THREATS - SURVEY PERSPECTIVE	109
1. BULGARIA	111
2. NORTH MACEDONIA	128
3. POLAND	144
4. AUSTRIA	159
V. RECOMMENDATIONS FOR PREVENTION OF SOCIAL MEDIA THREATS IN PARTNER COUNTRIES	175
A. TARGETED PROGRAMS AND ACTIONS FOR YOUNG PEOPLE	180
<i>1. Digital media literacy education</i>	<i>181</i>
<i>2. Critical thinking</i>	<i>184</i>
<i>3. Reporting and blocking</i>	<i>184</i>
<i>4. Protection of personal information</i>	<i>185</i>
<i>5. Online harassment awareness and education</i>	<i>185</i>
<i>6. Education about digital reputation</i>	<i>187</i>
<i>7. Raising awareness of fake news and disinformation</i>	<i>187</i>
<i>8. Verification of friends and followers</i>	<i>187</i>
<i>9. Balance online and offline activities</i>	<i>187</i>
<i>10. Positive online engagement</i>	<i>188</i>
<i>11. Support and mental health resources</i>	<i>188</i>
<i>12. Digital citizenship education & responsible social media use</i>	<i>188</i>
<i>13. Screening of young people for problematic social media use</i>	<i>189</i>

B. TARGETED PROGRAMS AND ACTIONS FOR PARENTS & FAMILY	190
1. <i>Encouraging and supporting parental involvement and mediation.....</i>	190
2. <i>Strengthening parent education and skills in digital media.....</i>	190
3. <i>Open communication between parents and children</i>	191
4. <i>Create a family media plan</i>	191
5. <i>Parental guidance</i>	191
6. <i>Attention, monitoring and limiting screen time.....</i>	192
7. <i>Model parenting.....</i>	192
8. <i>Tech-free zones and in-person friendships</i>	193
9. <i>Work with other parents.....</i>	193
C. TARGETED PROGRAMS AND ACTIONS FOR SUPPORT COMMUNITY	194
1. <i>Support and assistance for victims of online risks.....</i>	194
2. <i>Introduction of peer learning programs.....</i>	194
3. <i>Better research of online harms.....</i>	194
D. TARGETED PROGRAMS AND ACTIONS FOR DIGITAL COMMUNITY	196
1. <i>Improving regulation of social media platforms</i>	196
2. <i>Development of social networks intended for the youth</i>	196
3. <i>Transparent and independent assessments.....</i>	199
VI. CONCLUSIONS.....	201
VII. APPENDIX A: SURVEY QUESTIONNAIRE.....	202
VIII. REFERENCES.....	206

ABOUT THE PROJECT

Title of the project: "Prevention of youth risky viral trends", Erasmus+

Duration: 36 months (From 01.11.2022 till 31.10.2025)

Priorities and Topics: Addressing digital transformation through development of digital readiness, resilience, and capacity; Increasing quality, innovation and recognition of youth work; Promoting active citizenship, young people's sense of initiative and youth entrepreneurship, including social entrepreneurship.

The project aims include:

- Improving the skills, knowledge and competences of young people and of those working with them to prevent the risks associated with the use of social networks (including cyberbullying, tracking dangerous risk trends, etc.)
- Prevention and protection from Internet addiction, dangerous encounters with strangers, theft of personal and financial data, lack of face-to-face contact and interpersonal skills, low media literacy, social isolation, reduced mental well-being etc.;
- Improving the quality of youth work and raising awareness about the risks in social networks.

Products of the project:

- Research of current risks, associated with social networks;
- Study of modern methods of preventing risks in social networks;
- Innovative social media risk prevention methodology (including risks such as cyberbullying, low media literacy, belief of fake news and misinformation and tracking dangerous viral trends that can take lives and cause injuries);
- Handbook for youth workers working in the field of digital safety.

This document is part of the activity "Development of results - study of modern methods to prevent risks in social networks".

Target groups of the project: Youth workers, youth leaders, youth, social workers, and other specialists working directly with young people.

Pilot application and multiplication: it will be organized during trainings for youth workers and youth. The sharing and multiplication of the products – during Dissemination events.

Leading organization: "Follow Me" Association, Dobrich, Bulgaria - a non-governmental organization, registered in 2018. It provides professional and methodical support in various spheres of public life - youth; ecology and environment; transportation; administrative capacity, human resources (HR), regional development, competitiveness, territorial and international cooperation, education, youth activities, health care, social activities, psychology, etc. The association has participated in various charitable initiatives, environmental and youth causes, conducting trainings on socially significant topics, organized conferences and seminars, studies and analyses, develops projects, programs, strategies and plans, provides consultations and expertise, research and innovation. The total number of members of the Association and the informal group is 63. Partners are municipalities, kindergartens and schools, administrations and business associations in Bulgaria and abroad.

Project partners: Academy for political education and measures to promote democracy, Austria; "Mother Teresa" University in Skopje, North Macedonia; Urban forum association, Poland.

- **Academy for political education and measures to promote democracy, Austria** (Akademie für politische Bildung und demokratiefördernde Maßnahmen, Austria) - a non-profit association dealing with political education, equal opportunities for unemployed and employed people of all ages, migrants, women in the labor market, innovative, digital trainings, digitization, entrepreneurship education, environmental protection and sustainability. It partners with a variety of schools, companies and public institutions, supporting the personal and academic development of children, adults, senior citizens and disadvantaged people. Every year the team develops and implements 10-15 innovative educational projects in which they participate as leading organization or partners, reaching over 10,000 participants.
- **"Mother Teresa" University in Skopje, North Macedonia** (Универзитет Мајка Тереза, Скопје, Северна Македонија) was founded in 2015. Its mission is to create academic opportunities for students where they can develop as individuals and as professionals by combining competence of critical and analytical thought and nurturing entrepreneurial spirit.

“Mother Teresa” University in Skopje offers education in natural and social sciences through its five faculties: Faculty of Social Sciences; Faculty of Informatics; Faculty of Technological Sciences; Faculty of Technical Sciences and Faculty of Architecture. The University has been awarded the Erasmus Charter for Higher Education for the Erasmus+ program 2014-2020 for supporting mobility opportunities for learners and staff in educational, training and youth institutions and organizations. It collaborates with institutions in higher education, governmental and non-governmental agencies, academics in Macedonia and abroad.

- **Urban forum association, Poland** - a non-governmental organization created to support civic initiatives, social innovation, education and implementation of green initiatives. Urban Forum was created by people with international experience and a local ambition to make immediate environment better. The aim is to actively face the challenges of the future - from the digitization of processes and climate change, through the energy and health related activities of citizens, to ecosystem actions and community building. The association designs and implements new solutions, technologies, civic initiatives and models for local community participation in areas of key importance for the modern world of challenges based on European experience. In 2021, the association has 8 experts.

I. INTRODUCTION

Children and youth are an important element of society, and as no small part of it, they contribute to the evolution of the dynamics of any problem or priority. Social networks play a significant role in the development of young people. Entire generations of students and teenagers experience their world, life and emotions through the filters of their social profile. This is how online social status is born as a term and a way of life, following the pace of collecting likes, friends in the social network, without distinguishing between real and virtual life. And whole generations remain unprepared for real life, but there are real problems for which students - the future adults, remain unprepared for online life as well.

Information flow is currently extremely fast, dynamic and constantly changing. Every online action is monitored and recorded, thereby turning the user into a product. Algorithm-based models are constantly being built to predict our actions and turn communication into a culture of dependency and manipulation. Under enormous pressure to prioritize organizational growth, technology platforms have created and continue to create a race for human attention that unleashes invisible harms on society and especially young people.

As social beings, we all need social connection, approval, and a sense of importance within the group or groups to which we belong. But, if in real life, our group counts less than a hundred direct contacts, in social networks there can be thousands. In the digital space, young people have illusory comfort and social validation available to them – whether it's deserved or not. Social networks create a problem that is changing the way young people perceive the world, their values and decisions.

When we feel uncomfortable or lonely, when we are insecure or scared, when we are stressed or need to feel validated, we resort to the places where it is comfortable, cozy and get the attention we want, namely social media. Getting likes is a psychological form of ego feeding and a need for other people's approval and validation. This, to some extent, makes people unable to act according to their own values, but to depend on the values, ego, and approval of others as criteria of rightness. The maturing and developing personality of the teenage inner child fails to create a unique version of their self, being subject to the expectations of the social network profile. This vicious cycle becomes an even more serious form of control over the personality. Unrestricted exposure to the influence of digital technology can have serious long-term consequences

for youth's development, creating permanent changes in brain structure that affect the way children will think, feel and act throughout their lives.

Some of the concerns about the safety of children and young people and their behavior when using the Internet are related to the increase in social isolation and increasing loneliness, because in most cases teenagers retreat to a secluded place to be online, undisturbed by the offline world. Additionally, some children and adolescents may have their privacy violated online or be exposed to potentially harmful content that may lead to addiction, anxiety, or aggression. And this is a prerequisite for danger, emotional and social isolation and distancing.

In a world where apps are constantly competing for human attention, individual awareness is under attack. Mindfulness means feeling in a calm and balanced way what is happening in our mind, in our body and around us. Mindfulness allows us to act on our intentions and avoid a life that becomes a series of automated actions and reactions, often based on fear, fleeting interest and lack of thinking. Like any other quality, the skill of awareness can be developed and nurtured in the individual¹.

This project aims to shift the focus of attention to the use of social networks and build awareness that there is a problem that is changing the way young people perceive the world, their values and decisions. The goal of this project is to support the development of skills and knowledge in young people to support their safety.

II. METHODOLOGY

The need to develop a methodology for studying the methods for prevention of risks, related to social networks is dictated by recent results from academic research and expert opinions about the positive and negative effect internet may have on young people's development and health. A serious work is needed to prevent risks, related to social media and to be successful it requires a scientific approach.

1. PURPOSE OF THE STUDY

The study aims to investigate, analyze and systematize the methods for prevention of the risks and harms, associated to social networks and their possible negative impact on young people (age 14 – 29 years).

2. TASKS

To achieve the purpose of the study, the following tasks are set:

1. Study of best practices and methods for prevention of risks, associated to social networks from theoretical perspective **worldwide**.
2. Study of best practices and methods for prevention of risks, associated to social networks from theoretical perspective in **partnering countries**.
3. Study the methods for prevention of risks, associated to social networks from a **survey perspective** in partnering countries.
4. Propose a list of **appropriate methods for prevention** of risks, related to social networks among young people in the partner countries.

3. METHODS

The research on current methods for prevention of risks among young people using social networks is conducted by using a combination of desk research and a questionnaire-based approaches. Here the specific methods are listed in both categories:

DESK RESEARCH:

- **Best practices & innovations** – collecting data about successful examples and models of preventing risks and harms, associated to social media, designed to help experts and youth to expand their capabilities and exchange knowledge to reach European levels and standards. The focus is on the published data, analyses and research basically in Bulgaria, North

Macedonia, Poland and Austria, but not only. The research looks for social, civic, and intercultural competencies, media literacy and critical thinking methods for combating risks, associated to social networks.

- **Literature Review:** An extensive review of existing studies, academic papers, articles, and reports on methods of prevention of the risks and harm for young people, related to social networks. This helps in understanding established methods, identifying gaps in knowledge, and determining the current state of research in the field.
- **Data Collection:** Gathering data from reputable sources, such as official reports, surveys, and databases, to collect statistics and information regarding social media usage patterns, efficient methods for prevention of risks and harms and trends affecting young users.
- **Analysis of Platforms:** Analyzing different social media platforms to understand their features, privacy settings, security measures, and policies related to young users. This helps in comprehending the platform-specific risks and vulnerabilities.
- **Analyses and synthesis for identifying trends and patterns:** processing the collected data to identify emerging trends, patterns, and correlations in social media usage and associated risks among young individuals

QUESTIONNAIRE-BASED APPROACH:

- **Questionnaire Design:** Developing a structured questionnaire aimed at gathering insights directly from young individuals regarding their social media habits, experiences, awareness of risks, methods of protection, and encounters with online threats. Questions cover topics such as privacy concerns, cyberbullying, exposure to harmful content, etc.
- **Sampling:** Defining the target demographic (e.g., age group, specific social media users) and employ appropriate sampling techniques to ensure representation and convenience sampling based on the research objectives. The sample of this study of methods for prevention of risks, related to social networks included **392 young people** from all project partner countries:
 - ✓ Bulgaria – 275 respondents;
 - ✓ North Macedonia – 30 respondents;
 - ✓ Poland – 41 respondents;
 - ✓ Austria – 46 respondents.

- **Distribution and Data Collection:** Distribution of the questionnaire through online platforms, schools, community centers, or other relevant channels. Collecting responses anonymously to encourage candid and honest feedback.
- **Data Analysis:** Collating and analyzing the questionnaire responses using statistical tools and qualitative analysis methods to derive meaningful insights and patterns regarding the perceived risks and experiences of young individuals on social networks.

INTEGRATION:

By combining desk research approach with a questionnaire-based approach and qualitative with quantitative data allows a comprehensive view of protection methods young people use in social networks and informing strategies to address online challenges. The specific methods include:

- **Induction, classification, specialization and generalization** related to both theoretical and empirical data, related to the risks and protection methods, associated with social networks. This will allow to reveal the current situation and what can be improved in the area of online risk prevention methods.
- **Triangulation:** Integrating findings from desk research and questionnaire responses to validate and complement each other, providing a comprehensive understanding of the current risk protection methods, used by young people on social networks.
- **Recommendations:** Compiling the research findings into a comprehensive chapter with recommendations, highlighting key findings, trends, prevention methods and suggestions for policy interventions or educational initiatives.

4. SCOPE AND TARGET GROUP OF THE STUDY

The target groups of the project are youth workers, youth leaders, social workers and other professionals working directly with young people to prevent risks related to the use of social networks (e.g., cyberbullying, following dangerous trends, addiction, social isolation, fraud, dangerous encounters with strangers, etc.) and the young people themselves, who will directly benefit from the increased competences and skills of the youth workers. Youth workers typically

work with young people to facilitate their personal, social, and educational development through non-formal education, care (preventive) or leisure approaches. These specialists also deal with the social inclusion of young people, including marginalized groups, enabling youth participation and empowerment, education on youth issues, providing guidance, instruction, mentoring and support. The needs of the target groups were defined based on monitoring tendencies and trends among young people. This revealed the need to help young people deal with the risk of social networks, how they want to achieve them through the implementation of the project, how they can contribute to it through their respective experiences and how they imagine the sustainability of results in the future. Research suggest that there is a need to improve skills, knowledge and competences for the prevention of risks related to the use of social networks, how to apply innovative methods, tools and practices in the field of digital safety; to develop high quality skills to promote social inclusion, active citizenship and good internet interaction; to raise awareness of the risks in social networks and to improve the prevention of dangerous encounters on the Internet, and to improve the quality and image of youth work.

The target groups of the project are:

- young people between the ages of 14 and 29 from partner countries Bulgaria, North Macedonia, Poland and Austria;
- youth workers and other professionals, working with young people;
- trainers and specialists, working directly with young people;
- experts, consultants, pedagogical advisers, psychologists.

5. TERMINOLOGICAL CLARIFICATION

According to Cambridge dictionary² the term **“social networks”** and **“social media”** are defined with the same meaning as: “website and computer program that allow people to communicate and share information on the internet, using a computer, mobile phone or another electronic device”. Therefore, in this document both terms would be used interchangeably to represent all accessible public digital media platforms that allow young people to communicate and share information.

III. METHODS FOR PREVENTION OF SOCIAL MEDIA THREATS – THEORETICAL PERSPECTIVE

Growing up has never been an easy and straight-forward process. The list of problems and challenges children have to deal with or overcome seems to be endless. The puberty brings the rapid physical changes, which can cause concerns, worries and uneasiness. There are different psychological and emotional changes, as the youngsters try to form new social networks outside their family and assert their role in these new relationships. This process helps the young people to become independent and self-confident, but can also lead to conflicts, rejections, disappointments, distress. Inevitably, the path to independence and adulthood leads through a field of new experiences, some of which may be risky or even dangerous. Wanting to fit in with their peers, many young people experiment with alcohol, cigarettes or even narcotics. The sexualized media environment and pressure to have a certain look or appearance can lead to depression, low self-esteem, eating and sleeping disorders and other psycho-emotional problems. Next on the list are the challenges related to school performance, sexuality and sexual relations, inter-generational conflicts, bullying and other abuse among peers. Internet and digital technologies should not be seen as another challenge on this list. Rather, they are a tool through which old challenges can appear in a new form. The more time children spend online, the more risks they face³.

A. PARTNERING COUNTRIES

In a world where the Internet permeates almost every aspect of modern life, keeping young users safe online has emerged as an increasingly urgent issue for every country. While Internet has become an infinitely richer resource for children to play and learn, it has also become a much more dangerous place for them to venture unaccompanied. From issues of privacy to violent and inappropriate content, to Internet scammers and the specter of online grooming, sexual abuse and exploitation, today's children face many risks. Threats are multiplying, and perpetrators increasingly operate simultaneously across many different legal jurisdictions, limiting the effectiveness of country-specific responses and redress⁴.

1. BULGARIA

The information campaign "Live in reality!", project "I and digital reality", which is implemented by the "My City" Association, Bulgaria

In 2020, the "My City" Association implemented the "Me and Digital Reality" project with the financial support of the Ministry of Youth and Sports under the National Program for the Implementation of Youth Activities. Thousands of young people were supported in the fight against aggression and various addictions in the digital environment, through the created interactive training program on the topic: "Recognition of cyber aggression and hate speech", which reached hundreds of young people through 6 video lessons distributed on the YouTube channel "I and digital reality". The project activities also helped 24 young people from Varna to build critical thinking skills, recognizing fake news and the "post-truth" phenomenon. A new educational resource was created - Media Literacy Handbook. A large-scale information campaign was implemented under the title: "Live in reality!", within which an educational film and a series of informational materials were distributed in social networks and media to support young people⁵.

Association "National Association for Development and Support" and the project "Be Safe on the Internet"

The trainings are conducted through an internet platform by the Creativity Training Center and help young people to enrich their knowledge on issues related to psychological differences between generations, cyber psychology and how digital devices affect our real lives.

The participants of the training on the topic "About my digital personality" were made aware of the fact that every action in the digital world can be tracked and recorded, thus everyone leaves a permanent digital imprint about themselves, which can have negative consequences. Particular attention was paid to preventive measures - skills for building digital hygiene, monitoring the information that young people publish about themselves and control of the digital footprint they leave behind.

The "Digital Psychology" training emphasized preventive awareness of the changes that occur in the psyche when interacting with the digital world. Young people aged 20-24 were made aware of the importance of building mental resilience against harmful influences in the internet space, realizing the need to reduce dependence on electronic devices, computer games and social networks and being directed towards their natural environment, related to free communication and sports.

Training on the project "Be safe on the Internet" on the topic "Combating information pressure and misinformation" intended for young people aged 24 to 29 years. The training aims to protect young people from informational pressure and misinformation, which have lasting negative effects on their psyche. It is important for young people to distinguish and not spread fake news by looking for information and being critical of what they read, to reduce the time and psychological consequences of constant information overload, to change the focus of information addiction by focusing on the search for positive news, ideas for sports and a healthy lifestyle and redirect their efforts in a positive direction.

Training program "Cyberscout", Bulgaria, "Applied Research and Communications" Foundation

The mission of the CyberScout training program is to create a community of CyberScout children and youth who demonstrate aware, responsible and safe behavior and promote it among their peers. The practice helps children recognize online risks, master strategies for dealing with those risks, and also introduces them to the options available to report and get help in the event of a problem. Children learn to advise their peers on what to do in the event of an online incident and where to find additional information and materials about using the Internet safely. Cyber Scouts share their knowledge with their peers in an informal setting and organize activities with their participation on topics related to Internet safety and online problem-solving skills. The practice focuses on strategies for prevention, raising awareness, along with defining and adopting safe and responsible behavior online. This not only increases children's resilience

to online hate speech, but also empowers them to recognize hate speech and know how to report it to the authorities.

The target group includes students aged 11-12 years in Bulgarian schools (fifth graders). The practice targets all children of this age group, but the selection criteria give priority to schools with students from vulnerable social groups. The practice has been applied in Bulgaria since 2015. By the end of 2019, over 1,800 students had participated in the two-day training program. A further 3,500 children (ages 11-12) took part in peer learning activities conducted by already certified Cyber Scouts.

The mission of the training program "Cyberscout" is to create a community of children and youth cyberscouts throughout Bulgaria, who demonstrate aware, responsible and safe behavior on the Internet and promote it among their peers. A Certified Cyber Scout is a trained student who exemplifies safe and responsible online behavior within their peer group and can provide them with advice and recommendations on online matters. Cyber Scouts organize and hold events to promote the topic of online safety, both to the public and with a tailored approach to their own peer group. The training methodology is built on the principles of autonomy and experiential learning. The program takes place over two consecutive days and includes eight hours of training for the participants each day. On the first day of training, through a supportive environment and interactive methods, participants are gradually faced with challenges related to the main risks in the online space and ways to deal with them. After each challenge, participants reflect on their experience and apply what they have learned to each subsequent stage of training.

Cyber Scouts gain the following knowledge:

- How to check if a stranger online is who they say they are.
- How to determine if the new "friend" could be a pedophile or not.
- Where and how to report in case of concern.
- How to respond to blackmail or online harassment.

On the second day, participants use the knowledge gained to step into the role of cyber scouts, giving advice to peers and organizing public activities in

simulated and controlled situations. The methodology develops both these practical skills and the teamwork and critical thinking skills of the participants. Future Cyber Scouts are prepared through simulations and discussions for three key roles:

- to be an example of safe use of the Internet;
- to act as advisors and support their peers;
- to reach out to their peers and impart knowledge to them.

Cyber Scouts who successfully complete the training receive a certificate and can participate in a national competition with other Cyber Scouts from around the country. The competition consists of preparing and conducting peer-directed activities related to online risks and how to deal with them. To complete their initiatives, students are divided into Cyber Scout Troops that compete against each other. A special jury selects the three best activities, and the participating students are awarded during the "Safer Internet Day" event, which takes place in Sofia, Bulgaria in February. In parallel with the competition, squads are given the opportunity to participate in monthly missions, through which they further improve their skills as cyber scouts. Communication with all teams that have successfully completed the training takes place through closed Facebook groups. These groups serve as forums for sharing information related to emerging online risks and various initiatives, events, and regular missions in which Cyber Scouts can become involved⁶.

"EU Kids Online" survey of 9–16-year-olds and their parents in 25 countries

Research has long considered the role of parents in relation to their children's media use, typically distinguishing collaborative use - the parent is present, even sharing the activity with the child, active mediation - the parent talks about the content (e.g. interprets, critiques) to guide the child, restrictive mediation - the parent sets rules that limit the child's use (e.g. by time or activities), monitoring - the parent checks the available and technical restrictions - use of software to filter, limit or monitor the child's use of the Internet. A distinctive feature of the EU Children Online survey is that it asks children about several types of mediation practiced by parents, teachers and peers. In practice, it is difficult to

distinguish sharing from active mediation, since sharing an activity usually involves talking about it. Therefore, in the present analysis we combine these concepts, distinguishing instead between "active mediation" of Internet use in general and active mediation of Internet safety in particular. Together they reveal the main sources of support available to children. In terms of policy, this may indicate children's need for additional support, differentiated by demographic factors and by country.

Both forms of active mediation can also be practiced by teachers at school, and in addition, children can support each other by discussing and sharing the use of the Internet; although informal, this represents a potentially valuable form of peer mediation.

Briefly, this section analyses eight sources of social support and mediation available to children:

- Active mediation of the child's Internet use – the parent is present, stands nearby, encourages or shares or discusses the child's online activities;
- Active mediation of the child's Internet safety - whether before, during or after the child's online activities, the parent guides the child on how to use the Internet safely, while also possibly helping or discussing what to do in case of difficulty;
- Restrictive mediation – the parent sets rules that limit the child's use (of specific apps, activities, or providing personal information);
- Monitoring – the parent then checks available records of the child's internet usage;
- Technological mediation of the child's use of the Internet - the parent uses software or parental controls to filter, limit or monitor the child's use;
- Teacher mediation - these questions included a mix of active mediation about the child's Internet use and Internet safety, plus a question about restrictive mediation;
- Peer mediation of child's internet safety - children are assumed to talk about their online activities in general, so the focus here was on peer

mediation of safety practices. These questions were asked two-way – do the child's friends help them and do they also help their friends?;

- Other sources of safety awareness – both parents and children can benefit from a range of sources of guidance – from the media or from experts in their community. The use of such sources was also included.

Handbook “Media Literacy in the Classroom”

In 2019 an initiative has been developed to act at national levels, given the growing importance of ICT in the lives of children around the world and the inherent risks for the youngest in Bulgaria. “**Media Literacy in the Classroom**” is an aid to teaching media literacy and critical thinking. This handbook was developed in cooperation with the Fulbright Commission the America for Bulgaria Foundation and Founder Association of European Journalists – Bulgaria⁷.

In the handbook are included protection methods for dealing with fake news online and ways to spot misinformation or manipulative content. **Special attention is paid to spotting fake news and checking sources of information online**, including following recommendations to young people:

- ***Pay attention to the domain and internet address.*** Established news organizations usually own their own domain and have a standard look that you are familiar with. Sites that end in ".com.co" should make you think twice and tell you to do a little more digging to see if you can trust them. This is even if the site looks professional and has a semi-recognizable logo. For example, abcnews.com is a legitimate news source, but abcnews.com.co is not, even though it looks similar;
- ***Check the "About Us" section.*** Most sites would have a lot of information about the newsroom, the company that runs it, the members of its management, the mission and ethics of the organization. And the language used is simple and clear. If it's melodramatic and seems pretentious, you should be skeptical. You should also be able to find more information about the organization's leaders outside of this site as well;

- **See the quotes in the material.** Or rather, look at the lack of citations. Most publications have multiple sources in each of their publications who are professionals and knowledgeable in the field in which they speak. If the topic is serious and controversial, it is even more likely to have many citations;
- **Look who's saying them.** After finding the quotes, see who is speaking in the article and what exactly they are saying. Are these people reputable sources with a title that can be verified after a quick Google search? Find out what the speech was about, who it was aimed at, and what happened next;
- **See the comments.** Many of these fake or misleading stories are shared on social media. Headlines are meant to grab readers' attention, but they should also accurately reflect what the text is about. Recently, however, this has not been the case. Headlines are often written in exaggerated language with the intent to mislead and then tacked on to posts that are either on a completely different topic or simply not true. This type of post usually generates a lot of comments on Facebook and Twitter. If a large number of comments claim that the article is false or misleading, it probably is;
- **Search for the photos on Google.** A picture should do justice to the story it illustrates. That doesn't happen often. If the people who write fake news don't even leave their homes or interview anyone for those articles, they're unlikely to take their own photos either. If the photo appears on many other sites on many different topics, there is a good chance it does not illustrate what the first story claims;yut
- **Help a friend.** If you see your friends sharing obviously fake news, be a friend and politely tell them it's not true. Don't shy away from engaging in such conversations, even if you find them uncomfortable. As we've said before, everyone can help tackle the problem of fake news.

Another section of the handbook is dedicated to **protection of personal information and privacy**:

- **Personal data** is information that allows you to be identified. There are different categories of personal data: racial or ethnic origin, political beliefs, religious beliefs, sexual orientation, personal health and intimate life. Biometric and genetic data are also a special category of personal information. Your data can exist in many different forms – in paper or online format, as part of a written or oral communication, and in the form of an image, video, sound, or fingerprint. When you interact with the public, there is a high probability that you will be photographed. If this happens, and our image is saved by someone else, it can subsequently be used for various purposes. In situations where we ourselves actively share our image, for example posting a selfie on Instagram, our personal control over the use of the image is one aspect of the human right to privacy. We have the right to refuse the recording, sharing or storage of our image, as well as its publication by other people or institutions. At the same time, our right to control one's personal image may collide with other people's rights. In most cases, it is about freedom of expression, for example in cases where a journalist wants to publish or broadcast material of public interest, and our image is part of it. If we believe that our image has been recorded or used illegally and our right to privacy has been violated, we have every right to file a complaint against the media that violated our rights;
- **The right to privacy** is our right to control other people's access to and sharing of our personal information. We have the right to control the information related to our name, social security number, address, date of birth, personal correspondence, relatives, family and intimate life, health status. The right to privacy also includes the right to be left alone. Privacy is our basic human right that should be respected by all of society. However, in some specific cases there may be a good reason to disclose someone's data, for example when it is a matter of public importance. What and how can be disclosed and when it is in the public interest is a matter of discretion on a case-by-case basis. The public status of the people involved is also linked to public interest in their private lives. In the case of a public figure, such as a politician, whose actions have a high level

of public interest, the disclosure of data from their private life is considered more permissible than cases involving ordinary citizens;

- **Consequences of oversharing personal information on social networks** - media use supports young people's communication, entertainment and information needs, but sharing too much personal information can be dangerous. Social networks encourage their users to share personal data and details of their daily lives. As a result, private companies use our personal information to profile us for advertising purposes, employers check the Facebook profiles of job applicants, and thieves can learn when a family is away and rob it. Parents should also be aware that sharing too much information about their children on social media carries risks. They should remember that some things are better kept private;
- **How to protect your personal data in social networks?** with recommendations including following methods:
 - Use complex passwords and never use the same password for your accounts on different platforms.
 - Don't use social networks on public devices, for example on school computers, and if you have to, don't forget to log out of your account.
 - Do not allow your mobile apps to access your geolocation.
 - Be careful when following links shared by your friends on social networks - they may contain viruses or be hacked.
 - Use a two-factor authentication system or regularly change the passwords of all your online accounts.
 - Even on your personal social media profiles, share a minimal amount of personal information.
 - Think about who might read your posts.
 - Avoid filling out too many of the personal information fields in your profiles, such as city of birth, birthday, family members, etc.
 - Share your travel information carefully.
 - When you share something about you – whether it's a photo, video, or personal information like your phone number – be aware that it can end up being seen by people you didn't mean to send it to.

- It is also not a good idea to share anything when you are too emotional - whether you are angry, sad, or excited. Calm down first and then decides if it's a good idea.
- When you post your photo, answer the questions: Is this how I want people to see me? Can someone use this to hurt me? Will I be upset if someone shares this with others? What's the worst that could happen if I share this?
- Image is forever: Some people think that sharing a provocative photo with your partner shows that they love or trust them. Be extremely careful in such situations and think - the image can outlive the relationship.
- Think: Do you know everyone on your "friends" list? Why are you "friends" with someone online if you don't know each other? Will it be a problem if you delete it?
- If you don't want to delete these people from your contact list, consider how to limit their access to information about you.
- **Responsible use of social networks** - The term "information bubble" refers to a situation of online isolation in which a person finds himself because of the choice of friends, his political leanings, the information sources he uses most often. Because of the sources of information selected or by the algorithms of social networks, it often happens that it is more difficult for us to receive information that does not correspond to our beliefs, and mainly we allow information that reinforces them. This hides the danger of surrounding ourselves with a "bubble" of information that creates an illusory view of the world in which we live. And to make us hold wrong theories for a long time. A situation where objective facts take second place in shaping public opinion on a given issue, giving way to opinions that evoke emotional reactions and are based on the personal understandings of individual users. The development of technology has made it easier for everyone to live in their own "information bubble". The line between truth and lies in society is blurring;
- **"Viral" distribution of content in social networks** - the "contagious" distribution of content on the Internet is a phenomenon in which a piece

of information (video, photo, illustration, article, quote, idea, event, etc.) spreads across the web and social channels on the Internet like a virus, from user to user. Viral is often driven by an emotion that drives a user to share it – the information matches the user's own beliefs or interests. It's not just fake news that goes 'contagious' on the internet - so do all kinds of news, fundraising campaigns, funny pictures, music videos, etc. Due to the constant connection of a large part of people in social networks, the exchange of information at the local, national and sometimes international level is extremely fast, which brings with it both opportunities to reach many users and risks associated with the dissemination of false or misleading content⁸.

Recommendations of UNICEF, Bulgaria, for the prevention of cyberbullying among young people

The recommendations were compiled by UNICEF specialists, international experts on cyberbullying and child protection, together with experts from Facebook, Instagram and Twitter. They include description of cyberbullying, explaining the difference between teasing and bullying, what are the consequences of cyberbullying and why is whistleblowing important. There are specific recommendations for prevention of young people against cyberbullying, including: *“If you believe you are being bullied, the first step is to seek help from someone you trust, such as a parent, relative or other trusted adult. At school, you can turn to the pedagogic advisor, the sports coach or your favorite teacher. If you don't feel comfortable talking to someone you know, call a helpline to talk to a professional counsellor. If the harassment is happening on a social media platform, you can block the person who is harassing you and formally report their behavior to the platform itself. Companies that operate social networks are required to maintain the security of their users. It would be helpful to collect evidence - text messages and screenshots of social media posts to show what's going on. In order for bullying to stop, it must be identified and reported as something important. It would also be helpful to show the bullies that their behavior is unacceptable. If you are in immediate danger, you should contact the*

police. In order for bullying to stop, it must be identified and reported as something important."

In the recommendations are included also practical suggestions for actions in Facebook and Instagram – two of the most popular online social networks among young people in Bulgaria.

Safenet.bg The Bulgarian Center for Safe Internet

The Bulgarian Safe Internet Center has been operating since 2005 with the partial financial support of the European programs "Safe Internet" and since 2014 - "Better Internet for Children". It is coordinated by the non-governmental Foundation "Applied Research and Communications" in partnership with the "Parents" Association. The main activities of the Center include:

- processing reports of child pornography and computer abuse against children and minors;
- counselling by phone and online channels for children, minors, parents and teachers in case of incidents involving children online;
- developing and conducting various trainings for children, young people, parents, teachers and other professionals;
- development of various materials aimed at increasing public awareness of the risks for children when using the Internet, social networks and mobile devices, as well as ways of prevention and seeking help.

The center is a member of the European network of 30 centers for safe internet Insafe, as well as the International Association of Internet Hotlines INHOPE, which unites 42 countries⁹.

Yettel Bulgaria - Digital Scouts - the game that teaches children how to deal with dangers online

Yettel's online quiz - *Digital Scouts*, gives children and young people the opportunity on 29 and 30 December to demonstrate their knowledge and skills in dealing with online dangers. *"Know before you scroll"* is the main message of the fourth edition of Digital Scouts, which is part of the company's long-term Safer Internet program. Within 48 hours, kids will be able to answer questions

related to topics such as online bullying, password reliability, identity theft, phishing, malware, dangerous and inappropriate online content, and more. All those who participated in the two days of the game and answered the questions correctly in the Digital Scouts app were entered into a raffle for great prizes to encourage their desire to acquire new skills. Prizes include the latest iPhone model, Huawei smart bracelets and wireless headphones. The app is available to download completely free of charge on Google Play and the App Store. Recognizing dangerous situations for this target group is among the valuable skills that every child and teenager is important to acquire, especially today when children spend a large part of their time online, including for educational purposes. To date, Yettel's campaign has had three successful editions, reaching a total of 56,000 youth. The app teaches:

- How to protect your personal information on the Internet?;
- Is it okay to communicate with strangers on the Internet and, if it happens, what should you do?;
- How to react if someone is harassing you on the Internet or you witness your friend in such a situation?;
- What information on the Internet can you trust and how can you check if it is true?¹⁰

Yettel's Tips for Teens to Use the Internet Safely

New technologies and the Internet offer unlimited opportunities, but they also contain many risks. Sharing personal data can lead to unpleasant consequences in personal life. Uploading photos from a fun party today can have ramifications later when a potential employer is reviewing your application for a job. The Internet is a virtual place and not everyone is who they say they are.

- Be careful when providing personal information on the Internet;
- Posting or providing personal data or information online can be dangerous and lead to negative consequences in real life. Under no circumstances should you give strangers information about yourself, your family or friends (name, home address, phone number and other personal data);
- Not everyone on the internet is your friend;

- Do not meet people you met on the Internet - this can be dangerous and seriously endanger your security. There are people on the Internet who do not pretend to be who they are - for example, adults pretend to be children or teenagers;
- Don't forget that the username is a kind of "business card";
- Be careful when choosing a "username" (username) because a provocative username would increase the risk of harassment by ill-intentioned people;
- It is impossible to completely remove online content once uploaded;
- Whatever you upload is forever. Even if you later delete it, there is a chance that the uploaded content has been copied, redirected or forwarded. In addition, there are web archives that preserve content even after it has been deleted from a site;
- The background or foreground of the photo says a lot;
- Think about what is visible in the scene you are shooting - posters or pictures on the walls, signs, street names, car numbers - this information could reveal the location of the action;
- You are what you wear;
- When taking pictures, think about what your appearance says to people. Would you feel comfortable showing this photo to your boss or potential employer, your family, or even your future spouse's relatives?;
- Respect the personal rights of others;
- Be respectful of the personal rights of others. If you are taking pictures in a public place, make sure you are allowed to take pictures of bystanders and never take pictures of children without their parents' permission;
- You must be a good internet citizen;
- It is your right to express your point of view and even make jokes about public figures or politics, but no threatening or obscene language should be used. You may be held liable if you defame, insult or embarrass someone;
- You have to follow the rules;

- Most sites have terms of use that you must adhere to. Most of them strictly prohibit images with sexual content, violence, texts or images that constitute harassment, defamation, pornography, incite hatred, hatred or violate the privacy rights of others;
- You must respect copyright;
- All serious sites prohibit the use of material without the permission of its author - for example, a television or film company. Be careful about the music, photos and videos you upload;
- Choose safe and decent places on the web for dating and entertainment.
- Some sites can surprise you unpleasantly.

Project "Be safe on the Internet" - National program for the implementation of youth activities, Ministry of Youth and Sports Republic of Bulgaria¹¹

The project "Be safe on the Internet" is implemented by the Association "National Association for Development and Support" - Plovdiv, financed by the Ministry of Youth and Sports under the National Program for the Implementation of Youth Activities, Thematic Area "Prevention of cyberbullying and abuse online, disinformation and the spread of fake news".

The activity aims, on the one hand, to raise awareness of issues related to cyberbullying, online abuse, disinformation and the spread of fake news, with the aim of prevention and ways to recognize and deal with these threats. On the other hand, to comprehensively promote and ensure transparency in the implementation of the project financed by the IMS. The campaign also covers the Internet through social networks and the newly created electronic page for the project.

The project provides training on the prevention of cyberbullying and online abuse, disinformation and the spread of fake news. The three most important elements in the information security of young people are affected. The trainings are held with young people of different age groups, distributed by age and topics as follows:

1. "Info about my digital personality" (intended for young people aged 15 to 19) - aims to learn to avoid potential risks in various situations
2. "Digital Psychology" (intended for young people aged 20 to 24) - will reveal the connection between the digital world and human psychology
3. "Combating information pressure and misinformation" (intended for young people aged 25 to 29 years) - based on the acquired knowledge, a clear reflection will be built on countering false information on the Internet

2. NORTH MACEDONIA

In Macedonia, in 2022, "Kairos" - a media and communications journal was founded by the Institute for Communication Studies from Skopje, Macedonia. "Kairos" is an open access international scientific journal and a platform for the exchange of knowledge and ideas between teachers, academics, researchers, students and other professionals in the field of media and communications. It is intended for the academic and professional public who want to discuss innovative ideas and practices, and it also contains case studies from this field¹². The journal will be devoted to current issues and future trends and developments in media and information studies, media education, as well as their sociological, psychological, political, linguistic and technological aspects. In one of the papers entitled "How schools use public relations and social media to inform the public" it is recorded how a primary school in the country uses social media and how it avoids risks in social media. Social media provides a world of opportunities for an organization or individual to promote and expand a brand. A powerful form of communication that uses the internet, social media can provide any organization with a strong global presence. Because these platforms have billions of users across the world, many organizations view social media as a vital tool in reaching a large number of potential prospects, customers, partners, employees, and advocates all at once. Ultimately, social media platforms enable an organization's representatives and its followers to have interactions that involve sharing information, exchanging feedback, and creating content.

How to Protect Against Threats on Social Media Platforms

Social media can increase brand awareness and engagement with the public. It allows for a generally less-expensive form of advertising in a non-traditional way. There are many types of social media, from blogs to photo-sharing sites to instant messaging or video-sharing portals and more. That said, as with almost every form of new technology, social media does come with its own set of challenges too. One drawback for those using social media is that it can put users

at risk because it can open pathways that are insecure or tunnel beneath traditional cybersecurity.

How Does Social Media Affect Security?

There are five social media-related cyber threats to be aware of and to protect against. They include the following:

1. Social Engineering

Social engineering refers to a wide range of attacks that leverage human interaction and emotions to manipulate a target. Such an attack attempts to fool victims into giving away sensitive information or compromise corporate security. A social engineering attack typically involves multiple steps. The attacker will research the potential victim, gather information about them, and then use this newly acquired data to bypass security protocols. Then the attacker works on gaining the target's trust before finally manipulating them into divulging sensitive information or violating security policies. Obviously, Thanks to its casual nature, social media provides a social engineer with an avenue to naturally engage with the potential victim or organization to push them for information that can then be used to help launch an attack.

2. Phishing

In a phishing attack, usually via an email or an online message, the cybercriminal baits the potential victim(s) by trying to entice them into clicking on a malicious link or opening a malicious attachment. If the attacker uses social media to establish a rapport or relationship with their target, it will be easier to build the trust necessary to get them to click on malicious links or enter sensitive private information into an online form. Cyber criminals also apply pressure on their potential victim(s) by creating a sense of urgency or appealing to their curiosity. "Act now before it's too late..." is the epitome of the kind of encouragement an attacker uses on their target to get them to either click on a malicious link or provide private information via a form.

3. Malware

The malicious links promoted in social media lead to malware. Malware is the portmanteau of malicious software. There are many different types of malwares, such as viruses, trojans, spyware, and ransomware. Cyber criminals use malware to access devices and networks to steal data and take control of systems, create botnets, crypto jack, or damage systems.

4. Brand Impersonation

Another risk created by social media is when an individual or group tries to impersonate a well-respected company or brand to trick victims (employees or individuals) into providing confidential and valuable information that can be used by social engineers to hack systems and networks. In addition to harming the victims who fall for such impersonation tactics, brand impersonation can also damage the reputation of the organization being impersonated.

5. Catfishing

When a person takes information and images from another to create a fake identity and then uses this false identity to victimize an individual on a social media platform, it is known as catfishing. The cat fisher usually uses a fake identity to trick targeted individuals into associating with them or doing business online with the goal of stealing from the victim or humiliating them, or both.

7 Social Media Security Best Practices

The best practices for addressing social media threats include these seven strategies:

1. Enable multi-factor authentication. Multi-factor authentication is a security measure that protects individuals and organizations by requiring users to provide two or more authentication factors to access an application, account, or virtual private network (VPN). This adds extra layers of security to combat more sophisticated cyberattacks even after credentials or identities have been stolen, exposed, or sold by third parties.

- 2. Do not re-use passwords.** Use a different password for every account. This prevents other accounts from being easily accessed if one account is hacked. Use a password management tool to keep track of various passwords and make sure passwords are not easy to guess.
- 3. Regularly update security settings across platforms.** Stay on top of social media platform security options to ensure they are always current and set at the most stringent level.
- 4. Narrow down connections to reduce unknown threats.** Be wary of the types of individuals and entities that you are connecting with on social media platforms. Carefully review every connection, and don't affiliate with those that appear disingenuous or suspicious.
- 5. Monitor social media for security risks.** Stay aware of the threat news on specific social media platforms and respond accordingly. If you learn of vulnerabilities or hacking incidents, attend to your accounts and address issues that could lead to breaches or hacks.
- 6. Learn what a phishing attack looks like.** Be diligent and educate yourself on the latest types of phishing attacks going around, and always be skeptical when someone reaches out to you uninvited via a social media platform or email.
- 7. Look out for spoofs of your account.** Keep an eye out for brand impersonation attempts, report violations to the social media platform administrators immediately, and inform your followers as well.

What Is multi-factor authentication and why Is It Important?

Multi-factor authentication (MFA) is a security measure that protects individuals and organizations by requiring users to provide two or more authentication factors to access an application, account, or virtual private network (VPN). This adds extra layers of security to combat more sophisticated cyberattacks, since credentials can be stolen, exposed, or sold by third parties. Much like an organization might employ various layers of physical security, such as a fence with a gate, a guard station, an ID scanner, and locks on the doors, an organization can also use MFA to provide multiple layers of virtual security to

make sure anyone accessing the system, whether onsite or remotely, is both authorized and authenticated.

How Does Multi-Factor Authentication work?

A user is first prompted for their username and password, standard credentials used to log in, but then they are required to verify their identity by some other means. The most common is to enter a code sent by email, Short Message Service (SMS), via a mobile authentication app, or to a secondary device, but other forms may be hardware that scans biometrics or prearranged security questions. This second or even third factor in the authentication process serves to verify the user request is genuine and has not been compromised. Examples of Multi-Factor Authentication. MFA uses three common authentication methods to verify a user's identity:

1. **Knowledge:** This is the factor users are most familiar with. The user is prompted to supply information they know, such as a password, personal identification number (PIN), security key, or the answer to a security question.
2. **Possession:** This factor verifies the user's identity using something they possess. For example, by sending a code to a mobile phone.
3. **Inherence:** This factor verifies the person by some unique personal attribute, such as biometric authentication or voice recognition.

Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA)

Two-factor authentication (2FA) is a subset of MFA, both increasingly being employed to increase security beyond the level provided by passwords alone. 2FA, as its name implies, requires users to authenticate their identity using two steps that serve to validate their access. Most often, 2FA uses the "possession" factor as the second level of security. After a user enters their credentials, which the system recognizes as valid for network access or for logging in to an application, the server would then request an additional credential, such as a temporary code or password sent to a mobile device. Since a cybercriminal would most likely not have the user's mobile device in their possession, this

makes it difficult for them to steal a user's identity or account. Additionally, 2FA protects the organization, even in situations where a user's primary credentials have been stolen, since the second layer is still inaccessible to the thief. Each additional security layer added beyond 2FA protects the user and the organization even further, demonstrating the value of MFA.

Multi-Factor Authentication and Single Sign-on (SSO)

SSO, also called a unified login, is a method of identification allowing users to sign in to multiple websites and applications with a single set of unique credentials. While MFA may be included in the first login experience, SSO then authorizes the user to access all sites and applications to which they have been granted permission. This provides a better user experience since the user would not have to submit to the MFA process each time, they need to access something within the system. The fact that MFA provides layered security at the outset, authenticating the original login, helps to protect the organization from having the SSO exploited by malicious third parties. Given the growing sophistication of modern threats, we here at Fortinet often spend time discussing cutting-edge technology and strategies to secure today's complex, evolving, and highly distributed networks. However, everyday cybersecurity efforts often come down to something much simpler: passwords.

The 10 Password Security Best Practices

These practices could minimize password-based cyber risk when creating new accounts or updating well-used passwords:

Password Creation and Maintenance

1. **Multi-factor Authentication** – Add an extra layer of security by using multi-factor authentication wherever possible. This confirms your identity by utilizing a combination of multiple different factors, such as something you know or something they have, such as a token generator on your smartphone.
2. **Unique Passwords** – Never repeat the same password for different accounts.

3. **Routinely Change Passwords** – Change your passphrase at least every three months. This will lock out cyber criminals who may be using your account, protect you from brute force attacks, and remedy the issue caused by cyber criminals who purchase lists of usernames and passwords obtained through data breaches.

Physical Password Security Best Practices

4. **Maintain Privacy in Public** – Ensure no one is watching as you enter passwords.
5. **Remain Vigilant When Downloading** – Be cautious when downloading files from the internet as they may contain keyloggers or password grabber malware variants that will compromise your password. A good practice is to regularly scan for the presence of such malware.
6. **Implement a Cloud-Based Password Manager** – Use a cloud-based password manager to enable you to create and store strong passphrases. This is especially important if you require strong passwords for dozens of accounts. Password management tools allow you to securely store an encrypted list of passwords in the cloud that can be accessed from any device. Not only will you only need to remember one password to access your password locker, but the passwords you store there for your various accounts can also be even stronger because you don't have to remember them.
7. **Change Passwords When Leaked** – Change any passwords if they are stolen. Cyber adversaries are constantly tweaking their tradecraft to ensure successful intrusions in order to generate consistent revenue and profit. If your password is guessed or stolen, you may never know it happened until anomalous purchases appear in your bank account. And even more challenging, you may not be impacted directly at all. Data accessed by leveraging your compromised account may simply be used to move up the food chain, enabling an attacker to gain access to data and resources managed by someone else.

Common Mistakes

8. **Choose Hard-to-Guess Passwords** – Avoid using common words, phrases, and number combinations. Short, simple passwords take fewer resources for hackers to compromise. Some of the most common passwords are baseball and football team names, any variant of 123456789, and QWERTY.
9. **Avoid Using Personal Information** – Avoid using information linked to your personal identity, including birthdays, phone numbers, or the name of a pet.
10. **Don't Use Simple Obfuscation Techniques** – Don't use simple obfuscation techniques. "P@\$\$w0rd" is slightly more difficult to guess than "Password."

Implementing a strong passphrase is one of the easiest ways to protect yourself, your devices, and your personal and corporate data from these cyber threats. The basic rule of thumb is that the longer and more complex the password, the more difficult it is to crack. However, unless done carefully, it can also be easier to forget. Weak Passwords Create Cybersecurity Risks. According to the Verizon Data Breach Investigations Report, 81% of breaches leveraged either stolen and/or weak passwords. That problem is compounded because one of the biggest risks to data security is the reuse of passwords across accounts. Suppose one of your accounts is compromised and your username and password are posted on the dark web. In that case, cybercriminals who know how often passwords are reused will simply begin to plug that information into other possible accounts until they unlock one that uses the exact same credentials. This is a common risk, as 83% of people have admitted to reusing passwords across multiple sites. Even if you think it is safe to reuse passwords on accounts that don't house sensitive data – a breach there can be used as an entryway to move laterally across networks in search of critical business data or personally identifiable information (PII). Physical security of passwords is also important to keep in mind. The average US email address is associated with 130 accounts. With so many passwords to remember, many have admitted to writing passwords down on pieces of paper or keeping a list of passwords in unsecured documents on their computers. These items can easily fall into the wrong hands – whether they are simply lost or compromised in a malware attack.

Promoting Data and Network Security on World Password Day

Insecure or inadequate passwords are an easy target for cybercriminals. Accessing a network using a stolen password is much easier than breaking in through edge security protocols. Attackers can uncover or bypass weak passwords using brute force attacks, inject compromised credentials to gain access to user accounts using credential stuffing attacks, or leverage a host of other strategies to hijack user accounts to steal personal or corporate data. Since 2013, the first Thursday in May has annually been marked as World Password Day. The goal of this day is to promote better cybersecurity hygiene by upgrading easy-to-guess passwords or refreshing older passwords that may have been compromised through some data breach. Think of it as the cyber equivalent of testing and replacing your home smoke detector batteries. Being diligent about creating strong passwords and updating them regularly is the first line of defense in securing both your personal and corporate information. Maintaining strong passwords and having a password strategy you can easily manage – but that others cannot easily guess – is an essential cybersecurity effort that every employee and individual plays a crucial part.

When it comes to password security, everyone has a role to play in the protection of PII and corporate data. IT teams and stakeholders should review the common risks of weak passwords with their organizations, as well as remind everyone of these best practices. This simple practice can help employees better protect their data while minimizing unintentional insider threats to the organization.

Learn about how Fortinet's Training Advancement Agenda (TAA) and NSE Training Institute programs, including the Certification Program, Security Academy Program and Veterans Program, are helping to solve the cyber skills gap and prepare the cybersecurity workforce of tomorrow.

National cyber security strategy of Republic of Macedonia (2018-2022), cyber capacities and cyber security culture are defined^{13,14}

Over the period 30 January – 1 February 2018, the following stakeholders participated in roundtable consultations: academia, civil society, criminal justice, law enforcement, the defense community, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, computer emergency response teams, information technology officers from the private sector (including telecommunications companies and financial institutions), as well as international partners. The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five dimensions of cybersecurity capacity:

- Cybersecurity Policy and Strategy
- Cyber Culture and Society
- Cybersecurity Education, Training and Skills
- Legal and Regulatory Frameworks
- Standards, Organizations, and Technologies

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors consist of aspects and for each aspect there are indicators, which describe steps and actions that, once observed, define the state of maturity of that aspect. There are five stages of maturity, ranging from the start-up stage to the dynamic stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM. Cybersecurity Education, Training and Skills and Cybersecurity Culture and Society.

Safety Tips for Social Networking

Social networking sites like Facebook and Twitter can be a great way to connect with friends. But there are some social networking safety tips you should always keep in mind.

- Manage your privacy settings. Learn about and use the privacy and security settings on your social networking sites. They help you control who sees what you post and manage your online experience in a positive way. You'll find some information about Facebook privacy settings at the bottom of this webpage.
- Remember: once posted, always posted. Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online.
- Build a positive online reputation. Recent research also found that recruiters respond to a strong, positive personal brand online. So, demonstrate your mastery of the environment and showcase your talents.
- Keep personal info personal. Be careful how much personal info you provide on social networking sites. The more information you post, the easier it may be for someone to use that information to steal your identity, access your data, or commit other crimes such as stalking.
- Protect your computer. Security start with protecting your computer. Install Antivirus software. Keep your operating system, web browser, and other software current. Visit Microsoft support for information on automatically installing the latest security updates for Office 365 and Windows.
- Know what action to take. If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.
- Use strong passwords. Make sure that your password is at least eight characters long and consists of some combination of letters, numbers, and special characters (for example, +, @, #, or \$).
- Be cautious on social networking sites. Even links that look they come from friends can sometimes contain harmful software or be part of a phishing attack. If you are at all suspicious, don't click it. Contact your friend to verify the validity of the link first.

Facebook Privacy Settings

Make sure you know how to access and use Facebook's privacy settings. Log in to Facebook, click the Settings menu.

- Select Privacy to view and edit who can see your photos, activity and information.
- Select Apps and Websites to control access to your Facebook account by applications and websites
- Select Blocking to block specific users or application invitations.

Social media security might not be the most exciting part of your social marketing strategy. But it could be the part that saves your business from a critical security breach or major business loss.

Whether you're a one-person shop or an organization with a large social team, you need to understand the best ways to mitigate the risks of social media so you can better focus on reaping the rewards¹⁵.

3. POLAND

Being active in digital media is an integral part of young people's lives, therefore, it is affected by the same processes that exist in the real world. It also includes issues related to behavior typical of adolescence risky, i.e., carrying the risk of negative consequences. Therefore, it's important to undertake preventive actions. In modern prophylaxis, regardless of the area, two general approaches can be distinguished: defensive and positive prevention. They differ diametrically in their approach to the problem of threats to children and young people, although in practice their use need not be mutually exclusive¹⁶.

"I Click Sensibly" — Digital Education in Poland

The Electronic Communications Office of Poland (UKE) is the regulatory body responsible for overseeing the Internet in Poland. It was known that very young children often use smartphones with little or no restrictions or guidelines. The regulator needed to know what kinds of things children were doing online and what risks there might be. It also had to find a way to educate children and parents on how to be safer online and how to understand and manage risk.

In response to these challenges, UKE introduced the **"I Click Sensibly"** educational campaign educates children and parents on how to be more protected online and how to recognize and manage risk. This has two elements. The first was a series of Internet Safety classes. During the specialized classes, trainers from the Office of Electronic Communications discussed how to surf online responsibly, what you should know when surfing online and how to use telecommunications devices safely. Children attending the workshops were also taught how to deal with cyberbullying or hate speech, how to deal with online aggression and how to protect their data. The sessions also taught parents how to filter inappropriate content and control how children spend their time online.

At the same time, UKE surveyed many of the children attending the classes to find out how they use the internet and what risks and harms they may be exposed to. The surveys were conducted using computer-assisted personal interviewing. More than 50,000 children benefited directly from the classes.

Using the survey, UKE was also able to gather detailed data on how children spent their time online, what risks they were exposed to and how well their parents were prepared to support them. At a time when many national and international agencies do not even have data on children's online lives, UKE has detailed statistics on topics such as what percentage of children have been teased or bullied online, how well children are able to judge the accuracy of information, they find online, and how much control parents exercise over what their children do and see online.

The DBAM O MÓJZ@SIĘG Foundation¹⁷ contributes to the responsible use of new communication tools. The basis for action is a professional diagnosis of the problem, interaction in intersectoral cooperation, as well as the idea of participation as a means of including support for those who need it. *"Nobody's Children" Foundation* conducts the following social campaigns:

- ***"Protect Your Child from the Internet"***, which began on February 7, 2017, aims to educate parents of preschool and toddler-age children about harmful content on the Web, as well as their responsibility to keep children safe on the Internet. This action provides parents with information about specific policies and tools that will reduce children's risk from inappropriate online content.
- The ***"Add a Friend"*** campaign was created to make young people aware of the negative consequences of the attack and to encourage them to stand up against inappropriate behavior online. The campaigns are a response to this serious and constantly underestimated problem affecting young people on the Internet.
- ***"Stop the cyberbullying campaign"*** fights against violence. The main aim of the action is to draw attention to the problem of violence between peers using electronic media and to educate children and adolescents who play pranks on electronic media. This can lead to serious consequences for both the victims and the perpetrators of such activities related to school life.

"Child on-line" campaign

An important part of this campaign, in addition to media activities, is the wide range of educational materials offered. It was prepared by the Nobody's Children Foundation and is aimed at children, adolescents, their parents and professionals. In this campaign, an innovative course called "Child Online" was created. It shows various aspects of child sexual abuse on the Internet and other forms of threat to young Internet users (www.dzieckowsieci.pl). The current version of the campaign, titled "Protect Your Child Online," is aimed at protecting children from harmful Internet content.

Measures taken about cyber safety in Poland include several different approaches¹⁸:

Defensive prevention, in other words elimination, is to reduce risk factors and in the context of the network may include the following actions:

- installation of filtering programs,
- prohibition of use from telephones and the Internet at school,
- controlling the time spent on the network and
- activities undertaken by the child/youth, adapting games and applications to the age of minors.

Positive prevention, focused on strengthening protective factors is based on the promotion of constructive use of the web. Preventive actions for safety online in the school environment include **recognition** - based on available research or by conducting own research in the area of online functioning among children and adolescents. It would be good if adults (both parents and teachers) systematically initiate discussions with youth. In that way showing interest in their world, activities conducted on the web, as well as observed trends. Conversation with the youngest Internet users will allow adults to gain interesting observations. It is very important to give young people space for conversation, reflection and building an atmosphere based on trust, encouraging people to share their experiences. The barrier in seeking help from adults is the fear of criticism and punishment (e.g., picking up the phone/laptop

and limiting internet access). An essential element of effective preventive actions is the development of teaching and pedagogical staff competence in the field of methods and how young people use the Internet.

The security of children on the internet and social media is a critical concern for parents, guardians, educators, and society as a whole. Here are some key considerations and tips for enhancing children's safety online¹⁹:

Counteracting cyberbullying: Cyberbullying is a serious issue that can have detrimental effects on individuals' mental and emotional well-being. Counteracting cyberbullying requires a multi-faceted approach involving individuals, communities, and technology. Here are some strategies to help combat cyberbullying:

- **Education and Awareness:** Promote education and awareness campaigns to inform people about cyberbullying, its impact, and how to prevent it. This can be done in schools, workplaces, and community organizations to ensure that everyone understands the consequences and knows how to respond appropriately;
- **Create Safe Online Environments:** Online platforms should have strong community guidelines and enforce strict policies against cyberbullying. Encourage platforms to invest in advanced technologies, such as AI-based content moderation systems, to detect and remove cyberbullying content promptly;
- **Encourage Responsible Digital Citizenship:** Teach individuals about responsible online behavior, empathy, and respect for others. Promote positive online interactions and discourage any form of harassment or bullying. Encourage users to report cyberbullying incidents and provide them with the necessary tools and resources to do so;
- **Support Systems:** Establish support systems within schools, workplaces, and communities to help victims of cyberbullying. Provide counseling services, helplines, or online support groups where individuals can seek

guidance and share their experiences in a safe and supportive environment;

- ***Encourage Open Communication:*** Encourage victims of cyberbullying to talk to a trusted adult or authority figure about their experiences. Provide a safe space for individuals to discuss their concerns, seek advice, and report incidents without fear of retaliation;
- ***Collaboration with Law Enforcement:*** Work closely with law enforcement agencies to address severe cases of cyberbullying that involve threats, harassment, or illegal activities. Encourage victims and witnesses to report such incidents to the appropriate authorities;
- ***Parental Involvement:*** Educate parents about cyberbullying and help them understand the importance of monitoring their children's online activities. Encourage open communication between parents and children to foster a supportive environment where children feel comfortable sharing their online experiences;
- ***Positive Reinforcement:*** Recognize and celebrate positive online behavior. Highlight and reward individuals or groups who promote kindness, inclusivity, and respect in online interactions. This can help create a culture where positive behavior is encouraged, and cyberbullying is discouraged.

Counteracting harmful content: Counteracting dangerous content on the internet and social media platforms requires a multi-faceted approach involving various stakeholders, including platform operators, government entities, and individual users. Here are some strategies that can be employed:

- we should equip the computer with a filtering program;
- we should set technical parent control - use parental settings on the computer to make sure the child's personal information is only seen by people they want to share it with or to control the child's gaming;

- we should explain to children that information published on the Internet may be untrue and false.

Counteracting sexting: Counteracting sexting involves taking proactive measures to educate individuals about the potential risks and consequences associated with engaging in such activities. Here are some strategies and actions that can help address the issue:

- Schools and educational institutions should incorporate comprehensive sex education programs that cover topics like healthy relationships, consent, online safety, and the risks of sexting;
- Schools should offer workshops and seminars to parents, teachers, and students to raise awareness about the consequences of sexting and provide guidance on how to handle such situations;
- We should inform individuals about the legal implications of sexting, particularly for minors. Emphasize that sharing explicit images of minors can result in child pornography charges, even if the image was self-produced;
- We should encourage individuals to regularly review and update their privacy settings on social media platforms to control who can access their content;
- We should educate individuals about the importance of being an active bystander and intervening if they witness or receive unsolicited explicit images;
- We should encourage reporting of inappropriate behavior and provide resources for individuals who need support;
- We should ensure that individuals who have been affected by sexting incidents have access to appropriate mental health support services, such as counselling or therapy.

Counteracting Internet addiction: Counteracting youth internet overdose is especially important given the significant role the internet plays in the lives of young people today. Here are some strategies that adults should undertake to help address this issue:

- **Establish clear guidelines and limits:** Set clear rules and expectations regarding internet use for the children. Define specific time limits for daily internet usage and establish boundaries for what types of online activities are allowed;
- **Encourage offline activities:** Promote and support a variety of offline activities that engage your children's interests and hobbies. Encourage them to participate in sports, arts and crafts, reading, playing musical instruments, or any other offline activities that they enjoy;
- **Foster face-to-face interactions:** Encourage your children to have face-to-face interactions with their peers, friends, and family members. Encourage activities that involve socializing, such as playdates, joining clubs or organizations, and participating in community events;
- **Promote outdoor and physical activities:** Encourage the children to spend time outdoors and engage in physical activities. Encourage sports, going for walks, bike rides, or engaging in other physical activities that keep them active and help them disconnect from online distractions;
- **Teach responsible internet usage:** Educate your children about responsible internet usage. Teach them about online safety, the importance of privacy, and the potential risks and consequences of excessive internet use. Help them develop critical thinking skills to navigate online content and distinguish between reliable and unreliable sources;
- **Lead by example:** Be a positive role model by practicing healthy internet habits yourself. Demonstrate responsible internet use and limit your own screen time. Encourage family activities that involve

minimal or no internet usage, such as board games, outings, or shared hobbies;

- Create tech-free zones and times: Designate specific areas or times in your home as tech-free zones or times. For example, make bedrooms or mealtimes technology-free areas to encourage face-to-face communication and family bonding;
- Stay involved and communicate: Maintain open and regular communication with your children regarding their online activities. Be interested in what they do online and create an environment where they feel comfortable discussing their online experiences and concerns with you;
- Utilize parental controls and monitoring tools: Use parental control software and monitoring tools to help manage and restrict your children's internet access. These tools can block inappropriate content, set time limits, and track their online activities;
- Encourage a balanced lifestyle: Emphasize the importance of balance in life by encouraging your children to engage in a variety of activities. Encourage them to pursue their passions, explore new interests, and maintain a healthy balance between online and offline activities;
- By implementing these strategies, you can help youth develop healthy internet habits, strike a balance in their lives, and minimize the risk of internet overdose.

Existing knowledge on effective protection against threats indicates the huge role of family, the climate of young people's emotional life in relationships families, as well as in the school and peer environment. Among the defined factors risks and protections that may result in increased or decreased vulnerability risky behaviors, three basic areas are listed: bond with loved ones, interest in school education and relations with the environment peer.

4. AUSTRIA

There are various modern methods of risk prevention in social networks in Austria, which are offered by various organizations and initiatives. Some of these methods are:

Parent education

Imparting knowledge and skills to parents can help them better guide their children in using social networks and the Internet. Parent education programs such as "Saferinternet.at Elternabende" are offered throughout Austria. Which modern methods of risk prevention in social networks in Austria are there for parents within the framework of parent education? Various modern methods of risk prevention are offered in social networks as part of parent education in Austria. Some of these methods are:

- **Parents' evenings:** Initiatives such as "Saferinternet.at" offer parents' evenings where parents receive information and tips on safe Internet use for their children. Topics such as cyberbullying, sexting, data protection and social media use are dealt with;
- **Workshops:** Workshops are also offered in which parents are given concrete options for dealing with risks on the Internet. Here parents learn, for example, how to talk to their children about dangers on the Internet or which settings are important in social networks;
- **Online advice:** Various online advice provided by initiatives such as "Saferinternet.at" can help parents find out about the risks in social networks and receive specific recommendations for action²⁰;
- **Parent apps:** There are also dedicated apps that help parents guide their children using social networks and avoid risks. One example is the "Children's App" from "Saferinternet.at", which helps parents to keep an eye on their children's Internet use and to make age-appropriate filter settings. Other apps are^{21,22, 23}:
 - **"Famisafe":** This app offers features such as location tracking, device usage time limit and internet access filtering. Parents can also use it to keep track of what apps their kids are using and for how long;
 - **"Qustodio":** This app offers features such as screen time management, web content filtering, and social media activity monitoring;

- **"Net Nanny"**: This app allows parents to block web content, set time limits for device usage and monitor their children's social media activities²⁴;
- **"SaferKid"**: This app offers features such as real-time location, web content filtering, monitoring of social media activity and alerts for suspicious activity²⁵;
- **"OurPact"**: This app allows parents to set time limits for device usage, filter web content and control app usage. Our Pact is a Parental Control App & Family Locator for iPhone and Android.

It is important to note that parenting apps are only one part of a comprehensive online safety education, and they cannot eliminate all risks. Parents should include their children in conversations about online risks and codes of conduct and maintain open and trusting communication.

Teacher training

Teachers play an important role in teaching media literacy to young people. Training courses for teachers can help them better guide their students in using social networks and help them identify and avoid risks. What modern methods of risk prevention in social networks are there for teachers in Austria as part of teacher training? In Austria there are various offers for teachers that are intended to help support their students in the area of media competence. Some of these offers are:

- **"Saferinternet.at"**: The Austrian initiative offers training and further education for teachers to support them in teaching media skills to their students. The offer includes workshops, webinars and teaching materials²⁶;
- **"Media education in schools"**: This initiative of the Federal Ministry of Education, Science and Research offers teachers in Austria further training and workshops to strengthen their media skills and to help them to support their students in dealing with digital media²⁷;

- **"Austrian youth media protection"**: The facility offers training and further education for teachers to support them in teaching media skills and protecting children and young people from online risks²⁸;
- **"Klicksafe.de"**: The platform offers teachers teaching materials, training and further education to support them in teaching media skills to their students²⁹;
- **"Eltern-Medien-Beratung"**: The initiative offers training and further education for teachers to support them in teaching media skills to parents. This enables teachers to respond better to the needs and questions of parents and help them to support their children in dealing with digital media³⁰.

These offers are only part of the possibilities that teachers in Austria have to further educate themselves in the field of media competence. Teachers can also use online resources independently and find out about current developments in the field of media education in order to better support their students.

Online tools and platforms

Various online tools and platforms can help young people to be safer online and on social media. For example, the Saferinternet.at initiative offers an online platform that helps children and young people to become safe on the Internet. Which modern methods of risk prevention in social networks are there for young people in Austria? There are various online tools and platforms designed to help young people be safer online and on social media. Some examples are:

- **Saferinternet.at**: The Austrian initiative Saferinternet.at offers various online tools and platforms to sensitize children and young people to use the internet safely. These include an online lexicon with terms relating to the use of the internet and social media, as well as a quiz that informs users about various risks on the internet;
- **Klicksafe.de**: Klicksafe.de is an initiative of the European Union that advocates more media competence and safer use of the internet. The

website offers various online tools and platforms for children, young people, parents and teachers, such as games, worksheets and guides³¹;

- **Bee secure:** Bee secure is an initiative of the Luxembourg state that is committed to more security on the Internet. The website has various online tools and platforms for children, young people, parents and teachers, such as educational games, worksheets and guides³²;
- **Internet-ABC:** The Internet-ABC is a service provided by public broadcasting in Germany that supports children, parents and teachers in using the Internet safely and competently. The website offers various online tools and platforms, such as learning modules, games and a parenting ABC³³;
- **Jugendserver.at:** The Jugendserver.at is an online portal for young people. Viennese youth organizations and youth projects can register a free subdomain on jugendserver.at and get free web space to implement your own web idea³⁴;
- **Internet Ombudsman:** The Internet Ombudsman is an independent complaints office in Austria that deals with problems relating to Internet use. The website has various online tools and platforms, such as a glossary of internet terms and a database of judgments and decisions. (Internet Ombudsstelle - Kostenlose Schlichtung und Hilfe bei Problemen im Internet).

Initiatives to increase media competence in Austria

In all federal states in Austria there are various offers and initiatives to promote media competence and to prevent risks in social networks. Here are some examples:

- *Upper Austria:* The media center of the state of Upper Austria offers further training for teachers on the subject of media competence. The "Medienfit 2000" project is also committed to promoting media skills among children and young people³⁵;
- *Vienna:* In Vienna there is the project "Sicheres Netz hilft" which helps parents and children to surf the Internet safely and how to deal with

situations like online dating, password creation, etc³⁶. The "Digital Imagination" initiative is also committed to promoting media skills among children and young people³⁷;

- *Tyrol*: The state of Tyrol offers teachers further training on the subject of "Sicher im Netz"³⁸;
- *Salzburg*: The Medien: Werkstatt: Medienbildung und – Kompetenz in Salzburg offers workshops to promote media competence for young people in order to be able to deal critically with the media on the internet. This is funded by the city and state of Salzburg³⁹;
- *Styria*: The project "Digital? Sicher!"/" Digital? Safe!" developed and evaluated a playful learning app for cyber security and data handling awareness training for young people in the 9th to 13th grade. A playful approach (serious gaming) and case studies from the Styrian economy are intended to increase the attractiveness of the training⁴⁰;
- *Carinthia*: On the initiative of the women's department and the anti-discrimination agency of the state of Carinthia, experts and those affected have been providing information on the topic of digital conversation culture as well as dangers and consequences on the Internet since June 2019 as part of the "#Hass im Netz" series of events throughout Carinthia⁴¹.

Peer to peer counselling

Peer-to-peer counselling, in which young people help other young people to cope with problems, can help them feel more secure and better prepared to face risks.

In the "**DigiPros**" project, nominated students expand their knowledge of digital media, develop projects and campaigns at school and thus become digital experts. Through the knowledge they acquire about social media, apps, the Internet, traps on the net, etc. they can skilfully pass on the right interaction to their friends in the sense of the peer idea. The aim of the workshop is to strengthen the digital competence of young people and at the same time to let the participants become contact persons (DigiPros) in their circle of friends.

Together with participating teachers, media education projects, campaigns, etc. are developed and implemented at the school⁴².

In the **#makeITsafe2.0** project, young people and adult caregivers not only deal with how to move and behave safely online, but also how to prevent violence. On four workshop days, the young people are trained by the IT School in a group to become “peer experts” and develop a “toolbox” that they will need later when they pass on the knowledge they have learned to other children and young people. Adults who relate to the “peer experts” act as “role models” and support the young people in implementing activities. You will be brought in on one day and also trained. The aim is to pass on the knowledge gained in the project to as many young people as possible so that they too can use digital media safely⁴³.

Cooperation with social networks

Through cooperation with social networks, joint measures to protect children and young people from risks can be developed. For example, Saferinternet.at cooperates with Facebook and Instagram. In Austria, in addition to the cooperation between Saferinternet.at and Facebook/Instagram, there are other cooperations with various social networks and platforms. One example is the cooperation between the TikTok platform and the "Gemeinsam Sicherheit im Netz" initiative of the Austrian Federal Ministry of the Interior. The aim of this cooperation is to educate young users about the responsible handling of personal data and the prevention of cyberbullying. (GEMEINSAM.SICHER im Internet (markthartmannsdorf.at)) The Federal Chancellery also cooperates with various social networks, including Facebook, Instagram and Snapchat, to promote the implementation of child and youth protection measures on these platforms. These methods can help ensure that children and young people in Austria are safer on the Internet and in social networks. However, it is important that parents, teachers and young people themselves are active and informed themselves about the risks.

Best practice examples

There are several best practice examples of modern risk prevention methods in social networks in Austria. Here are some examples:

- ***“Antenne macht Schule/virtuell”/ “Antenna makes school| virtual”⁴⁴***
is free and can be flexibly adapted to the school hours of the class. In combination with “#Hass im Netz” the format is recommended from the age of 10. In the project ‘Antenna Makes School | Virtually, students can look behind the scenes of the antenna and learn how radio is made! The concept offers great added value for both school children and teachers. Children and young people deal with current topics and can make a lasting contribution by illuminating #hate on the internet.”
- ***Media literacy award:*** The media literacy award [mla] is an international competition that is advertised annually. It is aimed at teachers and students who, as part of the school want to implement media education projects in order to improve their ability to read media texts and create, expand. Schools from all over Europe can take part. Since the 2001/02 school year, under the motto “Media competence is identical to the ability to think critically” (Joseph Weizenbaum) Best practice projects with the [mla] excellent. Up to 500 media projects are submitted each year, around 90 percent each from Austria. The competition initiated by the Austrian Ministry of Education is one of the most important media competence initiatives in Europe and promotes creative and critical interaction with all kinds of media⁴⁵.
- ***“Aktiv gegen Cyber-Mobbing”/ Active against cyber - bullying*** at the VS Liezen - use the internet and smartphone safely. 61 children from the 4th grade of elementary school and parents of all grades had the opportunity to find out about the possibilities of the new media, i.e., mobile phones and the Internet. Topics such as cost traps through games (and how to avoid these costs), dangers in virtual space (including the Whatsapp groups), the initiation of sexual contacts on

the Internet and much more. were treated. In the morning for children and in the evening at parents' evening for parents⁴⁶.

- **"Medienkompetenz macht Schule (media literacy makes school)":** A project of the Austrian Federal Ministry of Education, Science and Research that supports schools in promoting media literacy and educating schoolchildren about the risks of the online world.
- **"klicksafe.at":** An Austrian initiative that provides online materials and tools to educate parents, teachers and young people about the risks and challenges of the online world.

These examples show that there are a large number of initiatives and organizations in Austria that are committed to promoting online safety and media skills among young people.

Saferinternet.at

Saferinternet.at is an information and coordination center for safer internet use and media literacy in Austria. Saferinternet.at supports internet users, with a special focus on children, young people, parents and educators, for safer use of digital media. The rich portfolio of ongoing activities includes the website www.saferinternet.at, free school resources and brochures, seminars and helplines throughout Austria, as well as networking with relevant users and as a contact point for journalists. The topics of the prevention of violence and addictions are summarized in the general concept "**UNDER 18**" and are divided into the programs "Everything is fine - everything is fine!", "Click and check" and "Look@your.life". Each of these programs meets criteria essential for proper implementation and sustainability. The Click & Check violence prevention program is concerned with promoting the responsible use of digital media. In addition, special attention is paid to preventive legal information, particularly with youth protection provisions, since young people in their most diverse life worlds encounter different legal provisions.

B. WORLDWIDE

In 2019, more than half of the world's population used the Internet (53.6%) with approximately 4.1 billion users. Globally, one in three Internet users is a child under the age of 18. In some lower income countries this rises to about one in two, while in higher income countries the ratio is about one in five. According to UNICEF, globally 71% of young people are already online⁴⁷. This is why children and young people are now significantly and constantly present on the Internet. Among children and young people, the most popular device for accessing the Internet is the mobile phone, followed by desktop computers and laptops. Children and young people spend an average of about two hours a day online during the week and roughly double that every weekend day. Some feel permanently connected. But many others still don't have access to the Internet at home. In practice, most children and young people who use the Internet access it through more than one device: Children and young people who connect at least weekly sometimes use up to three different devices to do so. The most popular pastime – for both girls and boys – is watching videos. Many children and young people can be considered "active socializers" using several social media platforms such as Facebook, Twitter, TikTok or Instagram. Many initiatives worldwide are designed to overcome the problems, caused by online risks that young people face on social media. Here in this chapter are presented best practices in different countries that produce positive result for youth around the world.

EUROPE

COUNCIL OF EUROPE — LANZAROTE CONVENTION⁴⁸

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Violence (Lanzarote Convention) requires states to propose a comprehensive response to sexual violence against children through the "4ps" approach: Prevention, Protection, Prosecution and Promotion pursuing and promoting national and international cooperation. The operation of the Convention in relation to the digital environment was clarified by the Committee of the Parties to the Convention on the Protection of Children against

Sexual Exploitation and Sexual Abuse (the "Lanzarote Committee") through the adoption of a number of documents. These are: opinion on sexual or explicit images and/or video material generated, shared and received by children (June 6, 2019); interpretative opinion on the applicability of the Lanzarote Convention to ICT-facilitated sexual offenses against children (12 May 2017); statement on Internet addresses of material or images containing sexual abuse of children or other offenses established in accordance with the Lanzarote Convention (16 June 2016) and opinion on Article 23 of the Lanzarote Convention - solicitation of children for sexual purposes through information and communication technologies (befriending children for the purpose of sexual abuse).

PROGRAM OF THE EUROPEAN UNION T.A.B.B.Y. (THREAT ASSESSMENT OF BULLYING BEHAVIOR IN YOUTH)⁴⁹

It addresses the negative challenges faced by teachers, school counsellors, instructors, principals, parents, and students related to youth use of digital media, the Internet, and mobile phones and other interactive devices: primarily cyberbullying, cyberbullying, and sexting. The project aims to increase the knowledge, skills to protect young people when using the Internet, mobile devices, social networks, school, but also outside the campus from victimization by peers or other youth or adults by creating a system for school officials and themselves students to identify risk factors and assess cyberbullying, cyberbullying, and sexting and take adequate preventive actions to protect themselves and victims from such harmful behavior. They created a game and some guidelines.

ALBANIA

SAFER AND BETTER INTERNET FOR CHILDREN AND YOUTH IN ALBANIA (FUNDED BY THE END VIOLENCE FUND)⁵⁰

Albania's '.al' internet domain is often featured as one of CSAM's top hosts. Although Albania has ratified all major international legislation related to CSAM, between 2016-2018 only 12 alleged cases of child abuse were identified by the police and only one potential perpetrator was found. The analysis showed that

an unclear and poorly developed legal framework regarding the protection of children from online harm contributes to low disclosure rates. The relevant international conventions are not codified in criminal law and as such international law cannot be accessed or used.

The 2017 Albanian Law on the Rights and Protection of the Child was drafted with the direct technical support of UNICEF. It enshrines the principle of protecting children from all forms of abuse, harm and exploitation (offline and online) and therefore obliges the government to implement it. UNICEF then created a robust partnership platform for all key government institutions, civil society groups, private sector representatives and children themselves to consult and discuss specific procedural provisions to protect children from online harm. Working with a range of public and private stakeholders, the partnership platform produced a final draft of secondary legislation developing the implementation of the protection of children from online harm, which was drafted within six months and successfully presented to the Council of Ministers for adoption.

In July 2019, the Albanian Council of Ministers approved the key decision (by-law) on "Measures to protect children from harmful and illegal materials online". This introduces for the first time a clear legal provision and institutional responsibilities to protect children from harmful and illegal content online. It also sets out procedures for the immediate removal of harmful and illegal content from the Internet, as well as reporting and referral pathways for online child abuse, harassment and sexual exploitation. The impact of this large-scale result will positively affect almost all children in Albania.

BELGIUM

RE: PEST: A game designed to reduce bullying behavior⁵¹. In this game, children learn different ways to respond to bullying. The University College West Flanders (HoWest) has developed a lesson kit against bullying called "Re: pest", with a 3D game for students in the first two years of secondary school. Via the simulation

game, students can experience what it's like to be in the shoes of bullies, bullied students and onlookers. They are encouraged to reflect on their own behavior and choices. The idea for the game derives from a Finnish project. According to Flemish education minister Pascal Smet, bullying in Finnish schools was reduced by 40% after the launch of the game. The kit also includes background knowledge and lesson suggestions for teachers and an info brochure for parents. The project was commissioned by the city of Kortrijk and co-funded by the government of Flanders.

CZECH REPUBLIC

INTERNSHIP OF RATOLEST BRNO ON "TRUTH OR LIE ONLINE"

„Truth or Lie Online” is a methodological approach, designed to help participants realize that the content they encounter online may not always be true. The practice teaches participants the principles of evaluating this content and provides guidance on why fake content is created. An additional partial goal is to show participants how they present themselves online (especially on social media) and what information they share, and that there may be consequences for this and what those consequences may be. The practice also highlights the risks that anonymity poses in online spaces and what precautions are needed when dealing with anonymity. The target audience of this practice is adolescents and young people in general, especially those who use social networks. The audience best engaged in this practice are young people with low levels of media literacy or who are unaware of the risks that social networks and anonymity pose online. Collectively, this practice consists of several separate activities. If necessary, however, they can be conducted independently. The individual activities are composed of two main categories: “Identifying what is (un)true” and “Creating false content”.

“Identifying what is (un)true”

Photos

In this activity, participants look at images that show unusual things. Some images are fake (for example, altered by graphics editing software), while others

are real. Participants then have to decide whether the image is fake or real. This can be done individually or in groups, although the argument is critical to the success of the activity. This activity is accompanied by a discussion on how to distinguish fake images from real ones. It is essential to note and discuss the different degrees of falsification that can be applied to images. Corrections can be made in many different and very complex ways, meaning that discerning what is real and what is fake can often be difficult, if not impossible, without the help of technology. Emphasizing the need for this aspect is extremely important when analyzing or examining certain media materials.

Text

In the same way that the question of the authenticity of the images is addressed in the previous activity, this activity involves showing the participants several texts, some of which are authentic and some of which present false or modified information. Ideally, the prepared texts should be interesting for the participants, both in content and in form. The texts should reflect an appropriate level of difficulty for the age range of the participants. The participants then have to decide together which texts they think are real and which are fictional. During this part of the activity, it is important to problematize the fact that it is possible to encounter modified (unrealistic) pictures and texts, especially on the Internet. Discussion on these topics must also address why participants believe such texts were created in the first place. An example can be given of the efforts of an established media with a particular agenda. This may include generating more income, attempting to defame or build a positive image of a politician, attempting to promote a particular opinion or political position, or misleading their viewers for political gain. If participants have their own experiences with modified or misleading media content - particularly on the internet and social networks - it is recommended that they be encouraged to share these with the group (provided they are comfortable doing so).

Resources for Identifying Fake Content (optional activity)

If this particular topic is of particular interest to participants, it is recommended that they become familiar with websites that collect the most known false

reports and discuss their veracity. Participants can review and use them to evaluate and confirm or refute the veracity of messages they find on the Internet.

“Creating fake content”

In this activity, participants will try to create their own fake copy to show them how difficult or easy it is to fake something convincingly enough for others to perceive it as true. They will also learn what purposes the creation of fake content serves and what impact their fake product has on others.

Photo

In the first phase, participants will be asked to take a number of photos of themselves - in various forms. On average, four photos are enough. One of the photographs will capture the 'true form' of the participants, e.g. unedited photo without any modifications. Other photos will be modified by participants according to their own imagination to make them look as good or extraordinary as they want. Any available graphics editing program can be used. When piloting this approach, Ratolest Brno chose to use the Snapchat mobile app and its filters because his customers were familiar with the app and it was user-friendly. The app allows users to easily retouch their face, adjust their eyes, nose or mouth and add other features to the photo like hearts, dog ears and more. The resulting photo may be very far from the actual appearance of the object. Once participants have edited their photos and downloaded them from the app, they can be transferred to a computer by whatever means is most convenient. The entire group then reviews and evaluates the photos—both the modified and the original—together. They can choose which photo or photos they like best and which they would prefer to feature on social media. Each participant then prints the photo they chose.

Facebook profile

Each participant is provided with a blank sheet of paper on which to present their Facebook profile. They can start by attaching their photo to it and then create and fill in a sheet of paper with their own content. Participants can create the

entire content for their profiles to get the highest return. The benefits and negatives can be drawn from this experience. During the activity, moderators can ask participants to share their thoughts on how they can make the profile engaging with others. They'll probably talk about what it's like to create a fake profile; some of them can share if they have had previous experience with this. This can devolve into discussions about the creator's attention to detail or the credible impression the profile makes on others. As the activity progresses, participants can like or comment on each other's profiles via sticky notes. This gives participants the opportunity to experience others reacting publicly to the content they create. This phase should only be included if the participants are able to accept other people's opinions, especially contradictory or negative ones. If the participants can handle the conflict, the moderator (there may be more than one) can introduce a "hater" role. The hater is responsible for the hate and negative reactions to the profiles. This can be manifested by providing negative or insulting comments, usually directed at the person themselves. After the hater reacts to several profiles, members of the group can discuss how they felt after receiving such negative comments or seeing how others received them. Participants could also share their own experiences with haters on social networking sites if they wished and felt comfortable doing so. Emphasis can be placed on the fact that fictitious content can have consequences for both the creator and the user.

FINLAND

OTANVASTUUN.FI – “I TAKE RESPONSIBILITY”⁵²

A self-help program for adolescents and adults who are concerned about their sexual interest in children. The program was created in January 2018 and can be used anonymously and for free⁵³.

HELP.SOME

A mobile app launched in 2016 that provides information and advice to children and young people about their concerns and issues. The app offers reliable

information and support from trained professionals and volunteers. It allows users to get help for things like harassment, issues related to sexual harassment and abuse, and other criminal acts. The discussions are held by experts from Save the Children, Helsinki Virtual Police and Victim Support Finland.

GERMANY

ALWAYS ONLINE-NEVER ALONE AGAIN? PREVENTION OF DIGITAL STRESS IN A SCHOOL ENVIRONMENT, DIGI CAMPS AND TEACHERS DIGI CAMPS IN SCHOOLS, BARMER, GERMANY

'Always online - never alone again?' is a digital stress prevention project. It aims to promote media literacy among young people, who are often left alone in the digital world, and to strengthen the conscious use of digital media.

The project is intended for two target groups: students and teachers. In relation to digital media, students should:

- Learn to use them wisely.
- Recognize opportunities and learn to use them positively.
- Know the risks and dangers, especially regarding their own (mental) health.
- To find and adopt the balance between healthy eating, measures to deal with digital stress and regular physical exercises.

Teachers should:

- Raise awareness about healthy lifestyles - coping with digital stress, nutrition, exercise - in a digital world.
- Get incentives to integrate digital media into everyday school life in a health-friendly way.
- Among other things, be able to act as multipliers to prevent digital stress in schools - e.g., in terms of improving health in the area of coping with stress.

Among other things, parents are informed about children's media use and preventive measures in education through parent-teacher discussion.

Digital health and the prevention of digital stress are the focus of the prevention project "Always online - never alone again?". Digital media has become an integral part of young people's lives, but it can also be burdensome. As part of the project "Always online - never alone again?", students and teachers deal with the risks and opportunities of digital media in workshops and training courses, for a healthy lifestyle in harmony with the digital world. The main idea is to strengthen media literacy in order to promote the conscious and healthy use of digital media. At the same time, the content of the project also aims to bring participants closer to a balance between healthy eating, digital stress management measures and regular physical exercise in relation to the use of digital media.

The prevention project starts in the school environment and takes into account all participants - the students' parents are also involved in the project. The project offers the following approaches:

Pedagogical approach

DIGI CAMPS project module: In three-day workshops on site at school, students and teachers deal with the opportunities and risks of the digital world. Lecturers and speakers impart knowledge and develop practical content together with participants. For example, YouTube stars and influencers introduce participants to techniques for the proper use of the Internet. Because: If you know the mistakes made, you can better pay attention to the balanced level of consumption and disclosure of information - and use the advantages for yourself. DIGI CAMPS addresses key areas such as YouTube, Instagram, blogging, journalism in the digital age, and more. Students also offer their own contributions, for example YouTube videos, Instagram photos, blogs or journalistic formats.

Content:

- How do platforms like Snapchat, Instagram and the like work? How to optimize my online profile?
- How do I know if someone is addicted to social media?
- What can I do against digital stress?
- How to become a YouTube star or blogger?
- How to edit videos and photos?

The project module TEACHERS DIGI CAMPS

In one-day training courses, teachers receive valuable tips on digital health, media prevention and modern teaching. In a combination of lectures by specialized lecturers and interactive seminars with teachers from the media practice, all questions related to the lessons are discussed. Topics such as digital stress prevention, cyberbullying, data protection and security (DSGVO) and digital teaching and learning are covered. From a preventive and health-promoting perspective, the aim is, among other things, to achieve an understanding of healthy lifestyles in harmony with the influences that the digital world brings with it, and to convey this to students and, if applicable, to their parents.

Content: On five didactically prepared cards, teachers will find different ideas and suggestions for their lessons. The topics are:

- The use of the smartphone
- Social networks as a detonator for stress
- Physical exercises against tension
- The right nutrition for better concentration

The content of DIGI CAMPS aims to provide participants with a balanced and healthy lifestyle in relation to the use of digital media. Participating schools should lead by example on the topics of media literacy and promoting stress coping skills. The presented prevention project offers a broad approach to promoting media literacy and healthy living, as well as reducing digital stress, for students and teachers⁵⁴.

VERKLIKT!⁵⁵

Verklickt! is a 50-minute feature film aimed at children and young people aged 12 and over and designed to teach them about safety and security in their digital everyday lives. An educational booklet is included in the media package for teachers and educators. It focuses on cyberbullying, illegal downloads, cost traps, personality rights and copyright. Additional topics include e.g. social media behaviour, content that is harmful to young people and password security.

ProPK issued a brochure for victims entitled "Opfer, Schlampe, Hurensohn - gegen Mobbing"⁵⁶. This booklet, designed like a comic book, shows how cyberbullying takes shape. It explains the features included in smartphones and shows how mobile devices connected to social networks can be used as a tool for cyberbullying. However, his main message is that bullying should not be tolerated. Victims of cyberbullying can and should seek help from third parties. The brochure is aimed at children and adolescents. ProPK has also developed a child-friendly comic titled 'Hallo – jetzt reicht's', which addresses children's experiences of violence, bullying, blackmail, property damage and internet chat and teaches children how to behave in these situations. The comic is aimed at children of primary school age.

THE PROGRAM “MEDIENHELDEN”⁵⁷ (Media Heroes”) is a universal, modulated, theoretically based and carefully evaluated preventive intervention for use in schools (7th to 9th grade students). The aims of the program include: preventing cyberbullying/victimisation and teaching children and young people to protect themselves online. "Medienhelden" aims to change attitudes and beliefs through knowledge transfer by providing students with definitions, teaching them the legal implications of cyberbullying, providing information on how cyberbullying affects the victim and promoting empathy for victims of cyberbullying.

ITALY

Connected Generations – Center for Safe Internet, Italy⁵⁸

Generazioni Connesse (Connected Generations) is a project funded by the European Commission within the framework of the "Connecting Europe Facility - CEF". The overall goal is to develop services with innovative content and higher quality. The aim is to increase the media literacy of young people who use the Internet. At the same time, it is an investment in the social and economic growth of the entire community. "Generazioni Connesse" consists of a platform with easy-to-understand and attractively designed educational material. In general, the platform is accessible, but it is intended for the target group of the school and especially for teachers. The site deals with topics such as:

- Learning to identify and resist online temptations
- Cyberbullying
- Online addiction: learning to recognize and deal with addictive online conditions
- "No to hate speech", also online to learn to be respectful
- Online child pornography, the legal framework and how to intervene
- "Privacy", data protection in school, the new European data protection regulation
- Online relationships: when virtual relationships replace real relationships
- Sexting: what students need to know about it
- Conscious use of the Internet: to learn safe and conscious use.

The part specially prepared for teenagers contains:

- Online temptations: what to do to avoid falling into a trap?
- How can I help my friends with Internet problems
- Recognize inappropriate content and manage it properly
- Cyberbullying
- Online addiction: how much is too much?
- Online Etiquette, Internet Friends and Feelings: The Ten Rules for Living Your Best Online Life.
- Sexting, a dangerous game.

For parents, the site provides information on these topics:

- Online temptations - how to help my children cope with them.
- Communicate with your children: advice to improve dialogue.
- Inappropriate content: how to recognize it and how to report it.
- Cyberbullying, what it is and how to learn to recognize and deal with it.
- Addiction to video games and online gambling, how to recognize them and how to deal with them.
- Net addiction, are my kids spending too much time online?
- Gambling, explaining to children the risks of online gambling.
- Privacy, how you can respect your children's right to privacy.
- Data sharing and protection.
- Malware and phishing, how to recognize them and avoid the associated risks.
- Parental controls: protection for your children, what you need and how e.g. security software can be activated.
- Online child pornography, how to report online material and what the risks are.
- Sexting: the risks to your children and how to recognize them.
- Aimed at all target groups: schools, young people, teachers, parents
- Fake news: recognizing and developing the topic in class.

The Generazioni Connesse - Safe Internet Center Italy project, co-financed by the European Commission under the Connecting Europe Program (CEF), is a program that the Commission uses to promote strategies that make the Internet safer for younger users and promote its positive and conscious use. The project is aimed at children, adolescents, parents and teachers: fourth and fifth grade of primary school and all grades of secondary school. Teachers have the opportunity to enroll their institute in the project. The project provides participants with a guide that allows them to think about their approach to security issues, the proper use of the Internet and the integration of digital technologies in the classroom. A web series is presented to help children think about the connection between themselves and the world, about the emotions, feelings and experiences that can occur every day. In addition, in-depth studies of online dangers (e.g., on the topic of cyberbullying) and 'etiquette' for online behavior are given. It offers an introduction to the possibilities of the online world and the "enemies" that can

lurk on the web. The metaphor of over-understanding is interesting: 7 figures that help children and adolescents to better understand and recognize the dangers of the Internet and, through everyday adversity, teach them how to prevent these dangers by using Internet resources consciously and competently. Parents can find useful tips to help their children use the Internet initially when they are young, to accompany them in discovering the endless possibilities of the Internet and to help them identify and avoid risks, when faced with sensitive issues such as relationships, feelings, image in the group.

The "Generazioni Connesse" portal aims to introduce young people to various topics that cause stress and destabilization in young people. Didactics tries to make them understand how some behavior that are common in today's reality can be problematic. To achieve this, the project uses words and graphics that are close to the target groups, without judging the behavior, but try to explain the "way out" of the vicious circles and traps that lie behind trivial habits. The portal teaches how to recognize dangerous behavior, both for the children themselves and for parents and teachers. The following topics are covered in depth: Online seduction, cyberbullying, online addiction, hate speech, online etiquette, online child pornography, protecting school data, the new European privacy regulation, online relationships and sexuality, using the internet safely and responsibly. In addition, tips are given on how to communicate with children, how to improve dialogue and how to report inappropriate content.

School information packages now reach 5 million students. Students have the opportunity to analyze their own behavior and talk with a partner. If they did not feel comfortable discussing these issues with their loved ones, they have the opportunity to trust the special "helpline" number. The following aspects should be considered:

- Media literacy in relation to online security and the beneficial use of digital technologies;
- Knowledge of standards of behavior and ways of using information and communication technologies.

LATVIA

“MANA DROŠĪBA” (“MY SAFETY”)⁵⁹

The State Police „Mana drošība“ Mobile App is for everyone who cares about their safety on the road every day. It is an easily accessible and easy-to-use tool that allows the user to obtain information about current and important security issues, test or supplement their knowledge by completing an interactive safety quiz, and find out what the right course of action is after an incident. Also, this application provides an opportunity to communicate with the state police in a convenient way when reporting such incidents.

JUVENILE INSPECTORS OF THE STATE POLICE OF LATVIA⁶⁰

In 2017, they organized 162 interventions on online safety, indicating possible threats in the virtual environment (amount of personal information provided, correspondence with unknown persons, potential offensive elements, etc.). Children's inspectors gave lectures on communication on the Internet and the topics "Internet Safety", "About the Internet", "Your Internet Safety" and lectures on the challenging game "Blue Whale".

LUXEMBOURG

CYBERMOBBING GUIDE⁶¹

The Cyber Mobbing Guide is the result of intensive collaboration between the police and BEE SECURE. It provides practical advice on how to deal with cyberbullying for police officers and victims. The flyer also states the need for adequate psychological support for victims and who to contact for such help.

ROMANIA

One of the biggest problems of the media in Romania is the content that can be accessible to children and teenagers. On June 25, 2008, the Senate passed an amendment that would require television and radio broadcasts to have 50% "good" or "positive" news. However, the Constitutional Court ruled the law unconstitutional before promulgation, so it never became law. The Romanian

Press Club has a code of ethics and an honorary council to question journalists and media found in breach of professional norms, although its decisions have often been criticized as arbitrary. The Convention of Media Organizations (CMO) also adopted a code of ethics; Community member organizations have developed guidelines for self-regulation and greater accountability in the Romanian media. In October 2009, a "Unique Code" was issued, which was adopted for the whole profession by COM, the trade union Media Sind and the Association of Journalists in Romania. One of the national/school actions taken is a high school curriculum called "Mass Media Competence". It is part of the curriculum in the school decision for secondary education within the field of study "Man and Society" and the curriculum is addressed to teachers who are interested in teaching the discipline "Competence in the mass media" and is designed according to such a way to meet the requirements imposed by the new concept of the goals of education, emphasizing not the content but the competences. The curriculum takes into account the following aspects:

- the "openness" of the school to everyday life, a necessity emphasized as such from the point of view of the concept of education and role-play in the school;
- the implementation of civic education through mass media.

“THE WHITE DOT TOLERANCE” PROJECT⁶²

It was implemented in the city of Deva during the period May 1 - June 19, 2015 and was aimed at teenagers aged 15. The activities were: debate, intensive training course for 25 students, meeting with 27 parents, human street exhibition (human chain) and six information activities in schools to raise awareness.

SLOVAKIA

STOPLINE.SK⁶³

An online form to report illegal content or activities on the Internet and plays a key role in spreading awareness of this type of crime. This project has the function of a national center for reporting illegal content or activities on the

Internet. As a result of the cooperation of all parties involved in this project, the regular publication of statistical information on illegal content and activities on the Slovak Internet and the identification of new trends in cybercrime will also lead to a more effective fight against child abuse and other illegal phenomena in Internet. Online cyber prevention program under the auspices of the civil association "eSlovensko". It discusses in detail what cyberbullying is and how to recognize it, what are the principles of protection against cyberbullying, and also illustrates examples from Slovak schools and the world. The interpretation of the subject is complemented by educational films.

SLOVENIA

EXAMPLES OF PRACTICE: PROJECT "DIGITAL STRESS SKILLS TRAINING IN THE FORM OF A WEB-BASED APPLICATION", LEAD ORGANIZATION: PCO - POKLICNI CENTER OBALA⁶⁴, SLOVENIA

Digitalization defines people's lives together and creates many new rules and norms. Such as the almost automatic expectation of employees reading emails after hours. This leads to stress, digital stress. Practicing digital stress competence in the application sandbox and thus gradually integrating it into our own actions is the aim and purpose of the TRIGS project. Therefore, the following examples that already exist in practice are an important model for further developing our skills based on their experience and existing knowledge. The partner organizations found many examples in their countries and selected those that seemed particularly innovative and targeted. The "Generazioni Connesse" (Connected Generations) project is a national project that primarily appeals to parents and young people and makes them competent in the issues of stress that the Internet and digital media generate in family life. As parents are often overwhelmed by their own digital stress, they can get important tips and guidance here to support their teens in the digital world. The "Stress Management and Health Care" training gives participants the opportunity to expand their knowledge of stress, its effects and possible measures to reduce it. This knowledge makes it easier for participants to help themselves and others

cope effectively with stress and thereby improve their own health. Because with the knowledge gained, it is possible to offer competent advice on stress issues, the project has a large-scale multiplier effect. The project "Always Online - Never Alone Again?" deals with questions of knowledge, especially in the field of education, helping young people and teachers to understand how the Internet and the media in general are trying to lure them as users and get their data. Staying safe online can be difficult and stressful for all ages, so help is often welcome.

The game Healthy Team ("Spiel Gesundes Team") is not actually deductive, but it is also intended as a stress prevention. A business training simulation is played out, deliberately causing stress to encourage appropriate responses and supportive thought patterns. After a build-up of stress, debriefing helps keep beneficial stress responses in practice.

All the methods mentioned so far have been developed to prevent stress for specific target groups. Everyone deals with stress in certain situations.

"ALWAYS ONLINE - NEVER ALONE AGAIN?" is a digital stress prevention project. It aims to promote media literacy among young people who are often left to their own devices in the world of digital technologies, as well as to strengthen the conscious use of digital media

The project is intended for two target groups: students and teachers. In relation to digital networks, students should:

- To learn to use them wisely.
- To recognize opportunities and learn to use them positively.
- To know the risks and dangers, especially regarding their own (mental) health.
- To find and adopt the balance between healthy eating, measures to deal with digital stress and regular physical exercise.

Teachers should:

- To raise awareness of healthy lifestyles - coping with (digital) stress, nutrition, exercise - in a digital world.

- Get incentives to integrate digital media into everyday school life in a health-friendly way.

Among other things, to be able to act as multipliers to prevent digital stress in schools - e.g., in terms of improving health in the area of coping with stress. Among other things, parents are informed about children's media use and preventive measures in education through parent-teacher discussion.

Digital health and the prevention of digital stress are the focus of the prevention project "Always online - never alone again?".

Digital media has become an integral part of young people's lives, but it can also be burdensome. As part of the project "Always online - never alone again?", students and teachers deal with the risks and opportunities of digital media in workshops and training courses, for a healthy lifestyle in harmony with the digital world. The main idea is to strengthen media literacy in order to promote the conscious and healthy use of digital media. At the same time, the content of the project also aims to bring participants closer to a balance between healthy eating, digital stress management measures and regular physical exercise in relation to the use of digital media.

In three-day on-site workshops at school, students and teachers deal with the opportunities and risks of the digital world. Experienced teachers and speakers impart knowledge and develop practical content together with participants. For example, YouTube stars and influencers introduce participants to techniques for the proper use of the Internet. Because: If you know the mistakes made, you can better pay attention to the balanced level of consumption and disclosure of information - and use the advantages for yourself. DIGI CAMPS addresses key areas such as YouTube, Instagram, blogging, journalism in the digital age, and more. Students also offer their own contributions, for example YouTube videos, Instagram photos, blogs or journalistic formats.

SPAIN

CONRED CYBERBULLYING PREVENTION PROGRAM

The ConRed program⁶⁵ addresses cyberbullying and other emerging issues related to the use of the Internet and seeks to promote positive use of this medium. The main objectives of the ConRed program are:

- to improve the feeling of control over information on the Internet,
- to reduce the time devoted to the use of a digital device
- to prevent and reduce cyberbullying.

The impact of the program was evaluated with a quasi-experimental design with a sample of 893 students (595 experimental and 298 control). The results of the ANOVA indicated that ConRed contributed to the reduction of cyberbullying and cyberdependence, to the adjustment of the perception of information control, and to the increase of the perception of school safety. ConRed is an evidence-based intervention using procedures in successful anti-bullying, it focuses on the risk factors for cyberbullying mentioned above. ConRed builds on the following previously successful strategies:

- *Proactive policies, procedures and practices:* implementing clear policies with practical procedures to reduce harassment. ConRed implements a specific action plan to combat the risks associated with the use of the Internet and social networks, improve technical and procedural skills with digital devices and teach young people how to use social networks safely and healthily.
- *Key understandings and competencies of the school community:* the implementation of mechanisms that help develop skills to prevent, identify and respond to the problem. ConRed's main function is to educate students, teachers and parents and improve their skills to facilitate safe and healthy use of the Internet and social networks. The program mainly focuses on increasing people's awareness and procedural skills in digital communication, aiming to improve students' online social competences.

- *Safe school environment*: the provision of safe spaces that positively influence student behavior. ConRed helps schools create a safe, healthy virtual communication environment for students, fostering in them a culture of mutual support, empathy for the weakest and better social relationships (including digital communication) between the three groups involved in the school: students, teachers, and families.
- *School-family-community partnerships* to promote collaboration between school, families and leading local organizations through greater involvement as a means of promoting support and reducing threatening behavior on social networks. The ConRed program encourages collaboration between the three groups – students, teachers and families – through collaborative activities, offering a virtual environment where the school community can meet to discuss issues of bullying and cyberbullying.

ConRed emphasizes the importance of critical awareness about the compulsive use of the Internet and social networks, the naivety and fallacy of believing that one has complete control over personal information uploaded to cyber environments and the negative consequences of data misuse.

The ConRed program is designed and developed to prevent cyberbullying by increasing the levels of technical, procedural and communication knowledge and improving social skills in virtual scenarios, especially on the Internet and social networks. Although the approach was 'holistic', taking into account all three social groups in the school community - students, teachers and families - the most important element was the work done with the students, who underwent eight trainings conducted by external experts. The experts worked in collaboration with each school's school climate planning team for three months.

The work carried out with the students was aimed at:

- Improving students' social networking habits, especially those related to controlling personal information as a form of reducing vulnerability;

- Raising their awareness of the time spent using social networks, especially the excessive time devoted to Internet activities and the risk of addiction;
- Analyzing the morally unjust, unhealthy nature of cyberbullying and the risks faced by victims of abuse committed through digital devices.

The ConRed program focuses on working directly with students. Over three months, weekly contact was maintained with participating schools and eight classroom sessions were conducted. These sessions were structured to form three main points:

- A section on the Internet and Social Networks focused on the importance of privacy and control over shared content and processes and highlighted the negative consequences of not having control or establishing safety measures in online communication processes;
- In the section on the benefits of healthy and intelligent use of the Internet and social networks, students were taught to improve their technical skills, prioritize pro-social spaces and practices, and exercise moral awareness and justice by avoiding and reporting cyberbullying;
- The section on dealing with the problems that can arise if the Internet and social networks are used in a naive or malicious way provided students with strategies to deal with the problems associated with inappropriate, irresponsible use, with a special focus on cyberbullying prevention and Internet addiction.

ConRed Training Sessions:

Session 1: What does ICT mean to you? And to people in general?

Session 2: How do you use social networks?

Session 3: Our Action Plan to Become an Expert.

Session 4: How do I feel doing different activities on the Internet?

Session 5: How can the Internet help me and others? How can I help others?

Session 6: What do we do on the Internet and why can it be harmful?

Session 7: The advantages and disadvantages of social networks.

Session 8: Reflection: knowledge consolidation quiz.

Tips for teachers and families in the ConRed awareness campaign:

Tips for teachers	Advice for families
Knowing and mastering the potential of the Internet and social networks is one of your goals.	Teach your kids to navigate the Internet the same way you teach them to navigate the street: to be careful not to bump into someone or let someone bump into them.
Creating spaces for dialogue and engagement is crucial to bringing the school closer to students and avoiding their alienation.	Protect your children from the harmful elements of the Internet just as you taught them to protect themselves from the cold, the rain and the dangers of the street.
Include social climate in cyberspace as part of your school climate project because connections between students continue on social networks.	Teach your children to be careful with invitations and messages from strangers. On the Internet, not all friends are real friends.
Adapt detection and deterrence policies to emerging issues such as cyberbullying.	Don't forget the keys. In social networks, the keys are the passwords. Teach your children how to use them safely.
Ask for guidance if our intervention is not having the desired effect.	Help your son or daughter make their own decisions when online and not be influenced by what others do or say.

The ConRed program produced positive results in terms of the three main objectives: the experimental group showed a marked global improvement both in comparison with the control group and in the measurement before. Regarding the first objective, a significant reduction in the perception of control over personal information on the Internet and social networks was observed. There is a growing awareness of the risks that may affect personal information and the need to improve security measures to protect personal content available on the

Internet. Given that all the information exposed on the Internet has an impact on the construction of the personal identity of adolescents, it is necessary to control it. Therefore, the above-mentioned reduction can be identified as a better adapted perception of adolescents about the real control they have over their personal information on the Internet, which in turn can be identified as a greater awareness of situations of potential uncertainty.

The program was created specifically with a focus on teenagers to protect themselves from cyberbullying. Awareness of risk and training of teachers and parents to monitor and guide youth behavior reduces high-risk behavior, prompts the taking of precautions, and promotes protective attitudes in online activity. This is important because it offers victims a way out of their isolation, helping them feel supported by influential adults and better able to deal with cases of gratuitous and sometimes violent aggression. This interpretation is reinforced by the changes observed in ConRed's measures of empathy, with increases in feelings of understanding, recognition, and affection for victims of cyberbullying⁶⁶.

UNITED KINGDOM

Age-appropriate design code - in early 2019, the Information Commissioners Office published proposals for its "age-appropriate design code" to further protect children online. The proposed code focuses on the best interests of the child as set out in the UN Convention on the Rights of the Child and sets out several expectations for industry. These include strict age verification measures, location services to be turned off by default for children, for industry to collect and store only the minimum number of children's personal data, for products to be safe by design, and for explanations that are age-appropriate and accessible.

BBC Own IT App⁶⁷ - a wellbeing app aimed at 8 - 13-year-olds getting their first smartphone. Combining state-of-the-art machine learning technology to track children's smartphone activity with children's ability to self-report their emotional state, it uses this information to provide personalized content and interventions to help children stay happy and healthy online. Featuring specially commissioned content from the BBC, the app provides useful material and

resources to help young people make the most of their time online and build healthy online behavior and habits, helping young people and parents lead more constructive conversations about their experiences online. The app does not collect any personal data or user-generated content, as all machine learning takes place within the app/within the user's device⁶⁸.

Project Evolve UK <https://projectevolve.co.uk/> - A fully resourced Digital Competence Education Framework identifying digital skills for each age of child to help parents and teachers understand the competencies that their children must possess, along with resources and activities that will provide them with the specific skills⁶⁹.

360 Degrees Safe - an online self-assessment tool for schools to review and assess their overall online safety provision, providing guidance and support to meet specified standards⁷⁰. The 360-degree safe self-review tool is free to use and is intended to help schools review their online safety policy and practice. It provides⁷¹:

- Information that can influence the production or review of online safety policies and develop good practice.
- A process for identifying strengths and weaknesses.
- Opportunities for commitment and involvement from the whole school.
- A continuum for schools to discuss how they might move from a basic level provision for online safety to practice that is aspirational and innovative.

Children's experiences online: Building global understanding and action, UNICEF, 2019 Global Kids Online research includes a wealth of information on good practice and responses to online harm. Global Kids Online is a research network initiative led by the London School of Economics and Political Science (LSE) and the UNICEF Innocenti Research Office (UNICEF Innocenti). It was launched in 2016 to build on the experience of the highly successful EU Kids Online program and further promote research on children's rights online on a global scale, with a focus on low- and middle-income countries. To understand the ways in which the research is received and used in partner countries and internationally, this research was commissioned in 2019 by UNICEF – Innocenti

and The London School of Economics and undertaken by an independent team at Matter of Focus. It uses an approach that allows for broad coverage of impacts internationally as well as specific impacts in partner countries, with a more detailed focus on three case countries (Uruguay, Bulgaria and Ghana) selected by the Global Kids Online management team⁷².

AMERICA

USA

The Child Online Protection Initiative developed by ECPAT International, Global Kids Online Network

In 2009, the International Telecommunication Union issued the first set of Guidelines on the protection of children online in the context of the COP initiative (<https://www.itu.int>). Over the past decade, the CPR Guidelines have been translated into many languages and used by many countries around the world as a starting point for roadmaps and national strategies related to protecting children online. The guidelines have been used to design, develop and implement national child online protection strategies in many Member States such as Cameroon, Gabon, Gambia, Ghana, Kenya, Sierra Leone, Uganda and Zambia in the African region; Bahrain and Oman in the Arab region; Brunei, Cambodia Kiribati, Indonesia, Malaysia, Myanmar and Vanuatu in the Asia Pacific region; and Bosnia, Georgia, Moldova, Montenegro, Poland and Ukraine in the Europe region. The Guidelines also formed the basis for regional events such as the Regional Conference on Online Child Protection (ACOP): Empowering Future Digital Citizens in Kampala, Uganda (2014) and the ASEAN Regional Conference on Online Child Protection, held in Bangkok, Thailand (2020). Pursuant to Resolution 179 (Rev. Dubai, 2018) the International Telecommunication Union, in collaboration with COP partners and stakeholders, was directed to update the four sets of Guidelines, considering technological developments in the telecommunications industry, including the Guidelines on Children with disabilities and children with special needs. As a result of this process, the Guidelines have been significantly updated and revised by experts and stakeholders, formulating a wide range of recommendations to keep children

safe in the digital world. The guidelines increase the scope of protecting children online by considering all the risks, threats and harms that children may face online to carefully balance the benefits that the digital world can bring to children's lives⁷³.

The International Child Sexual Exploitation Image Database⁷⁴

Managed by Interpol, the International Child Sexual Exploitation Image Database (ICSE DB) is a powerful intelligence and investigative tool that allows specialist investigators to share data with colleagues around the world. Available through Interpol's secure global communications system (known as I-247), the ICSE DB uses advanced image matching software to establish links between victims, perpetrators and locations. ICSE DB enables certified users in Member States to access the database in real-time — to query existing business entities, upload new data, sort materials, reduce the risk of conflicts, perform analysis and communicate with other experts around the world in response to inquiries related to child sexual exploitation investigations⁷⁵.

The WePROTECT Global Alliance

The WePROTECT Global Alliance (WPGA) is a global movement bringing together the influence, expertise and resources needed to transform the way Online Child Sexual Exploitation (OSCE) is addressed globally. It is a partnership between governments, global technology companies and civil society organizations. Its multi-stakeholder nature is unique in this field. The vision of the WePROTECT Global Alliance is to identify and protect more victims, apprehend more perpetrators and end online child sexual exploitation. The WeProtect Global Alliance consists of a number of components, notably a national response model and a global strategic response.

The 2020 Children's Online Safety Index

The DQ Institute 2020 Child Online Safety Index⁷⁶ (COSI) is the world's first real-time analytics platform that helps nations better monitor the online safety status of their children. COSI is based on six pillars that form the COSI framework. Pillars one and two — cyber risk and disciplined digital use — relate to the judicious use

of digital technologies. Pillars three and four, Digital Competence and Orientation and Education, are about empowerment. The last two pillars are related to infrastructure, these are the pillars of social infrastructure and connectivity.

International risk prevention programs in social networks - USA, UK, Ireland, Netherlands and Belgium Stop It Now!

A project that raises awareness of child abuse and has a helpline for people with pedophile feelings or relatives of pedophiles.

PERU

Intersectoral and Interdisciplinary Collaboration to Prevent and Respond to the Reality of Online Child Sexual Exploitation in Peru (Funded by the End Violence Fund)⁷⁷

According to the Institute of National Statistics, around 50% of 6–17-year-olds use the internet in Peru. The country's interior ministry said that between 2014 and 2017, 22% of recorded cases of trafficking for sexual exploitation started online. This echoes wider findings by the International Office for the Rights of the Child, which has warned that ICTs are being used to prepare children online to then be trafficked for sexual exploitation. Peru already has a relatively stable policy and legal framework to combat child sexual exploitation compared to Latin American countries. They are signatories to the SDGs, the CRC, the WPGA Model National Response Statement of Action and the Budapest Convention on Cybercrime. However, the number of complaints and cases that go to court is small. Moreover, none of these policies or frameworks explicitly mention how to approach and address the ever-growing problem of online CSEA. There are also huge gaps around information about CSEA, new forms of online exploitation, child protection resources and mechanisms, and cross-sector coordination, training and awareness. With the financial support of the End Violence Fund and Capital Humano y Social (CHS) Alternativo, (Alternative Human and Social Capital) — a non-governmental human rights organization based in Peru — the

country developed changes to Peru's Penal Code that expanded the definition of child sexual exploitation and criminalize this activity in any setting. CHS's most important contribution was technical support provided to the Committees on Women and the Family and Justice and Human Rights of the Congress of the Republic. Thanks to CHS and the efforts of supporting organizations, changes are foreseen in 10 articles of the Penal Code, and another seven will be added. The proposed changes create specific offenses and sentences relating to the sexual exploitation of children, the receipt of a benefit from, the co-ordination of, the promotion of or the facilitation of the sexual exploitation of children. Child contact payment is also covered by the revised code. In addition to systemic change work, CHS also raised awareness of the threat and trained nearly 400 children and 600 community members (teachers, parents, and service providers) directly on how to respond to child sexual exploitation, both through mainstream media engagement and providing personal training accordingly. Congress approved the bill, and the final version was signed by the President of Peru in June 2019.

ASIA

INDIA

K.R. MANGALAM SCHOOL, DELHI

Today, society plays a vital role in our children's lives and socialization is an essential aspect of it. In this technologically advanced world, social networking has been adopted as a new trend and has become a force to be reckoned with. For most teenagers today, social networks and virtual platforms have gained immense importance and rule their lives without even knowing it. There are certainly some positives, too, as children gather new experiences and perspectives through social media. It helps to expand their circle of friends, allows them to connect with online friends and also allows them to take some rest from the pressures of life. However, like any other technology, excessive use of social networks can also have adverse effects. That's why it's important to talk

to kids about using social media wisely to prevent them from getting too addicted to this enticing new platform.

K.R. Mangalam School not only focuses on instilling a sense of responsibility in students in handling such technology, but also advises parents and guardians to take appropriate steps if they find their children starting to lose their way in the virtual world of social networking. There are several effective methods that parents can use to identify and alleviate children's addiction to social networks:

Check: Being vigilant in today's interconnected virtual world is extremely important. If parents notice that the child tries to finish his meal as quickly as possible and tries to avoid other activities to jump on social networks, then this may be the first sign of addiction. Check their online activities and limit your child's online presence to curb this problem.

Don't let them reveal everything on social media: Sharing too much information, personal details and pictures on the social media platform can have much more adverse effects than you can imagine. Posting inappropriate things can jeopardize their reputation. More than being harmful, it is also a serious weakness in personal security that parents should guard against at all times by constantly monitoring their social media account, albeit indirectly.

Make them interact more with real people and experience real life: One of the most significant impacts of social media addiction is that a child is no longer able to concentrate on their education due to constant distractions coming from social media platforms. Cases of cyberbullying associated with the lack of real communication can also lead to the development of depression. Online discussion seems easier for children because it does not involve real emotions and face-to-face interaction and thus, they can fake their feelings as long as they are on virtual platforms while limiting the actual interaction in real life.

Engage them in outdoor activities and open discussions: Parents should ensure that children have enough exciting activities outside of social media. It can include various activities such as reading books, meeting friends, indoor and outdoor games and many more. Spending a lot of time with children and

understanding their needs and emotions so that they don't feel isolated is the best solution to let them get rid of social media addiction.

We, at K.R. Mangalam World School, one of the best CBSE schools in Delhi, believes that constantly interacting with children and letting them pour their hearts out is one of the most effective ways to stop them from getting addicted to social media or any other such virtual, unreal platforms. Only when children understand that making friends in the real world, with real people, is much more important than having hundreds of friends on social networking platforms, will they be able to understand the true meaning of life. We, at KRMS, always teach our students that technology, if used appropriately, can be a boon, but if its use goes wrong, it is nothing more than a curse. Likewise, if used appropriately, social networks can be an effective way to relax weary minds and make good connections with old friends. However, if it becomes a habit and an obsession, it keeps children away from experiencing the true taste of friendship and social life.

HOWRAH CBSE SCHOOL, LILWA, HOWRAH, WEST BENGAL

The growing popularity of social networks is becoming a human choice. But it also becomes a path to addiction, which can harm a child's mental development. Due to modern education, social networks create a great demand among young people for work, projects and education. Most of the time our child is distracted by social media like chatting, texting, watching videos and less engaged with e-books, Wikipedia etc. Therefore, it is the responsibility of the parents to allow the child to access a limited number of websites according to their age. HOWRAH CBSE school authority provides best guidelines to protect child from social media addiction.

Training for controlled use of social networks

Nowadays, children get access to the Internet from school age. They don't have a complete idea of how to use the internet from the start. They can use it to play online games and watch online videos. This is why we need to educate our children about the proper use of social media and the importance of social

media. It is also good to understand the limitations of internet access. Therefore, educate the child about the Internet and provide them with valuable knowledge about social networks.

Education about the negative impact on education

Social networks are so attractive with a variety of content that they create addiction in a child. As a result, it has a negative impact on his education. Children are no longer able to concentrate on their studies due to the excessive daily use of the Internet. So, educate your child about the negative influence of education due to social networks. Limit your use of social networks.

Parental controls for children's privacy

At a certain age, the child will be aware of certain facts from social networks and therefore he will start creating an account in general. In such cases, privacy and security settings should be made to limit the use of sites that may provide traumatic content.

Awareness of the influence of social networks

Everyone has access to the Internet, and therefore it is quite risky to provide information on social networks. Therefore, never provide your name, phone number, address, or personal information to unknown sources who have access for outside purposes⁷⁸.

PHILIPPINES

Ending Online Child Sexual Exploitation in Cebu (Funded by Fund to End Violence)

The Philippines has become a hot spot and online child sexual exploitation, and abuse (CSEA) is growing rapidly. The government decided something had to be done. In just one month in 2015, the Philippines received more than 2,600 referrals from the US notifying it of newly discovered Philippine child abuse

websites. Until laws in the Philippines are enforced more effectively, these numbers will continue to rise.

The International Justice Mission (IJM), a human rights NGO, is partnering with the Philippine government to strengthen its capacity to address child sexual exploitation and abuse online (CSEA), particularly the exchange of live-streamed sexual child abuse and other child exploitation material between paying clients and child traffickers. IJM works with the justice system to rescue and rehabilitate victims, hold perpetrators accountable for crimes, increase the capacity of local authorities and diagnose specific gaps in the public justice system that lead to impunity. The NGO also partners directly with local and international law enforcement agencies – including police and judicial systems – to identify and rescue victims, arrest perpetrators and gather sufficient evidence to support prosecution.

As of July 2019, IJM and Philippine authorities, working together, have rescued 123 children from sexual abusers. In addition to rescuing victims, IJM helped police apprehend and charge 20 suspected perpetrators and supported prosecutors in charging suspects, while supporting national and local prosecutors in ongoing cases. IJM further strengthened capacity by training more than 50 Filipino law enforcement officers and 100 judges and prosecutors in the ins and outs of investigating and prosecuting these crimes. IJM continues to advocate to the Philippine Congress and other agencies to implement the government's three-year commitment to strengthen the staffing and funding of the National Women and Children Protection Division.

SINGAPORE

DQ Institute —DQEveryChild is a global digital citizenship movement supported by the DQ Institute that started in Singapore with the support of Singtel and quickly expanded in collaboration with the World Economic Forum to include over 100 partner organizations. This movement aims to empower children with comprehensive digital citizenship skills from the start of their digital lives using the DQ World online education and assessment program. Data from this drive was used to create the 2020 Child Online Safety Index (COSI). The COSI

framework assesses and ranks children's online safety in 30 countries based on 24 areas grouped into six pillars that affect children's online safety. DQ Pro Family Readiness Package and DQ World provide opportunities for parents to assess their child's digital readiness and through educational materials to improve digital competencies such as digital citizenship, screen time management, cyberbullying management, cybersecurity management, digital empathy, managing the digital footprint, critical thinking and privacy management⁷⁹.

TURKEY

In August 1993, the Radio and Television Supreme Council (RTÜK) was established by the Radio and Television Act (Act 3984) to regulate private radio broadcasting and supervise broadcasts' compliance with the legal framework. RTÜK is responsible for assigning frequencies and issuing broadcast permits and licenses to private companies, and all television and radio broadcasters are placed under its supervision. RTÜK has the power to provide broadcasters with penalties (for violating the legal framework), which can range from a warning to the suspension of television and radio programs. However, RTÜK has no authority over TRT, as the public broadcaster is subject to a separate law (No. 2954). Social networks and internet addiction in young people are coordinated by four different bodies. They are MEB (Ministry of National Education), RTUK (Higher Council of Radio and Television), BTK (Information and Communication Technology Authority) and Health Services.

Activities of the Ministry of National Education (MOE): "Media Literacy" is offered as an elective course in primary schools as part of MOE regulations. However, the course is not taught in all primary schools in Turkey. Especially the schools in the western part of the country offer the course consisting of eight units covering communications, media, television, radio, newspapers, magazines and finally the Internet during the year. The first achievement of the latter unit is to learn about the Internet and discover innovation by promoting communication. The second achievement is to perform activities such as accessing information on the Internet, reading news, chatting, e-mail, distance

learning and gaming. The third and final achievement of the eighth unit is to be informed about the negative aspects and effects of the Internet in addition to its desirable characteristics (MEB, 2006: 93). This third achievement serves to prevent Internet abuse, not to prevent social addiction.

On the other hand, parents are offered 25 suggestions, which are called "aware and safe Internet users". Most of the suggestions are for the correct and safe use of the Internet. Some of the suggestions from the website that can be considered to prevent addiction are as follows:

- Do not allow the computer your child uses to access the Internet in his own room but keep it in the common room.
- Put some limits on the time your child uses the computer and spends on the Internet. Determine the length of time appropriate for your child's age.

VIETNAM

Online Child Protection in Vietnam (funded by the End Violence Fund)⁸⁰

As the number of young people online in Vietnam grows, so do the risks. To address the issue of online safety, Child Fund Vietnam initiated the Swipe Safe initiative. By 2018, young people aged 15-24 made up more than a third of Vietnam's 54.7 million internet users. This has increased their exposure to all forms of online sexual abuse and other dangers online and has resulted in one in three students suffering from cyberbullying. This is further exacerbated by the low levels of digital literacy among both children and their parents. In the absence of tools and materials promoting online safety, there is a poor understanding of risky online behavior and little or no advice on how to stay safe online. To help young people navigate the Internet safely, Child Fund Vietnam created the Swipe Safe initiative. This program educates about the potential risks online, such as cyber fraud, harassment or sexual assault, and provides advice on safety methods. Swipe Safe encourages parents, children, schools and the private sector to play an active role in children's online safety. It provides training for parents and Internet cafe managers to identify and address risks to children.

It also supports schools in developing child-friendly online safety policies and guidelines. A key innovation of the program is to engage young volunteers with extensive knowledge of technology to educate others in their local communities. These trainers are directly connected to the experiences of other young people and help to keep the curriculum up to date. As of June 2019, more than 8,700 young people, 1,100 parents and 1,000 'online safety partners' (including government officials, school representatives and Youth Union members) have received online safety training through the program. Studies show that 91% of targeted children have shown increased knowledge of online safety. This included skills such as privacy settings, information checks, responsible sharing, online searching and reporting harmful content. Of those surveyed, 89% knew where to go for support and 30% felt safer online:

- Remember that prolonged use of the computer or the Internet can have an adverse effect on your child's socialization and can lead to inactivity and other physical disorders;
- Have your child set aside time for games, books, sports, and art.

AFRICA

RWANDA

Child Protection Online in Rwanda (funded by the End Violence Fund)⁸¹

With the introduction of broadband and the increasing availability of smartphones, Rwanda decided to create a framework to ensure the safety of children online. Rwanda needed a child online safety policy that reflected the concerns of key stakeholders in Rwanda, incorporated best practices from the global community, followed cabinet procedures and documentation, and built institutional capacity in a new policy area. It is in this positive context that the Government of Rwanda has invited the 5Rights Foundation to develop a policy for the online protection of children. Working with Professor Julia Davidson from the University of East London, the 5Rights Foundation has developed a National Child Online Protection Policy and Implementation Plan. A multi-disciplinary

project group - comprising experts in law enforcement, child abuse and trauma, child development, law, data protection, telecommunications, business, education, government service delivery and children's rights - was formed in the UK to look at key policy areas. Similar disciplines were identified in Rwanda and with the support of the Rwandan Ministry of ICT and Innovation, they were able to engage with colleagues from justice, law enforcement, education, social work and family. Using extensive gap analysis—including interviews with members of the government, roundtable discussions, a literature review, and academic workshops—the team developed an understanding of Rwanda's existing digital capacity. Issues identified by the gap analysis, along with policy issues raised by existing international treaties and best practices, and the observations of expert working group members, were incorporated into the final policy and implementation document.

AUSTRALIA

ESAFETY COMMISSIONER (2015)

The eSafety Commissioner⁸² is the world's first government agency dedicated specifically to online safety. Established in 2015, eSafety has a legislative role to lead, co-ordinate, educate and advise on online safety issues to ensure all Australians have safe, positive and empowering online experiences. eSafety administers investigation schemes that focus on a range of harms, including serious: child cyberbullying, image abuse and prohibited content. It has the authority to investigate and take action to address complaints or reports related to these types of harm, including, in some cases, the authority to issue notices to individuals and online services to remove material. Alongside its investigative powers, eSafety adopts a holistic community approach that draws on social, cultural and technological initiatives and interventions. Its prevention, protection and proactive efforts provide a comprehensive approach to online safety.

THE AUSTRALIA ESAFETY TOOLKIT for Schools⁸³ is a set of resources designed to support schools to create a safer online environment. The toolkit reflects a

multifaceted approach to online safety education and is categorized into four elements, with resources that:

- prepare schools to assess their readiness to address online safety issues and provide suggestions for improving their current practices;
- engage the entire school community and participating in creating a safe online environment;
- educate by highlighting best practice in online safety education and helping schools develop the online safety capabilities of the school community;
- respond effectively to incidents while promoting safety and welfare.

Resources are categorized into four elements: preparation, engagement, education and response. Whether the resources from each element are used individually or collectively, each contributes to creating safer online environments for school communities. eSafety developed the toolkit in consultation with government and non-government education sector representatives in each state and territory. It was developed in response to the Royal Commission into Institutional Responses to Child Sexual Abuse and the Education Council's Work Program on Tackling Bullying and Cyberbullying. The toolkit should be used in conjunction with the eSafety Best Practice Framework for Online Safety Education, which establishes a consistent national approach to delivering high-quality programs with clearly defined elements and effective practices. The Framework Implementation Guide helps school leaders, educators and program providers use the Framework to design, deliver and review online safety training. It includes relevant links to the Schools Toolkit, eSafety classroom resources, the Australian Curriculum and existing policies and frameworks.

NEW ZEALAND

HARMFUL DIGITAL COMMUNICATIONS ACT (REVISED 2017)

The 2015 legislation made cyber abuse a specific crime and focused on a wide range of harms, from cyberbullying to revenge porn. It aims to deter, prevent and reduce harmful digital communication by making it illegal to post digital

communication with the intention of causing serious emotional distress to someone else, and sets out a series of 10 communication principles. It gives users the right to file complaints with an independent organization if these principles are violated, or to seek injunctions against the author or host of the message if the problem is not resolved⁸⁴.

C. INTERNATIONAL

RECOMMENDATIONS FROM TWITTER AND FACEBOOK

Twitter and Facebook⁸⁵ have issued special recommendations for children and young people on prevention of cyberbullying in their platforms. Here below some of their key elements are presented:

Facebook tips: If you are a victim of online bullying, we encourage you to talk to a parent, teacher or trusted person – you have the right to be safe. We're also making it easier to report harassment directly on Facebook or Instagram. You can always send our team an anonymous tip via a post, comment or story on Facebook or Instagram. We have a team that monitors these signals 24/7 from anywhere in the world in over 50 languages and will remove anything that is offensive or harassing. These alerts are always anonymous. We have Facebook Guidelines that can help you navigate the process of dealing with bullying – or what to do if you witness another child being bullied. On Instagram, we have Parental Guidelines that contain recommendations for parents, guardians and trusted adults on how to approach cyberbullying, as well as a central hub where you can learn about our safety tools.

Twitter Tips: If you believe you are a victim of cyberbullying, the most important thing is to keep yourself safe. It's important to have someone to talk to about what you're going through. This could be a teacher, another trusted adult, or a parent. Talk to your parents and friends about what to do if you or a friend becomes a victim of cyberbullying. We encourage people to report accounts that violate our policies to us. We can do this through the support pages in our Help Center or through the Tweets' built-in reporting mechanism by clicking on the "Report a Tweet" option.

I am being cyberbullied, but I am afraid to talk to my parents about it. How do I contact them?

If you are a victim of cyberbullying, one of the most important steps you can take is to talk to a trusted adult—someone you feel comfortable sharing with. Not everyone finds it easy to talk to their parents. But there are things you can do to

facilitate the dialogue. Pick a good time when you know you'll get their full attention. Explain how serious this problem is to you. Remember that they may not be as tech savvy as you are, so you need to help them understand what's going on. They may not have a ready answer to the situation, but they will most likely want to help, and together you may find a solution. Two heads are always better than one! If you still don't know what to do, think of other trusted people you can share with. There are often more people who care about you and want to help you than you think!

How can I help my friends report cyberbullying especially if they don't want to?

Anyone can become a victim of cyberbullying. If you see this happening to someone you know, try to offer support. It is important to listen to your friend. Why doesn't she want to report being a victim of cyberbullying? How does he feel? Explain that he doesn't need to report anything, but it's important to talk to someone who can help him. Remember that your friend may feel vulnerable. Be nice to him. Help him think about what he can say and to whom. Offer to accompany him if he decides to report. And something very important: assure him that you are on his side and want to help him. If your friend still decides not to report the incident, encourage him to choose a trusted adult who can help resolve the issue. Remember that in certain situations, the consequences of cyberbullying can be life-threatening. Inaction can make the victim think that everyone is against them, and no one cares. Your words can make a difference. Anyone can become a victim of cyberbullying.

Facebook/Instagram Tips: Reporting cyberbullying is always anonymous on Instagram and Facebook, and no one will ever know that you reported this behavior to us. You can report something that happened to you personally, but it's just as easy to report harassment against one of your friends using the tools included in the app. More information on how to report can be found in the Instagram Help Center and the Facebook Help Center. You can share with your friends about a tool on Instagram called Restrict, which allows you to discreetly protect your account without having to block someone – which may seem too harsh for some people.

Twitter Tips: “We have enabled a bystander reporting option, which means you can file a report on behalf of another child. This is now possible for personal information and impersonation alerts.”

How to stop cyberbullying without giving up the internet?

Using the internet has many benefits. However, like many things in life, it also carries many risks that you should beware of. If you become a victim of cyberbullying, you may want to delete certain apps or go offline for a while to recover. But staying off the internet isn't a long-term solution. You have done nothing wrong, why should you put yourself in a disadvantageous position? By doing so, you are only sending your bullies the wrong signal – you are encouraging their unacceptable behavior. We all want cyberbullying to stop, which is one of the main reasons why reporting cyberbullying is so important. But the desired safety on the Internet will not be achieved by eliminating harassment alone. We have to be very careful what we share or say because we can hurt others. We should be tolerant of each other online and in real life. We are all responsible! We have to be very careful what we share or say because we can hurt others.

Facebook/Instagram Tips: It's important that Instagram and Facebook remain safe and positive places for self-expression – people will only be able to share freely if they feel safe. Cyberbullying can be disruptive and cause negative experiences. That's why we at Instagram and Facebook are committed to fighting cyberbullying. We do this in two main ways. First, by using technology to protect people from bullying. For example, people can turn on a setting that uses artificial intelligence technology to automatically filter and hide comments aimed at harassing and abusing people. Second, by working to encourage positive behavior and interaction by providing people with tools to personalize their Facebook and Instagram experiences. Restrict is a tool designed to help you discreetly protect your account while keeping an eye on your harassers.

Twitter Tips: Hundreds of millions of people share ideas on Twitter, so it's no surprise that not all of us agree with those ideas. This is one of the benefits because in the process we all learn to show respect when we disagree or argue.

But sometimes, after you've listened to someone for a while, you might not want to listen to them anymore. Their right to express themselves doesn't mean you have to listen.

How can we prevent our personal information from being used to manipulate or humiliate us on social networks?

Think twice before you post or share something online - it can stay online forever and be used to hurt you later. Do not provide personal information such as your address, phone number or school name. Get to know the privacy settings of your favorite social media apps. Here are some actions you can take in many of these apps:

- You can choose who sees your profile, sends you direct messages, or comments on your posts by adjusting your account privacy settings.
- You can report offensive comments, messages and photos and request their removal.
- In addition to being able to "follow" people, you can also block them completely to prevent them from seeing your profile or contacting you.
- You can choose to make comments from certain people visible only to them without blocking them completely.
- You can delete posts on your profile or hide them from certain people.

Is there a penalty for cyberbullying?

People who are victims of any form of violence, including harassment and cyberbullying, have the right to justice and to hold perpetrators accountable. Anti-harassment laws, and cyberbullying in particular, are relatively new and do not yet exist everywhere. Therefore, many countries rely on other related laws, such as anti-bullying laws, to punish cyberbullying. In countries with specific anti-cyberbullying laws, online behavior that intentionally causes serious emotional distress is considered a criminal act. In some of these states, victims of cyberbullying can seek protection, barring communications from certain individuals and restricting the use of electronic devices used by that individual

for cyberbullying, either temporarily or permanently. However, it is important to keep in mind that punishment is not always the most effective way to change the behavior of bullies. It is often better to focus on repairing the damage and improving the relationship.

Facebook/Instagram Tips: “On Facebook, we have a set of Community Standards, and on Instagram, we have a set of Community Guidelines that we require our users to follow. If we find content that violates these policies, such as harassment or threats, we remove it. If you believe that content has been unfairly removed, you can file a complaint. On Instagram, you can submit a content or account removal complaint to our Help Center. Facebook uses a similar procedure through our Help Center.”

Twitter Tips: “We strictly enforce rules to ensure that all people can participate freely and safely in public discussions. These rules cover a number of aspects, including:

- Violence
- Sexual exploitation of children
- Harassment/threats
- Manifestations of hatred
- Suicide or self-harm
- Sensitive content, including violence and adult content

In relation to these policies, we take various enforcement actions when content is in violation. When we take such action, we do so either for specific content (e.g., an individual tweet or direct message) or for the entire account.”

AN INSTAGRAM GUIDE FOR SAFE USE⁸⁶

Elizabeth Milovidov, digital parenting expert and digital safety consultant to many of the European organizations focused on providing solutions and strategies for digital families has compiled a guide for safe use of Instagram. It supported the Council of Europe, COFACE Families Europe, EU KidsOnline, BetterInternetforKids, European Schoolnet and other European associations as

they created guides, research projects and tools for parents and families. These are the key recommendations from the document:

- 1. Account Privacy** - It's important to get the balance right between young people who love Instagram while keeping them safe. The goal is to avoid young people contacting adults they don't know or don't want to hear, and having a personal account is the best way to prevent this from happening. Having a personal account will allow the teen to control who sees or replies to their content. With a private account, people must follow us to see our posts, stories, and all follow requests must first be accepted by us. People we haven't accepted also can't comment on our content in those places, and won't see our content in places like Explore or hashtags at all. That's why anyone who signs up on Instagram and is under 18 will have the option to choose between a public or private account, with private being the default. For young people who already have a public Instagram account, they will receive a notification reminding them that their account is public and explaining how they can switch to private. Even with a public account, your teen can remove followers, choose who can comment, and turn off Show Activity Status so their friends can't see when they're online. If your teen's account is public, anyone on or off Instagram, with or without an Instagram account, can see the content your teen posts, such as in Stories, Feed, or Live, and follow your teen without having to approval. There will still be young people who prefer to have a public account – for example, young artists trying to build an audience – so we'll still give young people a choice, while doing what we can to highlight the benefits of a private account. If your teen already has a public account, they can switch to private at any time in their privacy settings.
- 2. Share stories only with close friends** - a teen can create a list of close friends and share their stories only with the people on that list. They can add and remove people from it at any time and people will not be notified when they are added or removed from their close friends list.
- 3. Control of messages** - at Instagram, we want young people to have control over who can message them, and we don't want young people to receive

unwanted messages from people, especially adults, they don't know. That's why we've launched a series of features to protect young people in their DMs (direct messages). Anyone on Instagram can limit who can send them direct messages and who can add them to group chats. This means your teen can choose to only receive messages from people who follow them. This year we introduced a new feature that prevents adults from sending messages to people under 18 who don't follow them. This means that when an adult tries to send a message to a teen who is not following them, they get a notification that sending a DM is not an option. This feature relies on the age people give us when they sign up, as well as our work to predict people's ages using machine learning technology. We've also developed new technology to help us find adult accounts that have shown potentially suspicious behavior – for example, they may have been repeatedly blocked or reported by young people. Our new technology prevents these accounts from finding and interacting with young people's accounts. Using this technology, we will not show young people's Explore, Reels or "Accounts Suggested for You" accounts to those adults. They will also not be able to see comments from young people on other people's posts, nor will they be able to leave comments on young people's posts. Finally, if a potentially suspicious adult account finds accounts of young people by searching for their username, they will not be able to follow them. We will continue to look for additional places where we can apply this technology to protect young people.

- 4. Limiting Targeting by Advertisers** - we've also made changes to how advertisers can reach young people with ads globally. We will now allow advertisers to target ads only to people under 18 based on their age, gender and location. We have already limited advertisers to these three categories for young people in Europe, but the age threshold differs from country to country based on various factors, including local GDPR requirements. Now we're taking this further by raising the age to under 18, removing the opt-in to more personalized ads, and introducing these targeting restrictions to all young people on Instagram globally. We already give people ways to tell us they prefer not to see ads based on their interests or their activities on other websites and apps, such as through controls in our ad settings.

- 5. Relationship Management** - there is no place for abuse and harassment of any kind on Instagram. It is against our policies to create an account, post photos, or make comments to abuse or harass someone else. Let your teen know that if they notice an account, photo, video, comment, or message that is intended to harass or bully someone, they can report it in the app by tapping "..." in the top right corner of the post or profile by swiping left on the comment or by tapping and holding the message and tapping Report. Reporting is completely anonymous; we never share your teen's information with the reported person.
- 6. Managing the number of likes** - we want people to be able to focus on the photos and videos being shared on Instagram, not just how many likes the posts are getting. We also want to put our community in control of their own Instagram experience. That's why we're now giving everyone the option to hide the number of likes on all the posts you see in your feed – and you can do this by visiting the new Posts - Settings tab. You'll also have the option to hide the number of likes on your own posts so others can't see how many likes your posts are getting, and you can do this on a post-by-post basis.
- 7. Block unwanted account** - your teen can block accounts they don't want to interact with. This will block people from seeing and commenting on their posts, stories, reels and live streams. We know that sometimes teens don't like to block people because they're worried that person will be notified - this isn't the case. We don't tell people when they were blocked or who blocked them, and you can unblock an account at any time. We also recently announced an update to our blocking feature to make it harder for someone you've already blocked to contact you again through a new account. Now, when you choose to block someone on Instagram, you'll have the option to both block their account and pre-emptively block any new accounts that person may create.
- 8. Account Muting** - there may be accounts that your teen isn't interested in interacting with but is hesitant to unfollow. Muting will keep posts or stories from these accounts from appearing in your teen's feed. The other person won't know they've been muted, and your teen can turn it on at any time.

9. Account Limitation - sometimes young people don't feel comfortable blocking or unfollowing someone because they feel it could lead to awkward or escalating situations. To help you, we've developed a restriction mode that allows your teen to protect their account from unwanted interactions without notifying the abuser. After restricting someone, comments from that person will only be visible to them. Restricted people can't see when you're active on Instagram or when you've read their direct messages. Your teen can remove the restrictions at any time.

10. Managing Comments - your teen controls who can comment on their photos and videos. In the Comment section of Instagram's privacy settings, they can choose to allow comments from everyone, the people they follow and those people's followers, only the people they follow, or only their followers. They can also remove comments from their posts entirely.

- ***Filtering offensive comments*** - in addition to turning off comments completely, we also have controls that help you manage what comments can appear under your posts, as well as controls that can hide comments that are offensive or harassing. We've created filters that automatically hide potentially offensive or harassing comments, and we've just launched an option to "Hide More Comments" that may be potentially harmful, even if they don't violate our rules. Your teen can also create their own personalized list of words, phrases or emoticons they find offensive. Any comments using these terms will be hidden under their posts, so they and their followers won't see them. We really encourage them to do this to protect them from having to see offensive comments.
- ***Filtering abusive messages*** - we don't want anyone on Instagram to receive abusive, insulting or offensive messages. Because messages are private conversations, we don't proactively look for hate speech or harassment there in the same way we do elsewhere on Instagram. In addition to our existing messaging controls that let you choose who can message you, we've also created a new tool that, when turned on, will automatically filter private message requests containing offensive words, phrases and emoticons, so you never you don't have to see them. When your teen turns this feature on, they can either choose to use our

predefined list of offensive terms that we've developed with leading anti-discrimination and anti-bullying organizations, or they can also create their own custom list of words, phrases or emoticons. which they personally find offensive. We encourage them to do this because we understand that different words can hurt different people. Any private message request that contains these offensive words, phrases or emoticons will be automatically filtered into a separate hidden requests folder and they will not be notified when they receive it. If they choose to open the hidden requests folder, the text of the message will be masked so they won't encounter offensive language unless they tap to reveal it. They then have the option to accept the message request, delete it, or report it. You can turn both comment and request filters on and off in a new dedicated section of your privacy settings called *Hidden Words*.

- **Negative comment warning** - we use AI to detect when someone might be trying to post a comment that might be harmful or offensive and send them a warning to give them a chance to reconsider. If someone repeatedly tries to post offensive comments, we display a stronger, more prominent warning - reminding them of our Community Guidelines and warning them that we may remove or hide their comment if they post it. Since rolling out these comment warnings, we've seen that reminding people of the consequences of bullying on Instagram and providing real-time feedback as they write the comment is the most effective way to change behavior.
- **Group comment management** - we know it can feel overwhelming to manage an influx of comments, so we've introduced features to bulk delete comments, as well as block or restrict multiple accounts that post negative comments. To enable this feature on iOS, tap a comment or "View All Comments" and then tap the "..." icon in the upper right corner. Select "Manage Comments" and select up to 25 comments to delete at once. From here, you can also choose to restrict or block accounts in bulk.
- **Block comments** - your teen can block accounts they don't want to interact with. Comments will no longer be displayed from a blocked

account. Your teen can also turn off comments from all posts or individual posts.

11. Time Management – the Activity Dashboard shows your teen how much time they've spent on Instagram over the past day and week, as well as their average time on the app. They can tap and hold the blue bars to see how much time they've spent on Instagram in a given day. Your teen can also use the daily reminder to set a limit on how much time they want to spend on Instagram. In addition, your teen can use the “Pause All Notifications” feature to mute Instagram notifications for a set period of time. When the present time is up, the notifications will return to their normal settings without having to reset them.

12. Security Management - keep your teen's account secure and their logins private. You can manage your teen's security by:

- Two-factor authentication setup.
- Ensuring that you and your teen read all important emails from Instagram.
- Checking activity on login.
- Make sure your teen has access to backup codes that allow them to sign in if they can't get their two-factor authentication code through an authenticator app or via text message.

IV. METHODS FOR PREVENTION OF SOCIAL MEDIA THREATS - SURVEY PERSPECTIVE

Children and young people worldwide are spending more time online at increasingly younger ages. Even though many of them are technically competent and skilled internet users, fewer children have knowledge and skills to avoid risks, social networks hide and act in a proactive way. In addition, the COVID-19 global pandemic saw a surge in the number of children joining the online world for the first time, to support their studies and maintain social interaction. The constraints imposed by the virus not only meant that many younger children began interacting online much earlier than their parents might have planned, but the need to juggle work commitments left many parents unable to supervise their children, leaving young people at risk of accessing inappropriate content or being targeted by criminals in the production of child sexual abuse material. More than at any time before, keeping children safe online requires a collaborative and coordinated international response, demanding the active involvement and support of a broad number of stakeholders – from industry stakeholders including private sector platforms, service providers and network operators, to governments and civil society.

Considering the trends observed below are presented the results of survey among young people in partnering countries about their knowledge and skills related to prevention of social media threats. The sample included young people between 14 and 29 years old. The selection of the respondents was not based on gender, ethnicity or race. A special questionnaire with 26 questions was developed and implemented in all four countries so there could be a comparability of the results later (see appendix A). For the development of the questionnaire, an analysis of the available literature on Internet security issues was carried out, with special attention being paid to the best practices and methods for prevention of social media's risks for young people in the age group of 14-29 years. Against the background of rapidly developing trends in social networks and the constant activity of young people to reflect their personal lives in them, the survey in partnering countries is looking for more data about:

- What is the level of awareness, experience and knowledge of young people about the methods for prevention of risks, associated to social networks?
- Whether young people manage to distinguish the right methods for risk prevention when it comes to the use of social networks?
- Do young people have risky behavior online and/ or offline?
- What are their skills and whether they can adequately protect themselves?
- What are the attitudes, the level of media literacy and critical thinking of young people about the risk's prevention methods?

In general, the respondents in all partnering countries welcomed the survey provided to them with interest and positive attitude. The filling of the electronic questionnaire did not cause any difficulties because the questions were formulated considering the age group of the respondents. The respondents treated the filling out with the necessary seriousness and attention.

1. BULGARIA

The survey in Bulgaria was initiated in 2023 by the leading organization of the project - "Follow Me" Association, Bulgaria. The sample involved **275 respondents**, selected from schools and universities in the city of Varna. The respondent's characteristics are as follows:

- ✓ **Age:** Around 95% of the respondents were in the age group 14 to 18 years old. The rest of the young people - around 5 % - were in the age group 19-29 years old. The age distribution corresponded to the purpose of the survey since the prevalent number of respondents are in the age group that is most active in social networks and are particularly exposed to risks.
- ✓ **Gender:** Young people of both sexes participated in the survey without pre-selection according to gender. In the current survey the distribution between male and female is 52% (143 boys) and 48% (132 girls).
- ✓ **Social status:** All the respondents are students - most of them are just students (97%) and 3% are studying and working. That allows to objectively see the attitudes of the most vulnerable target group regarding methods of protection in social networks.

QUESTION №1: How do you prefer to communicate with your peers? It is interesting fact that 66% of the respondents prefer live communication with their peers. Only 3% prefer online form of contact with their friends and 31% have no preferences and would use both ways to communicate. A comparative analysis of the answers to this question and the inclusion of the gender indicator shows that there is no difference between both sexes in communication preferences. There is a slight variation in answers regarding the lack of preferences and the males are a bit more likely to communicate in both ways – 47 boys vs. 38 girls, but statistically this is not a significant difference.

QUESTION №2: When you are on vacation, is it mandatory for you to have internet? The answers to this question are impressive, because 75% of the respondents prefer to have the Internet during their vacation, which respectively gives information about the lack of skills to disconnect from social networks and the need to be constantly informed. This is somehow in contrast to the answers to the previous question where most respondents answered that they prefer live communication with their peers. Only 25% of the respondents said that they don't need internet during their vacation. There are no gender specific differences in the answers to this question.

QUESTION №3: Do you think there are things on the Internet that can harm you? It is interesting that around 80% of the respondents know about the risks and harms of online media and, respectively, from the previous questions, actively use social networks. The fact that 20% do not know or ignore the risks in the networks is worrying. In a comparative analysis with the gender indicator, the results provide information that there are no gender related differences.

QUESTION №4: Which social media protection methods do you know? Here, the most recognizable method to protect against risks in social networks is doubt and mistrust of information that is published on the Internet and social networks – this includes around 73% of the respondents. Around 61% rely on personal control over information. Around 60% of the respondents check if they have mutual friend with stranger who sent them a friend request and around 54% do not accept friend requests from strangers. A common answer from the respondents is not providing personal information and hiding their real name. Around 14 % of all the respondents admit that they are not aware about any protection method from the risks and harms of internet. The results of this question indicate some familiarity and awareness among young people about protecting themselves from the risks in social networks but still there are some serious gaps in their knowledge and skills. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №5: Did you know that there is a mobile application (App) that monitors how much time you spend on the Internet? Around 67% of respondents know about such mobile application, while around 22% have no idea about it. Only 11 % use it, which speaks of a distortion of personal judgment to protect against misuse of time on the Internet. It can be concluded that young people rely on their own personal control over the time spent or that they do not like to be limited. It is a bit surprising that the respondents in the age group 14-18 years are more aware of this kind of software than the respondents, in the age group 19-29 years. No matter of their age most of the respondents are uncritical to the time they spent online.

QUESTION №6: Can you spot a fake (fake news) from real news? The answer here is optimistic because 70% claim that they can distinguish fake news from real ones. Referring to the above question about methods, knowledge about fake news among youth is based more on accumulated experience than on learned and validated information. Worryingly, 20% ignore the truth of the news.

Comparing this question with the dangers of the Internet that can harm the young people who answered and comparing the positive answers, 159 young people are aware of the risks and fake news and confirm that they can distinguish it from the real thing. It is worrying that 10% of the surveyed young people answered that they cannot distinguish fake news and that they are aware of the risks on the Internet. The comparison makes it possible to better understand the risky behavior of young people on the Internet and social networks. Around 15% of all the respondents who said that there are risks and harms, associated with internet (Question №3) do not care about the truth in the news they read online. This is a clear indicator, that young people do not think that fake news could be dangerous in some way.

QUESTION №7: How will a day without internet access affect you? Access to the Internet is not so important for almost 60% of the respondents, who claim that a day without the Internet will not affect them and that they will have more time for useful things. The rest of the respondents are not keen on losing the internet connection because of:

- 24% say they will lose the touch with their contacts and will not be able to communicate with them;
- 12% of the respondents are worried for missing the news and trends they follow.

The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.

QUESTION №8: What will you do if your social network account is blocked? To this question, the prevailing answer is that the respondents will create a new profile on the social network (135 of the surveyed), which speaks of dependence on their activity and the attention they receive online – a possible reason for limiting social live contacts and voluntary social isolation. Of those who answered that they would create a new profile on social networks, 62 were girls and 73 were boys, which shows a gender difference in social network activity. The degree of importance of the social network profile depends on gender in these results, indicating that men are more active on the Internet and undertake more social network activities. **The sum of the percentages is more than 100%**

because some of the respondents have given more than one answer to the question.

QUESTION №9: If you get an invitation to join a group from a stranger, what will you do? On this question, 80% would refuse the invitation, which is based on a negative previous experience among the youth. This, in turn, responds to the knowledge and skills of young people to protect themselves from the risks in social networks and to what extent they can do it, which can be seen in 20% of the respondents who would accept the invitation - 10 girls and 44 boys. Here again, there is a gender difference in social media activity, expectations and willingness to take risks.

QUESTION №10: You come across an interesting article on the Internet. How will you verify its authenticity? Predominance of the answers to this question are related to checking on the Internet the validity of the article and its source. It means that there is some level of critical thinking among children and young people who participated in the survey. On the other hand, around 21% of the respondents will trust the information without any doubt which is a risky behavior. Around 15% will turn to friends and relatives for advice which means that they need the authority of the more experienced and trusted people. Analysis of critical thinking doesn't show significant differences in both genders as opinion and possible behavior. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №11: What are your ways of dealing with cyberbullying? Most respondents (56%) have answered that they would talk to relatives and friends – trusted people with authority of more experienced users. Active learning approach is shown by 35% of the respondents who said they would read about it and another group of 17% of the surveyed who will watch a video about how to manage with cyberbullying. Both answers could be a sign that the youth lack knowledge, skills and specific information needed to deal with cyberbullying, but they would like to learn new skills. An honest reply has been given by 21% of the respondents who state that they do not know how to cope and can be described

as a high-risk group. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №12: If a friend suggested you follow a popular trend, what would you do? The answers to this question show a criticality towards the information that is offered on internet. According to the answers, most of the surveyed young people will not follow blindly any new trend (38%) and will look for information about the trend in advance (another 38%) – this is altogether 76% of all the respondents. Around only 11% of the responses given by youth provide information on possible risky behavior since they show a readiness to follow a certain trend without preliminary research. A significant part of the respondents (32%) would watch TikTok videos about the trend, which means that they are ready to accept the idea of following. The level of critical thinking and the tendency to risky behavior is not influenced by gender. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №13: You use social networks because...?: To this question, young people mainly answered that they use social networks for fun in their free time (79%) and to connect with friends and relatives (77% and 51%). A small number of respondents have answered that social networks are a way to find out what others think of them (6%) and to compare their life with those of other people (6%). There are no significant differences in answers between genders. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №14: Do you share your negative experiences online with anyone? Most of the respondents do not share negative experience they had in social networks (57%). Around 23% ignore the problem. About 4% don't know who to share the negative experience with. These groups of respondents present 84% of all the surveyed. The fact that young people do not share about negative experiences on social networks and ignore the problems is very worrying. These results show that young people are not aware of the real risks and underestimate their effects. Since this is a threat for their mental health it requires serious

measures to educate young people with skills and knowledge about protection on the Internet. Only around 16% of all the respondents would share with friends and relatives which is a more active approach. There are no significant differences in the answers given by gender.

QUESTION №15: How do you deal with bullying on social media? Most of the respondents stated that blocking the profile is the method they use to deal with bullying online (60%). It is worrying that 43% of the respondents would ignore the problem and around 14% will respond with aggressive behavior which means that these young people are not skilled to manage harassment online. Only around 13% of the respondents would share with friends and relatives. Deleting the app will be done by 11% of the surveyed. There are some differences in the answers by gender. The question was answered by 132 girls and 143 boys and the variations are related mainly to the reaction of bullying on social media: 10% of the boys would respond to aggression with aggression, while only 2% of the girls would do the same. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №16: Have you come across videos with "sensitive content"? The distribution of videos with sensitive content is a network risk that young people often fall into (66%). Very often these videos are forwarded by friends or posted in groups where youth have easy access. Around 19% rarely come across sensitive content since they have specific sensitive content controls. Only 15% claim that they don't come across such videos. Looking at the results through the gender lens it turned out that boys (39%) come across such video materials more often than girls (23%), but girls pass them more often (48%) than boys (24%). Boys show activity on these materials and their willingness to maintain the channels they follow. Women's covert activity, unlike men's, shows risky curiosity and an inability to protect themselves in social networks.

QUESTION №17: How do you protect yourself from "sensitive content" video on your social network? The leading answer here is blocking the profile - 44% or 121 young people answered. Around 33% state that they will look out of curiosity

which could be considered as risky behavior. Changing profile filter is a relatively popular method that is used according to 25% of the answers. Sharing with friends and relatives is stated in only 10 % of the answers. Examining responses by gender provides the following information:

- Around 45% of girls would block the profile while only 34% of the boys would;
- Around 23% of girls would watch out of curiosity, while 32% of the boys would do the same;
- Around 5% of girls would share with friends versus 11% of the boys would intend to do the same.

In conclusion when it comes to online safety girls approach is with more caution and are more likely to take protective measures, while boys are more curious and take more risks. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №18: When you receive a message with hate language (Hate messages), you...?: There is a sharp edge in responses to this question: around 48% will ignore and block the profile that sends the message, 24% will delete the message and 23% will not even read the message if it is from an unknown profile. Around 22% will respond to the message with the same tone which suggests answering to the aggression with aggression and in conclusion – lack of knowledge and skills to manage hate language online. Only 8% would answer with positive tone. Looking at both genders there are some differences in the responses highlighting two main approaches: Girls more than boys would not read a message from stranger (20% vs. 6%), while boys would respond with aggression much more often than girls (12% vs. 30%). Considering the age and the social development of the young people, participating in the survey this behavior shows risky manifestations on the Internet. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №19: Have you personally sent such messages? Sending messages with hate speech have been confirmed by 10% of the young people surveyed. Around 24% of the respondents admit they sent such messages in answer to

some provocation. On the other hand, half of the respondents (52%) haven't sent such messages, and around 22% are avoiding doing it. Through the gender lenses the answers indicate that boys send hate messages more often than girls (16% vs. 4%), (57% vs. 41%) and boys surveyed confirmed that they have sent messages with hate speech more often than girls (24% vs. 19%). The conclusion could be that boys are more aggressive in online communication in social networks than girls and are more likely to engage in risky behavior. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №20: Do you know what is misuse of personal and/or financial data on the Internet? Most respondents (80%) state that they are aware of what is misuse of personal and/ or financial data. Only 15% have no information and 5% are willing to learn more. This means that around 20% of the young people surveyed realize the lack of knowledge about it. Considering the active use of the Internet and social networks, online shopping and risks, related to protecting financial data, young people do need additional and more specific information on how to protect their personal data on the Internet.

QUESTION №21: What methods of protection against misuse of personal and/or financial data do you know? Most popular protection method of personal and financial data online among young people surveyed is password protection with additional app and two-factor authentication (around 60% of the answers). Not sharing personal and financial data is mentioned in 56% of the answers and around 38% of the answers mentioned not sharing personal data at all. Antivirus program would be the next method chosen by young people according 27% of the answers. The distribution of the methods according to the answers suggests a relatively good knowledge and skills among young people needed to protect themselves from malicious interference in their personal profiles on social networks. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №22: If you find out that your friend has an addiction to social networks, how will you help him? Personal support is offered in 50% of all the answers from the young people surveyed. Around 23% of the respondents want actively to help and that they would look for information how to do it. Around 22% of the respondents stated that they don't know how to do it. Both groups indicate lack of suitable information and skills about how to help their peer and require education among young people. Around 17% of the respondents would recommend to their peer to delete the app as a method for helping the addicted person, and 12% would inform the parents of the person. It is surprising that 17% of the respondents indicate that they don't think addiction is or could be a problem and they claim that there is nothing wrong with dependence on the Internet and social networks. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №23: How will you protect yourself if an unknown profile writes to you and asks to meet you? Caution among young people is seen in 42% of the cases and they would block the profile or in 41% of the cases they will not respond to the message and delete it. Around 27% of the respondents would communicate and meet in real life with the person and 19% would answer to the message since they don't think there could be a risk for them. It is worrying that a huge group of the respondents would not take any precautions and meet with a stranger in the real life – this is a very risky behavior. Only 6% of the young people surveyed would share with their friends and relatives about the situation. From the analysis of the results, 27% of the surveyed boys are willing to take the risk of dating, while 18% of the girls would do it. This shows that boys are more prone to take risks in their communication on social networks. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

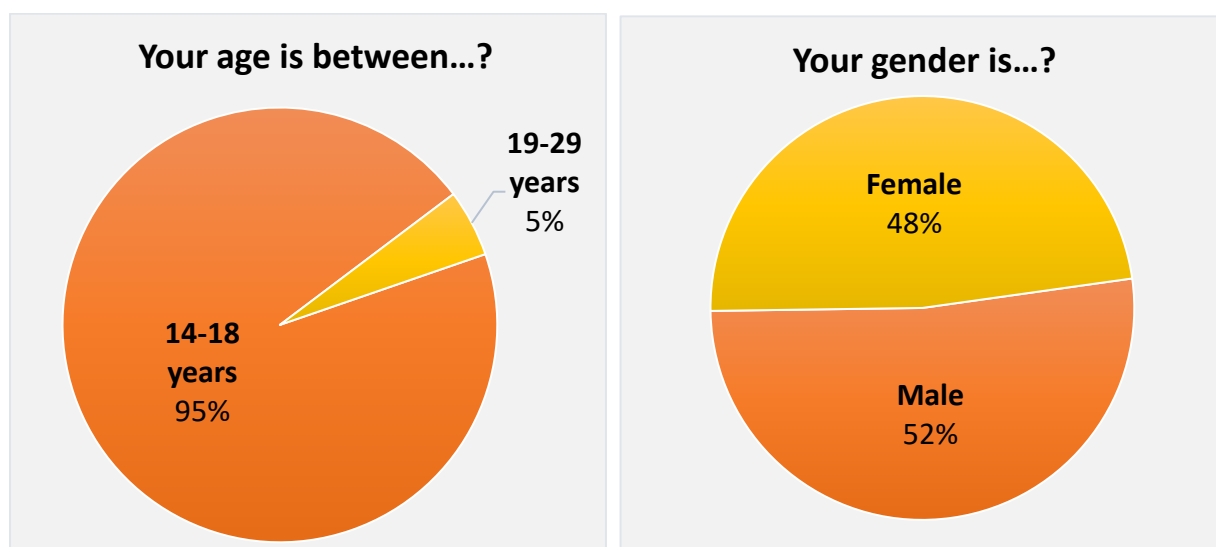
QUESTION №24: Do you personally send such invitations? Most of the respondents (64%) deny sending invitations for communication to strangers. surveyed young people answered that they did not send such messages. It is worrying that rest of the respondents do send invitations as an excuse for their

limited social life and as a way for finding new friends – a signal, that they are quite addicted to social media and internet and lack normal communication in real life. Gender differences are observed in two aspects: Only 10% of the girls are maintaining their social contacts through online communication, while 17% of the boys do the same. And the second aspect – girls are more cautious in online communication and 70% deny sending invitations to strangers, while 59% of the boys do that.

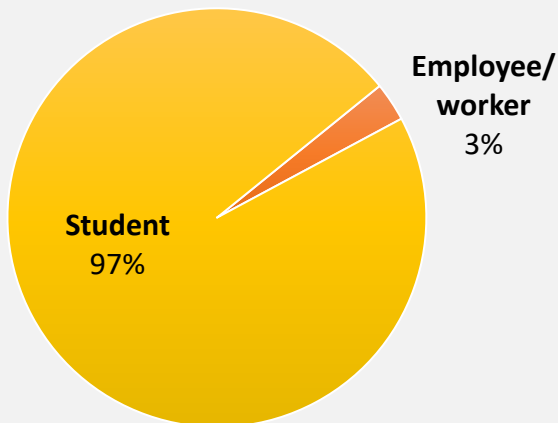
QUESTION №25: Have you received provocative photos? The response ratio was almost equal: 53% of the respondents had received provocative photos, while 47% had not. This provides an answer to the extent to which young people in social networks are protected from sensitive and harmful content. Of those surveyed, 22% of the boys received photos and 27% of the girls, indicating that girls are more vulnerable online.

QUESTION №26: Have you sent provocative photos that you wouldn't post on the Internet? Here the answers are almost unequivocal: 92% of the respondents claim that they did not send provocative photos. Broken down by gender, there is a slight difference in favor of girls who deny sending provocative photos (42%) while 36% of the boys deny it. A solution for protection online could be having a filter on youth profiles and knowing how to control the content they receive protects them from malicious and provocative messages.

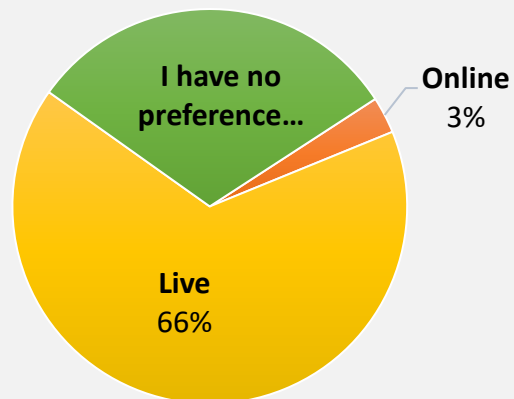
VISUAL REPRESENTATION OF SURVEY RESULTS IN BULGARIA:



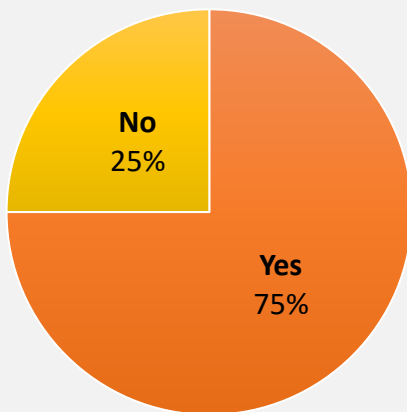
Your status is...?



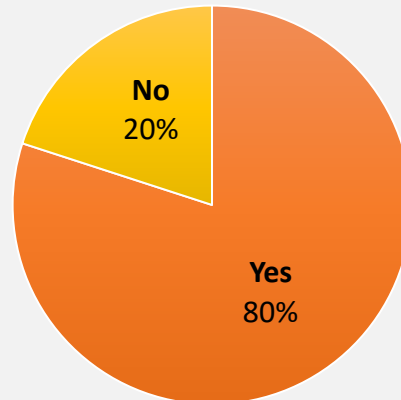
1. How do you prefer to communicate with your peers?



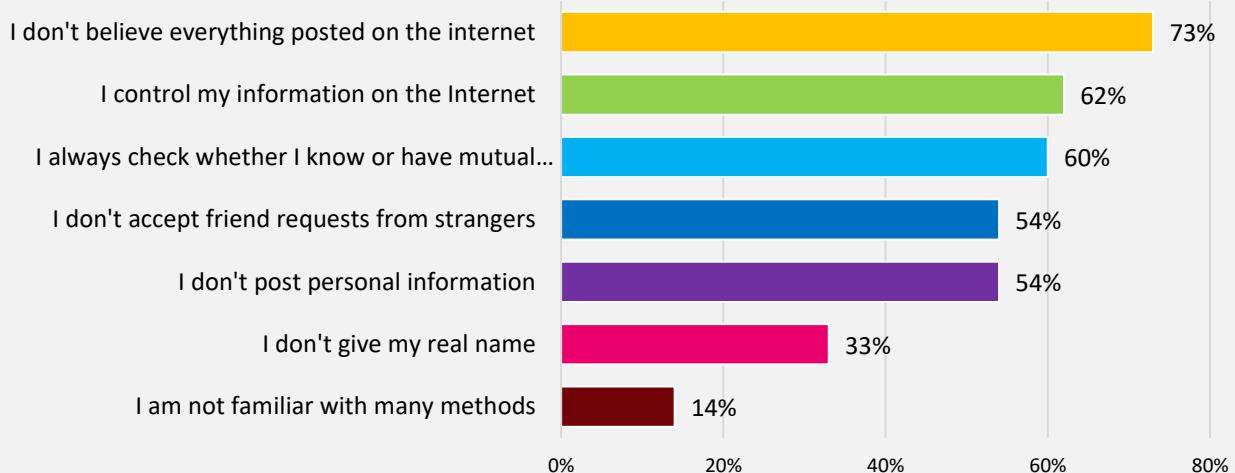
2. When you are on vacation, is it mandatory for you to have internet?



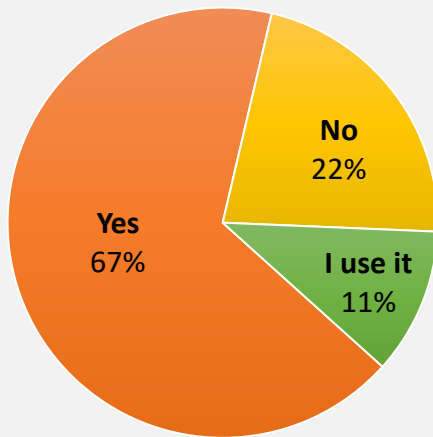
3. Do you think there are things on the internet that can harm you?



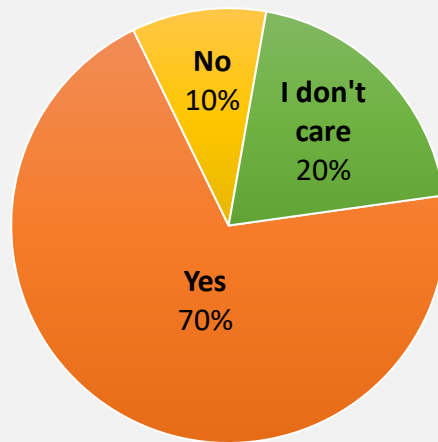
4. Which social media protection methods do you know...?



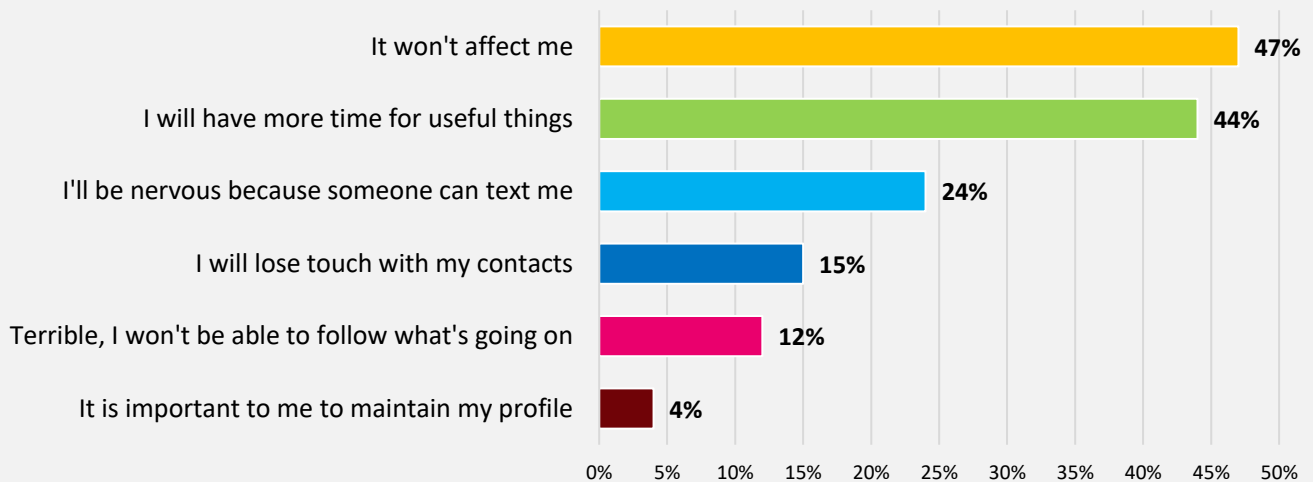
5. Did you know about mobile application that monitors time you spend on the Internet?



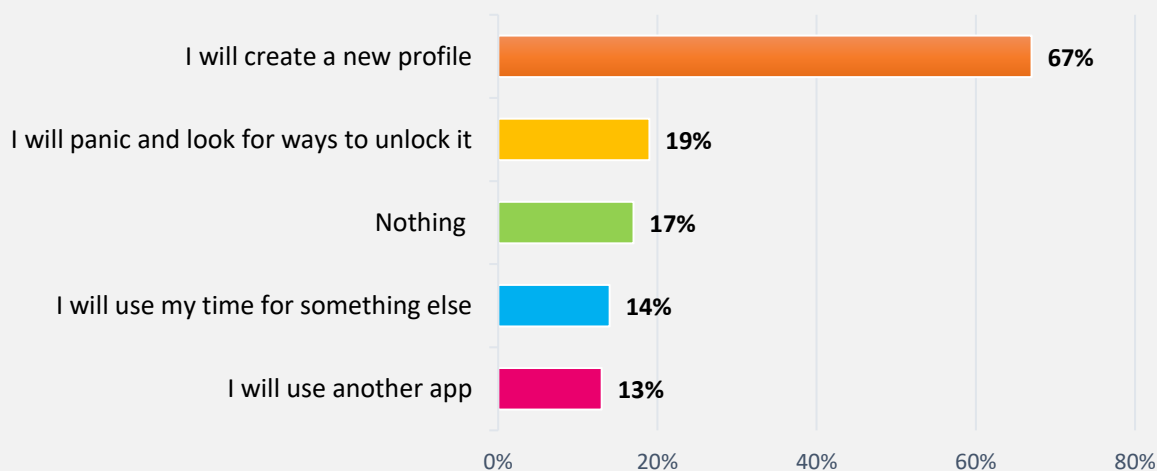
6. Can you tell fake news from real news?



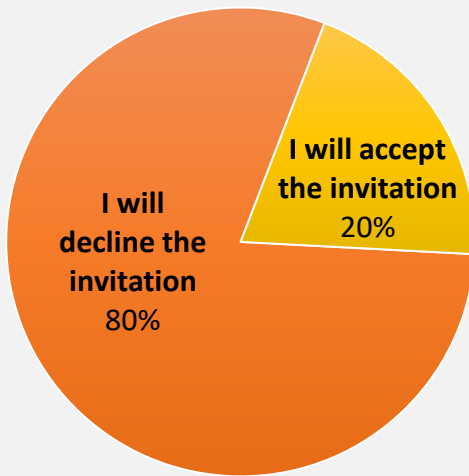
7. How will a day without internet access affect you?



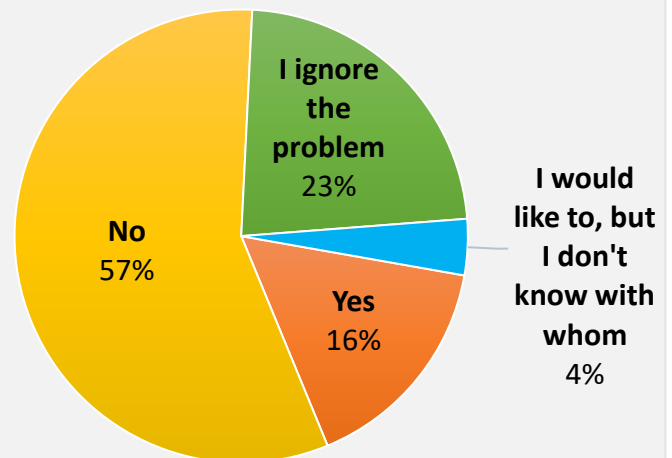
8. What will you do if your social network profile is blocked?



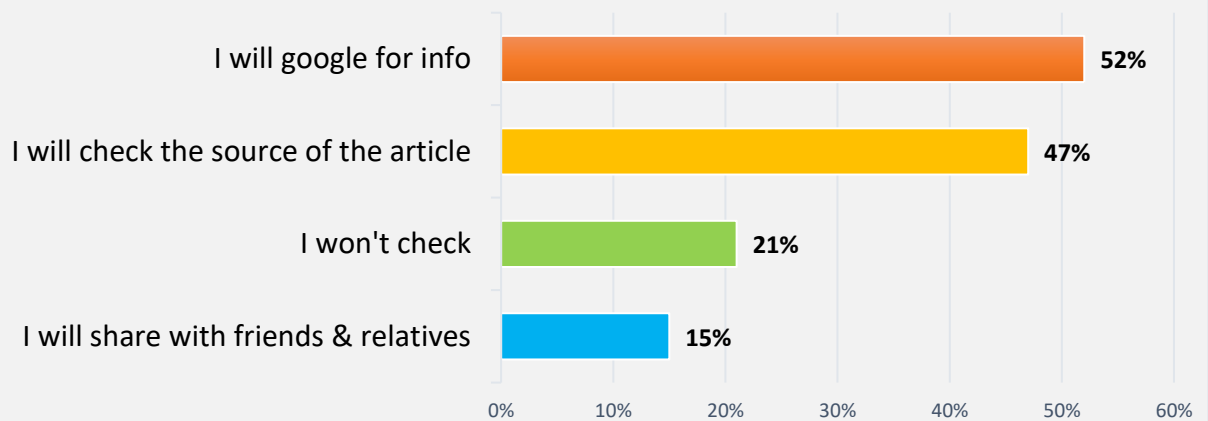
9. If you get an invitation to join a group from a stranger...?



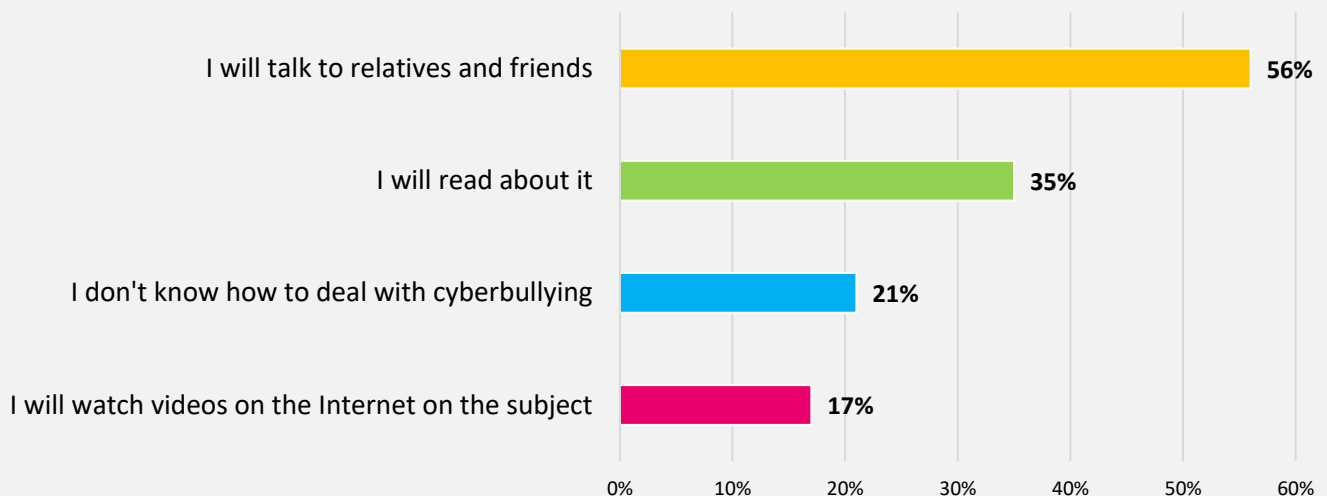
14. Do you share your negative experiences online with anyone?



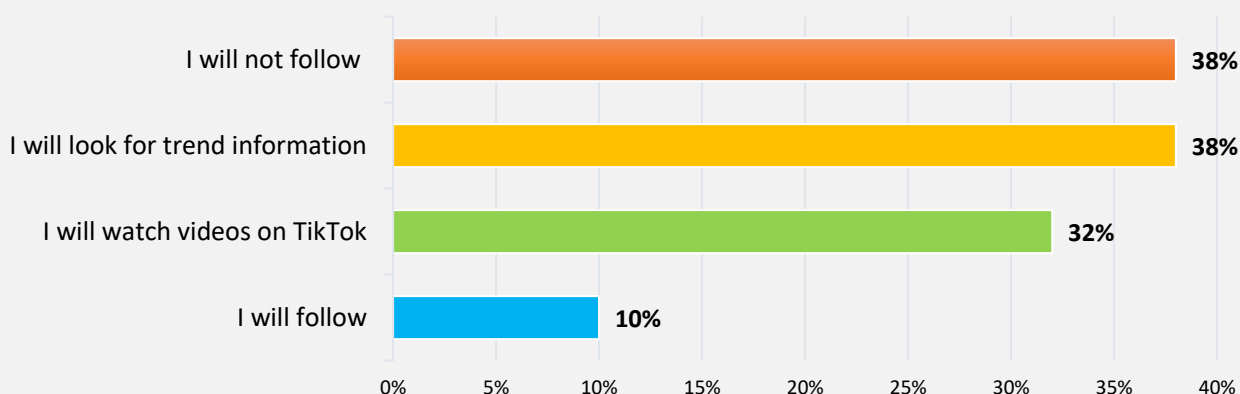
10. You come across an interesting article on the Internet. How will you verify its authenticity?



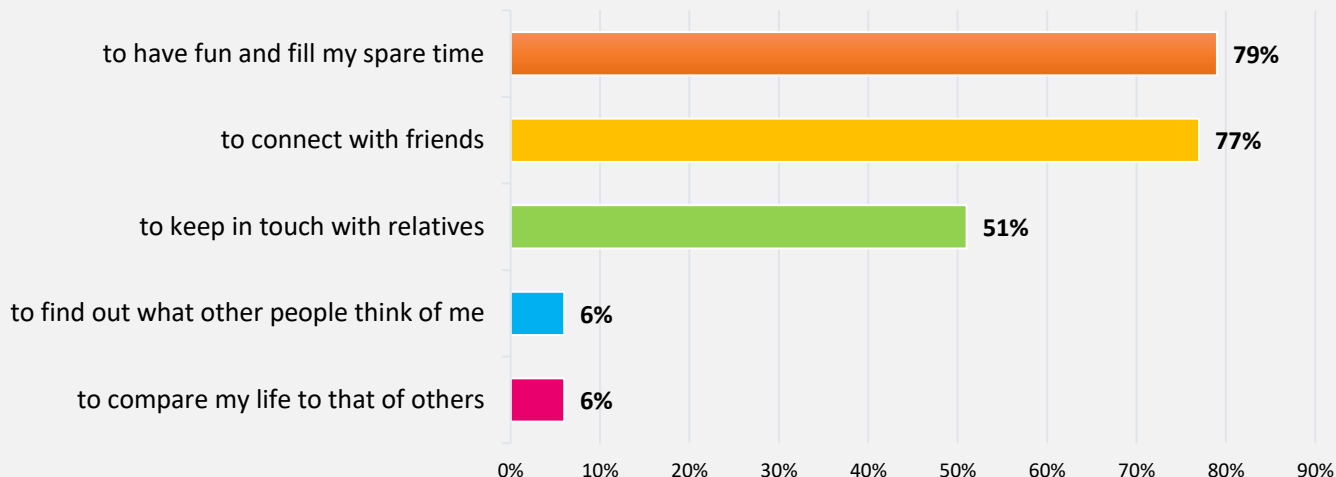
11. What are your ways of dealing with cyberbullying?



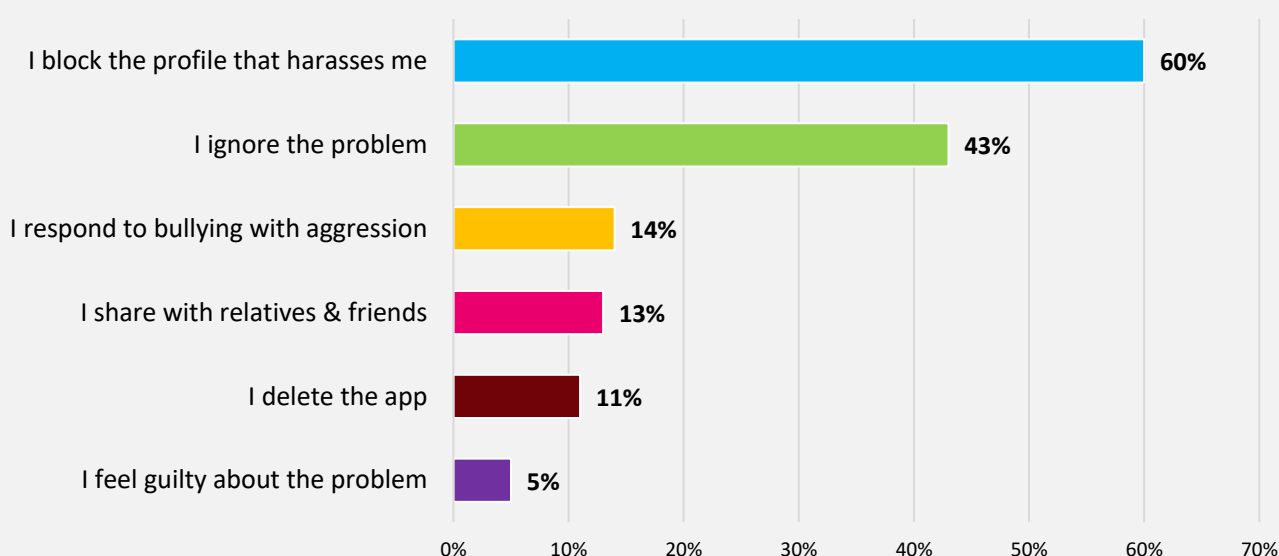
12. If a friend suggested you follow a popular trend...?



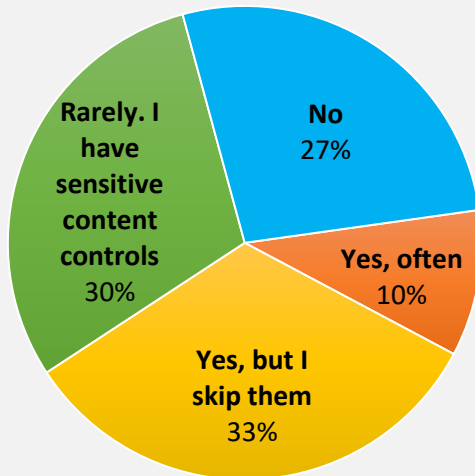
13. You use social networks because...?



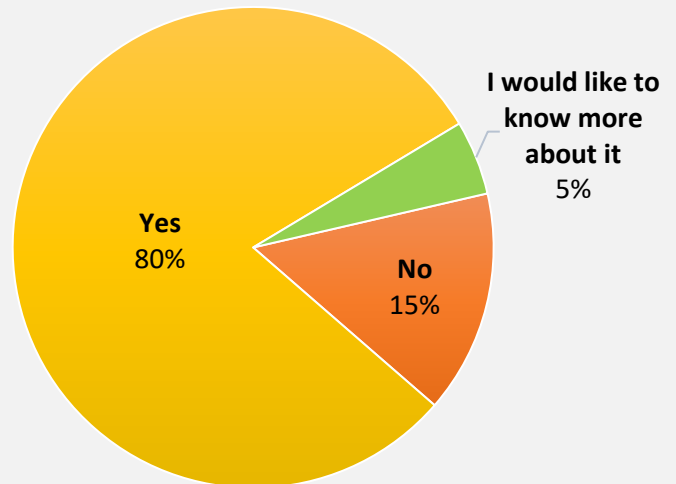
15. How do you deal with bullying on social media?



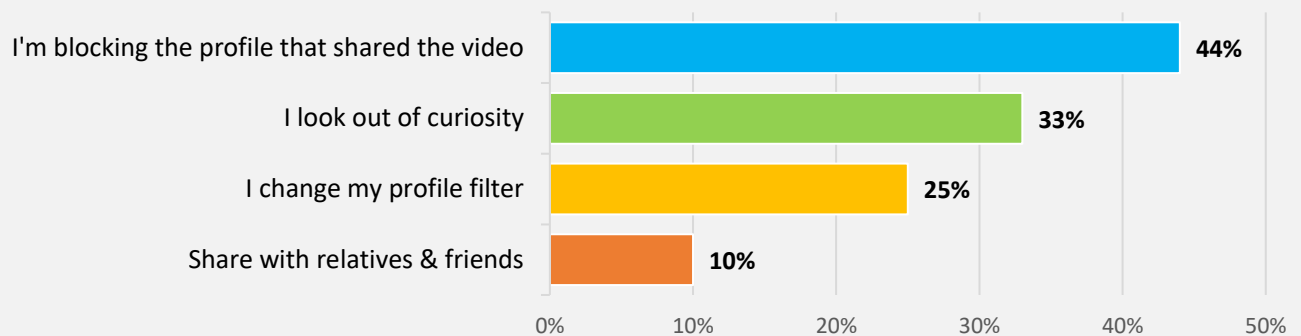
16. Have you come across videos with "sensitive content"?



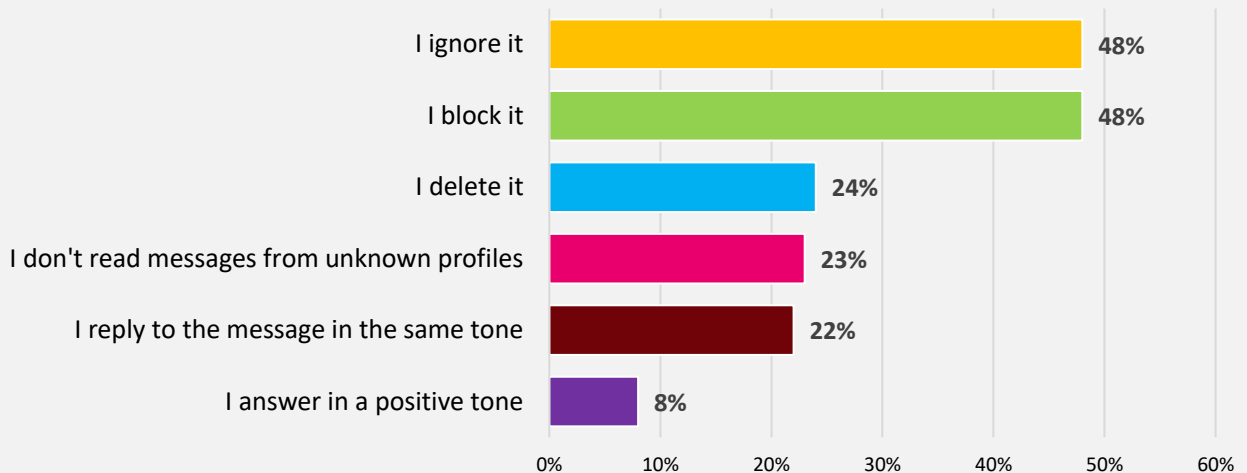
20. Do you know what is misuse of personal and/or financial data?



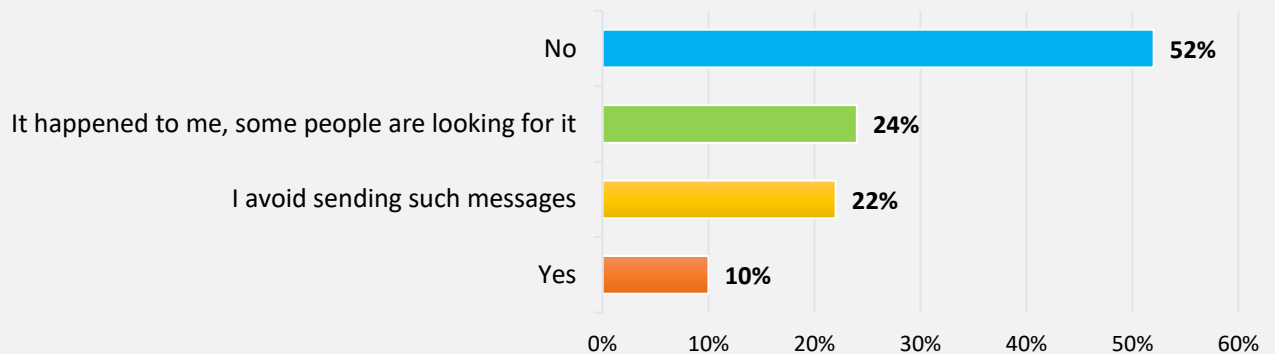
17. How do you protect yourself from videos with "sensitive content" on your social network?



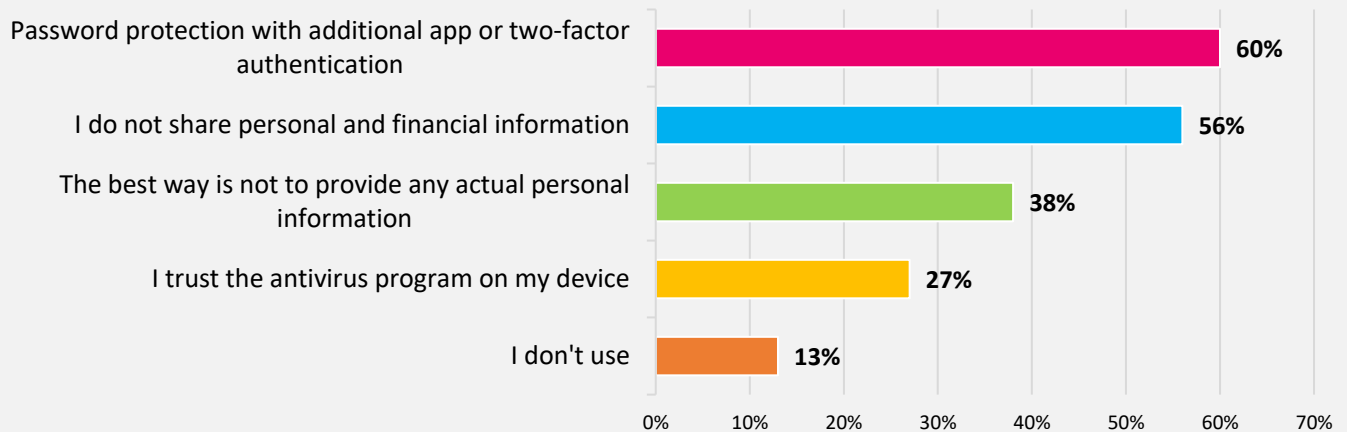
18. When you receive a message with hate language, you...?



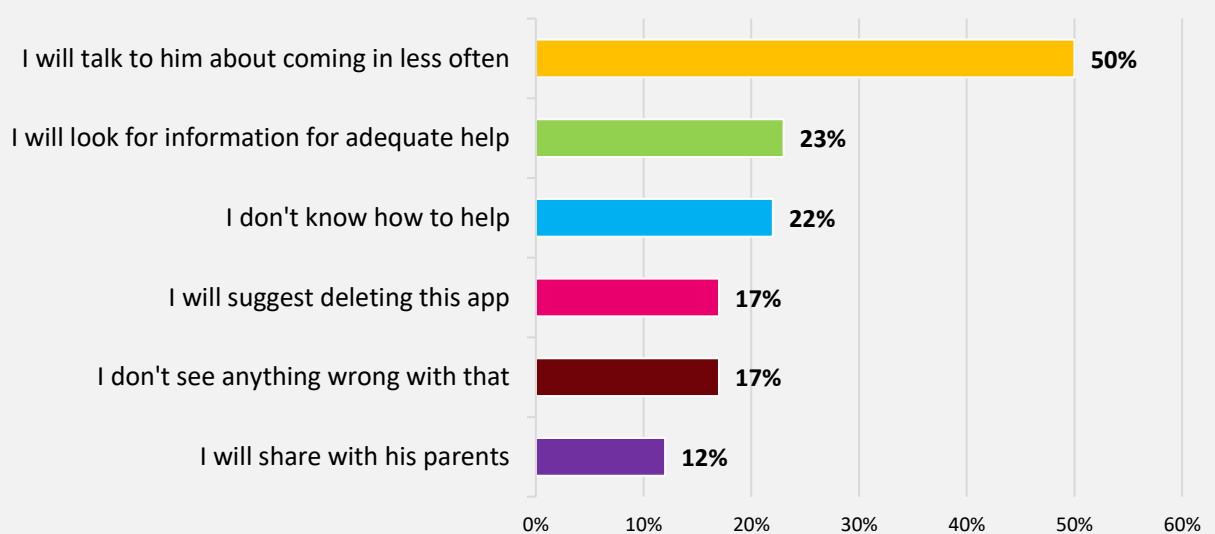
19. Have you personally sent such messages?



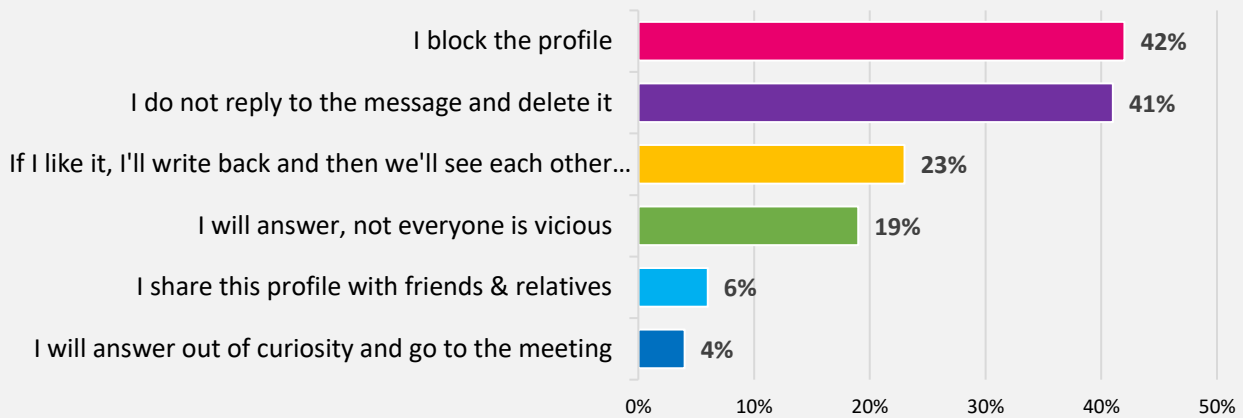
21. What methods of protection against misuse of personal and/or financial data do you know?



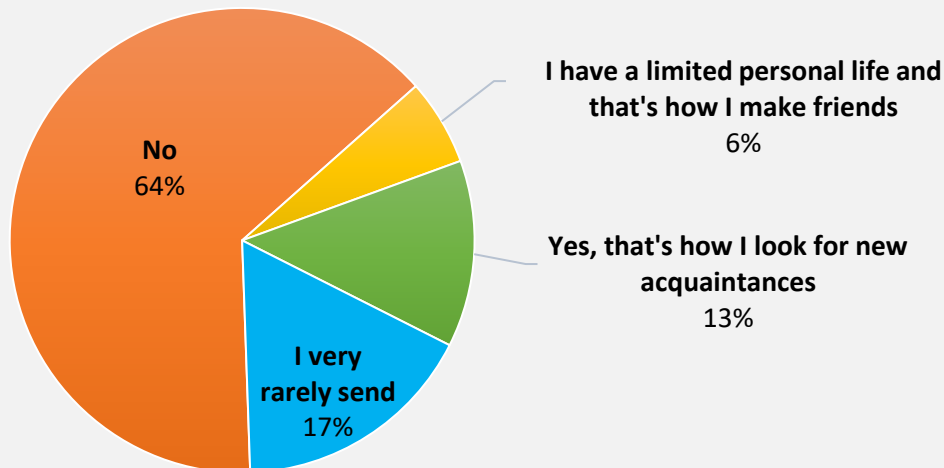
22. If you find out that your friend has an addiction to social networks, how will you help him/ her?



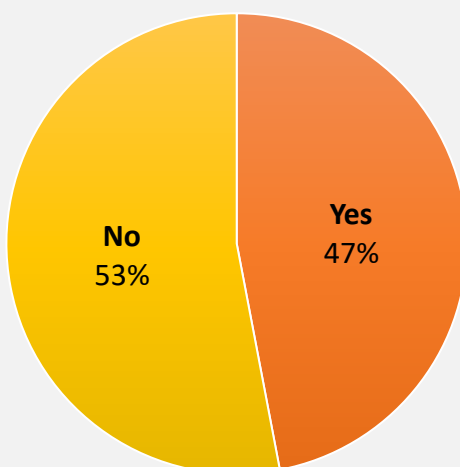
23. How will you protect yourself if an unknown profile writes to you and asks to meet you?



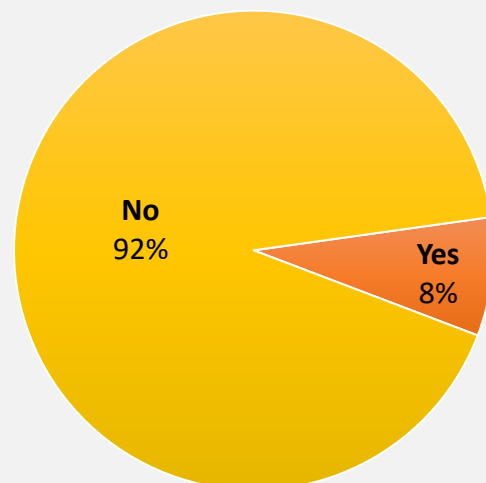
24. Do you personally send such invitations?



25. Have you ever received provocative photos?



26. Have you ever sent provocative photos?



2. NORTH MACEDONIA

The survey in North Macedonia was initiated in March – April 2023 by the partner organization “Mother Teresa” University of Skopje, North Macedonia. The sample involved **30 respondents** selected from schools and a university in the city of Skopje. The respondent’s characteristics are as follows:

- ✓ **Age:** Around 23% of the respondents were in the age group 14 to 18 years old. The rest of the young people - around 77 % - were in the age group 19-29 years old. The age distribution corresponded to the purpose of the survey since the respondents are most active in social networks and are particularly exposed to risks.
- ✓ **Gender:** Young people of both sexes participated in the survey without pre-selection according to gender. In the current survey the distribution between male and female is 47% (14 boys) and 53% (16 girls).
- ✓ **Social status:** All the respondents are students. That allows to objectively see the attitudes of the most vulnerable target group regarding methods of protection in social networks.

QUESTION №1: How do you prefer to communicate with your peers? It is interesting fact that 70% of the respondents prefer live communication with their peers. Around 27% prefer online form of contact with their friends and only 3% have no preferences and would use both ways to communicate. A comparative analysis of the answers to this question and the inclusion of the gender indicator shows that there is no difference between both sexes in communication preferences.

QUESTION №2: When you are on vacation, is it mandatory for you to have internet? The answers to this question are impressive, because 75% of the respondents prefer to have Internet during their vacation, which respectively gives information about the lack of skills to disconnect from social networks and the need to be constantly informed. This is somehow in contrast to the answers to the previous question where most respondents answered that they prefer live communication with their peers. Only 25% of the respondents said that they don’t need internet during their vacation. There are no gender specific differences in the answers to this question.

QUESTION №3: Do you think there are things on the Internet that can harm you? It is interesting that around 73% of the respondents know about the risks and harms of online media and, respectively, from the previous questions,

actively use social networks. The fact that 27% do not know or ignore the risks in the networks is worrying. In a comparative analysis with the gender indicator, the results provide information that there are no gender related differences.

QUESTION №4: Which social media protection methods do you know? Here, the most recognizable method to protect against risks in social networks is doubt and mistrust of information that is published on the Internet and social networks – this includes around 33% of the respondents. A common answer by 66% of the respondents include not providing personal information, hiding their real name and personal control over information. Around 27% of the respondents check if they have mutual friend with stranger who sent them a friend request and around 23% do not accept friend requests from strangers. Around 20% of all the respondents admit that they are not aware about any protection method from the risks and harms of internet. The results of this question indicate some familiarity and awareness among young people about protecting themselves from the risks in social networks but still there are some serious gaps in their knowledge and skills. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №5: Did you know that there is a mobile application (App) that monitors how much time you spend on the Internet? Around 67% of respondents know about such mobile application, and only 10% are not aware about it. Around 23% of the respondents do not care about such application indicating they would not use it which speaks of a distortion of personal judgment to protect against misuse of time on the Internet. It can be concluded that young people rely on their own personal control over the time spent or that they do not like to be limited. No matter of their age most of the respondents are uncritical to the time they spent online.

QUESTION №6: Can you spot a fake (fake news) from real news? The answer here is optimistic because 71% claim that they can distinguish fake news from real ones. Worryingly, 9% share that they wouldn't be able to distinguish fake from real news and 20% ignore the truth of the news which indicate the lack of knowledge and need of further training of specific skills in young people.

QUESTION №7: How will a day without internet access affect you? Access to the Internet is not so important for almost 73% of the respondents, who claim that a day without the Internet will not affect them and that they will have more

time for useful things. The rest of the respondents are not keen on losing the internet connection because of:

- ☑ 50% say they will lose the touch with their contacts and will not be able to communicate with them;
- ☑ 10% of the respondents are worried for missing the news and trends they follow.
- ☑ Looking at the results by gender there are no significant differences in the answers given by the respondents.
- ☑ **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №8: What will you do if your social network account is blocked? To this question, there are two prevailing answers:

- ☑ 30% of the respondents will create a new profile on the social network and 30% will panic and look for ways to unblock it. Using another app is the answer given by 23% of the respondents. This behavior indicate dependence on their activity and the attention they receive online – a possible reason for limiting social live contacts and voluntary social isolation. The degree of importance of the social network profile do not depends on gender in these results, indicating that both sexes are active on the Internet and undertake many social network activities.
- ☑ It is interesting that around 30% of the surveyed boys and girls answer that they would do nothing (20%) and they would spend the time for social media for something else (10%).
- ☑ **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №9: If you get an invitation to join a group from a stranger, what will you do? This question responds to the knowledge and skills of young people to protect themselves from the risks in social networks and to what extent they can do it. Around 50% of the respondents would refuse the invitation, which is probably based on a negative previous experience among the youth. It is worrying that around 47% of the respondent would accept the invitation. Here again, there is a gender difference in social media activity, expectations and

willingness to take risks - larger percent of girls (69%) will accept the invitation from a stranger compared to boys (23%) which obviously makes girls more vulnerable in this section.

QUESTION №10: You come across an interesting article on the Internet. How will you verify its authenticity? Predominance of the answers to this question are related to checking on the Internet the validity of the article and its source in Google. It means that there is some level of critical thinking among children and young people who participated in the survey. Only around 10% of the respondents will trust the information without any doubt which is a risky behavior. Around 10% will turn to friends and relatives for advice which means that they need the authority of the more experienced and trusted people. Analysis of critical thinking doesn't show significant differences in both genders as opinion and possible behavior. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №11: What are your ways of dealing with cyberbullying? Most of the respondents (37%) have answered to this question with "other". This gives a clear message that the youth lack knowledge, skills and concrete information to deal with cyberbullying and how to deal with it. This is also seen in 33%, who will look for information on the Internet and 17% of the surveyed who will watch a video about how to manage with cyberbullying. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №12: If a friend suggested you follow a popular trend, what would you do? The answers to this question show a criticality towards the information that is offered on internet. According to the answers, most of the surveyed young people will not follow blindly any new trend (50%) and will look for information about the trend in advance (another 33%) – this is altogether 83% of all the respondents. Around only 10% of the responses given by youth provide information on possible risky behavior since they show a readiness to follow a certain trend without preliminary research. Part of the respondents (13%) would

watch TikTok videos about the trend, which means that they are ready to accept the idea of following. The level of critical thinking and the tendency to risky behavior is not influenced by gender. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №13: You use social networks because...?: To this question, young people mainly answered that they use social networks for fun in their free time (43%) and to connect with friends and relatives (37% and 30%). A small number of respondents have answered that social networks are a way to find out what others think of them (7%) and to compare their life with those of other people (7%). There are no significant differences in answers between genders. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №14: Do you share your negative experiences online with anyone? Most of the respondents do not share negative experience they had in social networks (47%). Around 27% of all the respondents would share with friends and relatives which is a more active approach. Around 20% would ignore the problem and about 7% don't know who to share the negative experience with. The fact that young people do not share about negative experiences on social networks and ignore the problems is very worrying. These results show that young people are not aware of the real risks and underestimate their effects. Since this is a threat for their mental health it requires serious measures to educate young people with skills and knowledge about protection on the Internet. There are no significant differences in the answers given by gender.

QUESTION №15: How do you deal with bullying on social media? Most of the respondents stated that blocking the profile is the method they use to deal with bullying online (47%). It is worrying that 30% of the respondents would ignore the problem. Only around 10% of the respondents would share with friends and relatives. Deleting the app will be done by 11% of the surveyed. Only around 3% will respond with aggressive behavior which means that these young people are not skilled to manage harassment online. There are no significant differences in

the answers by gender. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №16: Have you come across videos with "sensitive content"? The distribution of videos with sensitive content is a network risk that young people often fall into (43%). Very often these videos are forwarded by friends or posted in groups where youth have easy access. Around 30% rarely come across sensitive content since they have specific sensitive content controls. Around 27% claim that they don't come across such videos. Looking at the results through the gender lens it turned out that there are no significant differences in the answers given.

QUESTION №17: How do you protect yourself from "sensitive content" video on your social network? The leading answer here is blocking the profile - 67% of the respondents. Around 20% state that they will look out of curiosity which could be considered as risky behavior. Changing profile filter is not a popular method because it is mentioned only by one person. Sharing with friends and relatives is stated in only 10 % of the answers. There are no significant differences in the answers given by both genders.

QUESTION №18: When you receive a message with hate language (Hate messages), you...?: There is a sharp edge in responses to this question: around 67% will ignore and block the profile that sends the message, 20% will delete the message and 27% will not read the message if it is from an unknown profile. Around 27% will respond to the message with the same tone which suggests answering to the aggression with aggression and in conclusion – lack of knowledge and skills to manage hate language online. Only 7% would answer with positive tone. Looking at answers given by both genders there are no significant differences. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №19: Have you personally sent such messages? Sending messages with hate speech have been confirmed by 10% of the young people surveyed. On the other hand, half of the respondents (53%) haven't sent such messages,

and around 37% are avoiding doing it. There are no significant differences in the answers given by genders.

QUESTION №20: Do you know what is misuse of personal and/or financial data on the Internet? About 43% of the respondents stated that they are aware of what is misuse of personal and/ or financial data. It is worrying that 37% have no information and 20% are willing to learn more. This means that around 57% of the young people surveyed realize the lack of knowledge about the topic. Considering the active use of the Internet and social networks, online shopping and risks, related to protecting financial data, young people do need additional and more specific information on how to protect their personal data on the Internet.

QUESTION №21: What methods of protection against misuse of personal and/or financial data do you know? Most popular protection method of personal and financial data online among young people surveyed is password protection with additional app and two-factor authentication (around 37% of the answers). Not sharing personal and financial data is mentioned in 27% of the answers and around 7% of the answers mentioned not sharing personal data at all. Antivirus program would be the next method chosen by young people according 7% of the answers. The distribution of the methods according to the answers suggests a relatively good knowledge and skills among most of the young people needed to protect themselves from malicious interference in their personal profiles on social networks. What is worrying is that 33% of the surveyed stated that they do not use any protection method of personal or/ and financial data which indicates gaps in knowledge and skills, needed for safe internet life. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №22: If you find out that your friend has an addiction to social networks, how will you help him? Personal support is readily offered from the young people surveyed including conversation (30%) and advise for deleting the app (27%). Around 26% of the respondents want actively to help and they would look for information how to do it (13%) or share with the parents of the person

affected (13%). Around 20% of the respondents stated that they don't know how to do it. Both groups indicate lack of suitable information and skills about how to help their peer and require education among young people. It is surprising that 10% of the respondents indicate that they don't think addiction is or could be a problem and they claim that there is nothing wrong with dependence on the Internet and social networks. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

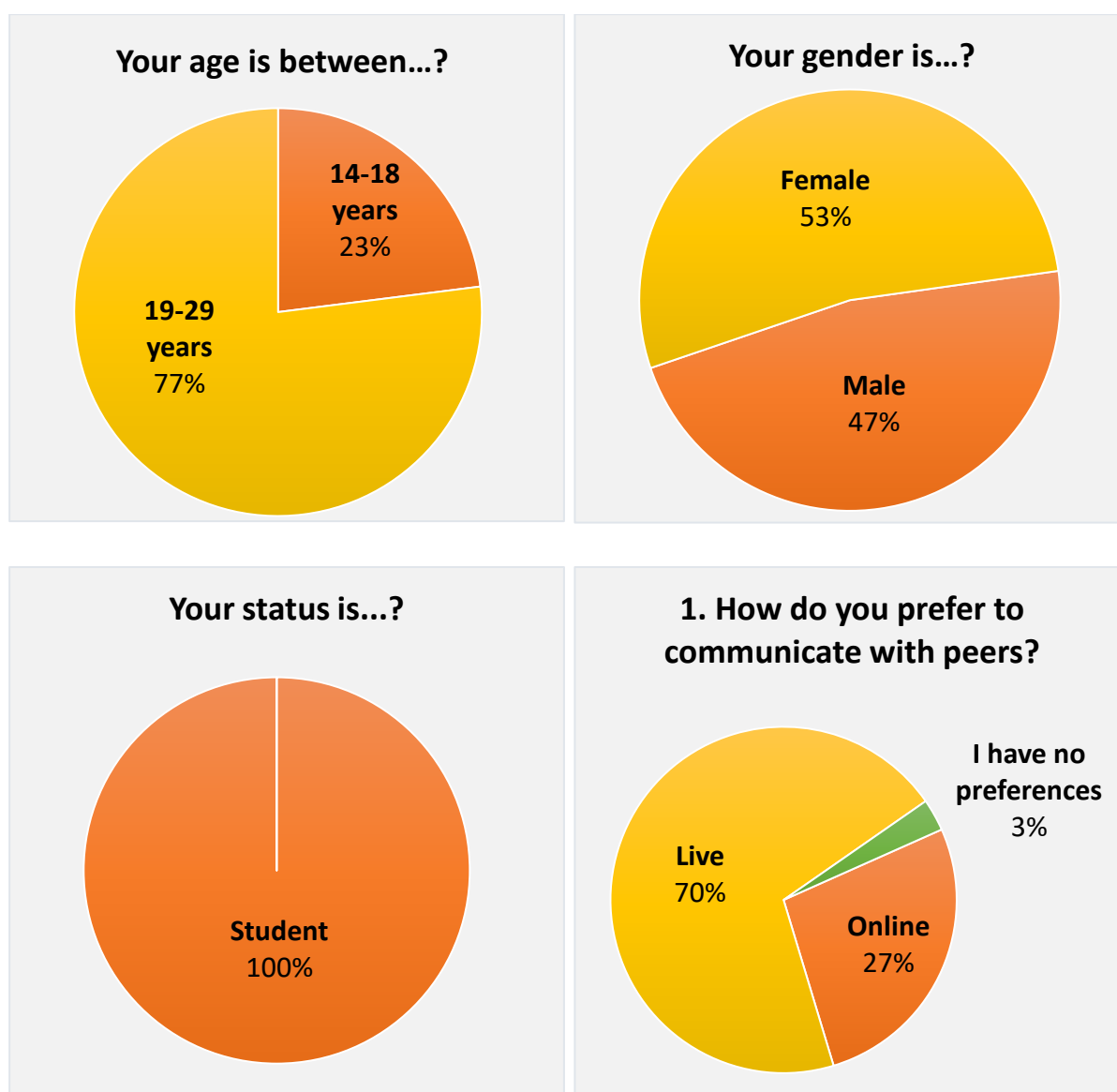
QUESTION №23: How will you protect yourself if an unknown profile writes to you and asks to meet you? Caution among young people is seen in 47% of the cases they will not respond to the message and delete it and in 30% of the cases where they would block the profile. Around 20% of the respondents would communicate and meet in real life with the person and 7% would answer to the message since they don't think there could be a risk for them. It is worrying that part of the respondents would not take any precautions and meet with a stranger in the real life – this is a very risky behavior. Only 7% of the young people surveyed would share with their friends and relatives about the situation. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №24: Do you personally send such invitations? Most of the respondents (63%) deny sending invitations for communication to strangers. surveyed young people answered that they did not send such messages. It is worrying that rest of the respondents do send invitations as an excuse for their limited social life and as a way for finding new friends – a signal, that they are quite addicted to social media and internet and lack normal communication in real life.

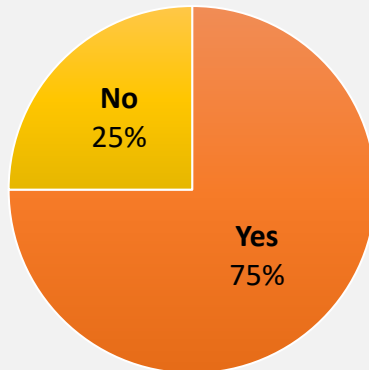
QUESTION №25: Have you received provocative photos? Around 80% of the respondents denied receiving provocative photos, while 20% confirmed such events online. This provides an answer to the extent to which young people in social networks are protected from sensitive and harmful content. There are no significant differences between boys and girls.

QUESTION №26: Have you sent provocative photos that you wouldn't post on the Internet? Here the answers are almost unequivocal: 87% of the respondents claim that they did not send provocative photos, while 13% confirm that they did. Broken down by gender, there is a slight difference in favor of the boys who sent provocative photos.

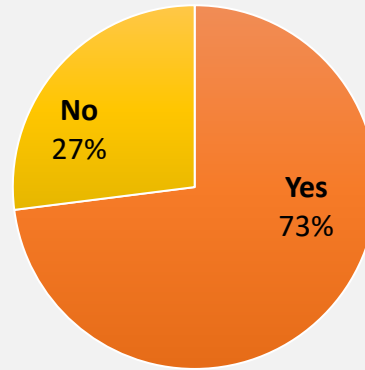
VISUAL REPRESENTATION OF SURVEY RESULTS IN NORTH MACEDONIA:



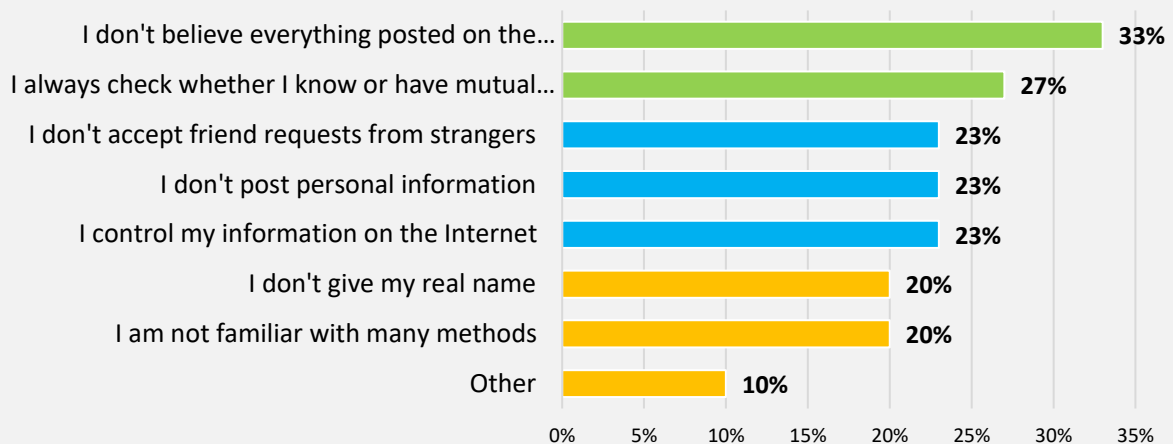
2. When you are on vacation, is it mandatory for you to have internet?



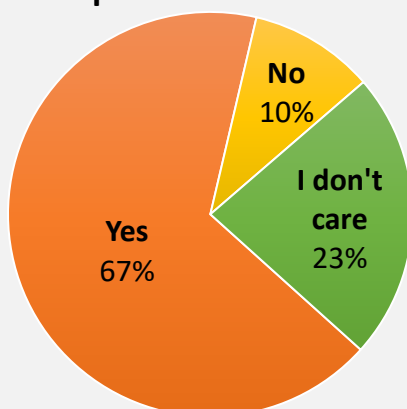
3. Do you think there are things on the internet that can harm you?



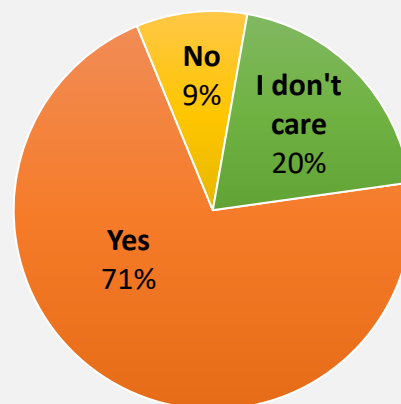
4. Which social media protection methods do you know...?



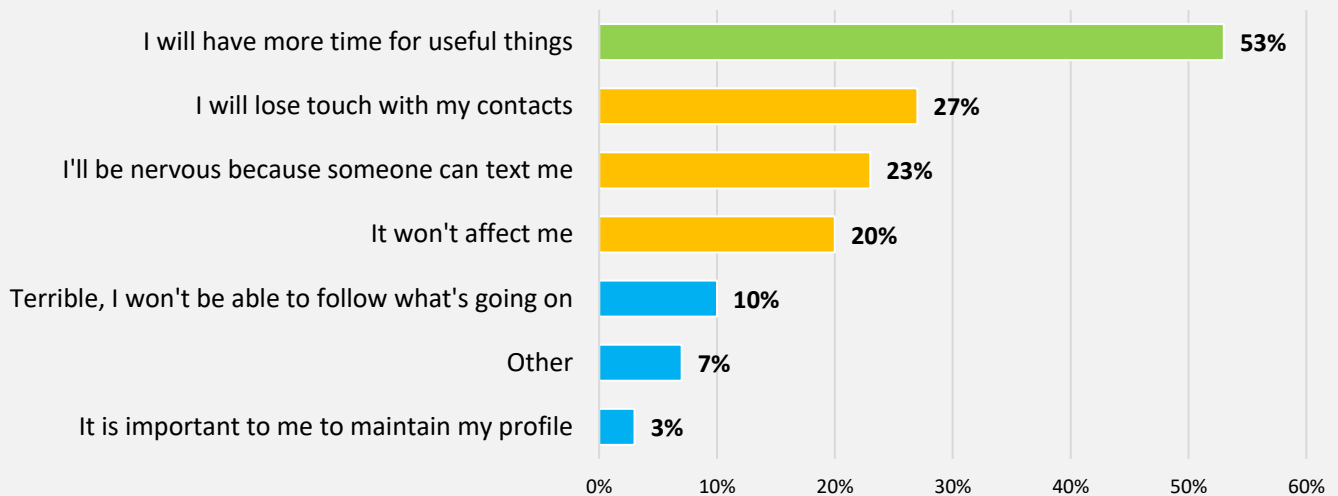
5. Did you know about an app that monitors time you spend on Internet?



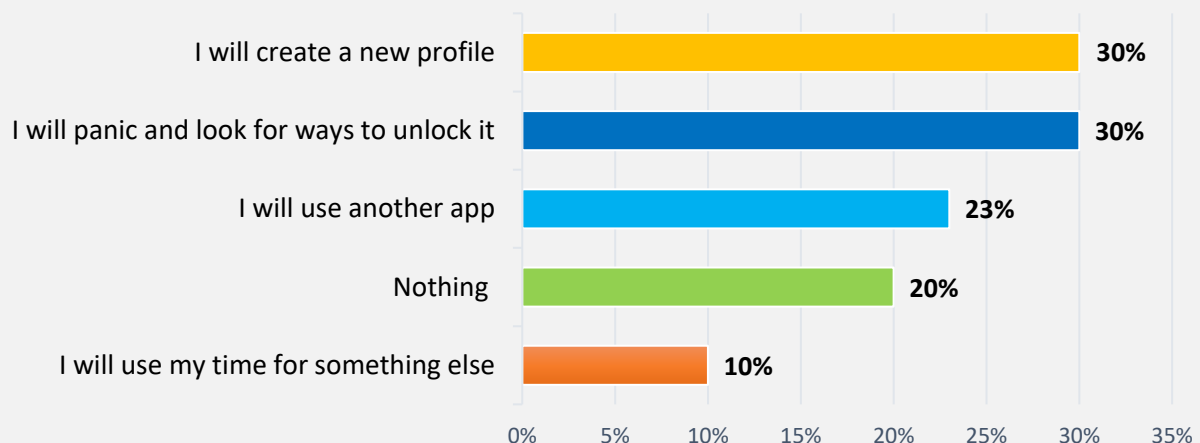
6. Can you tell fake news from real news?



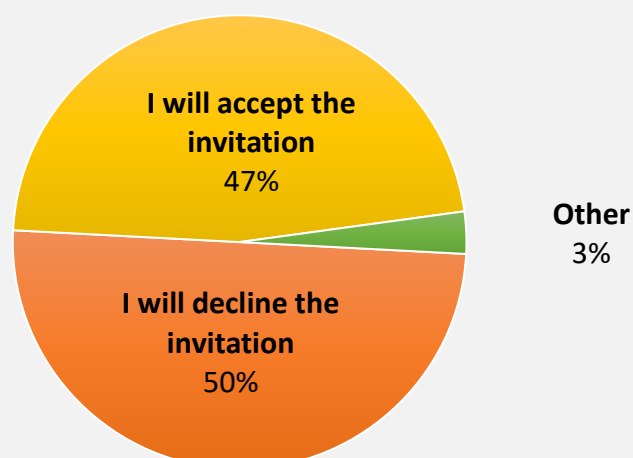
7. How will a day without internet access affect you?



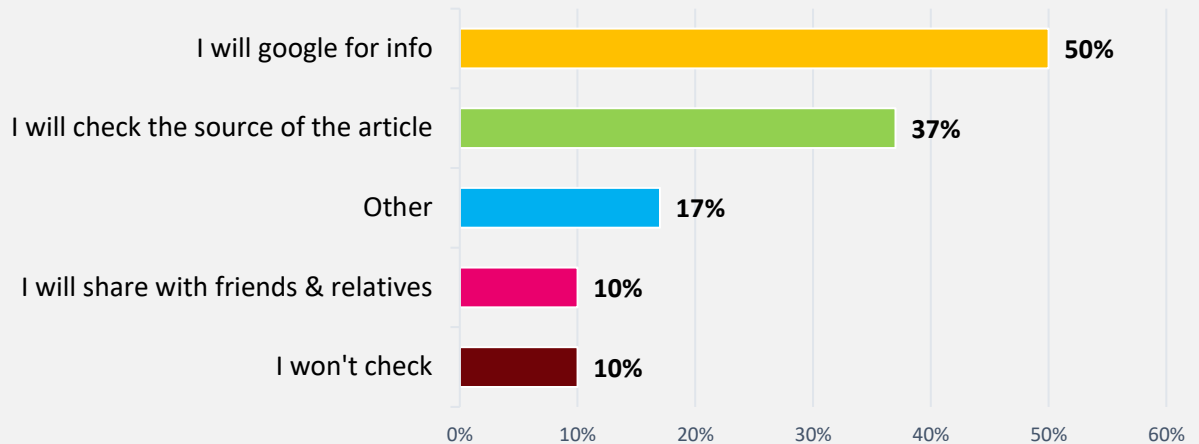
8. What will you do if your social network profile is blocked?



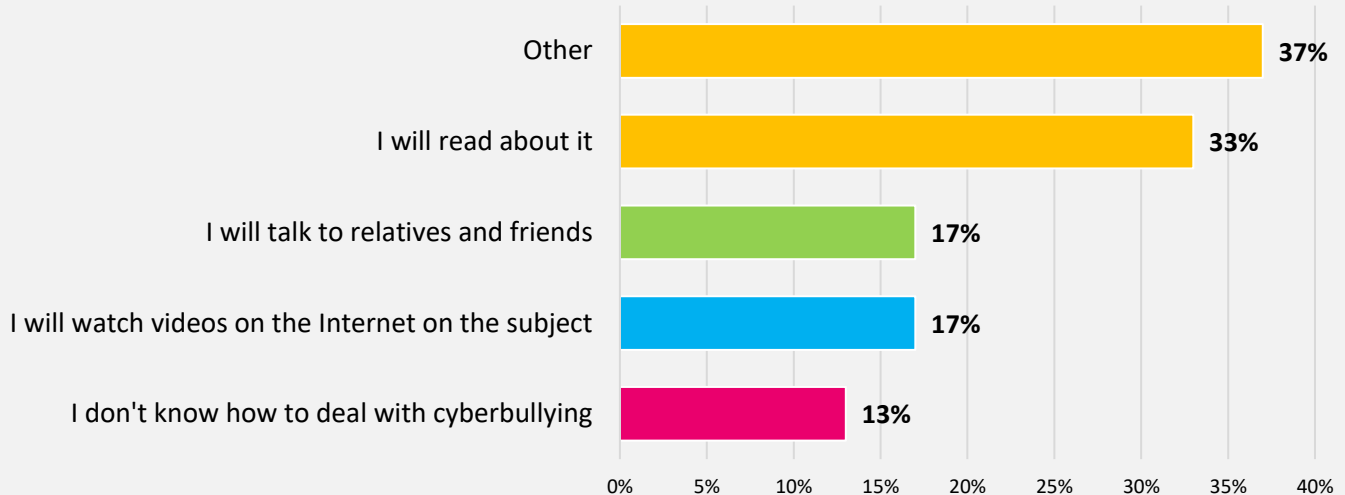
9. If you get an invitation to join a group from a stranger...?



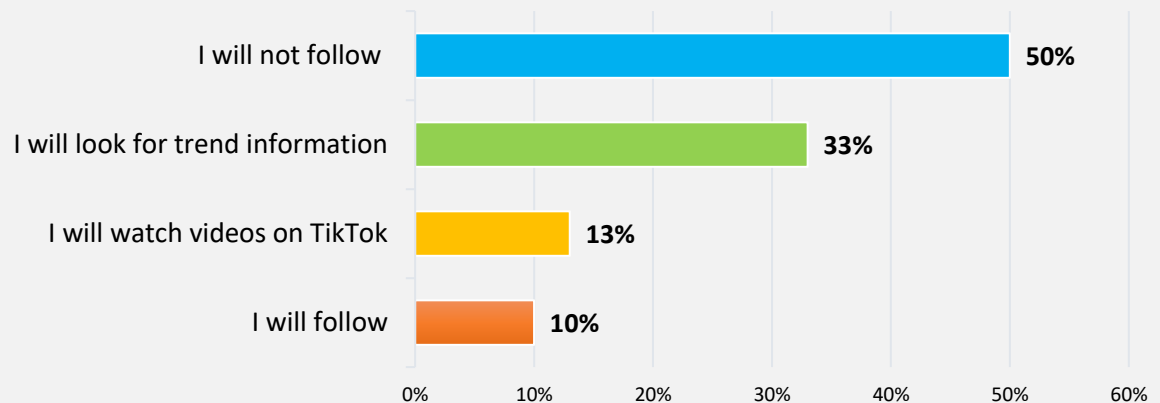
10. You come across an interesting article on the Internet. How will you verify its authenticity?



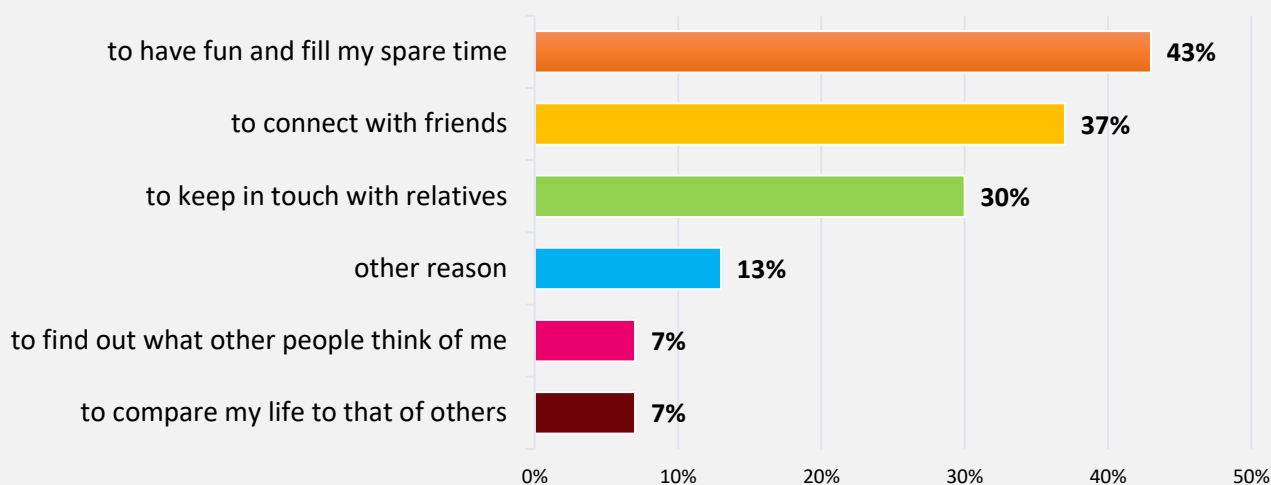
11. What are your ways of dealing with cyberbullying?



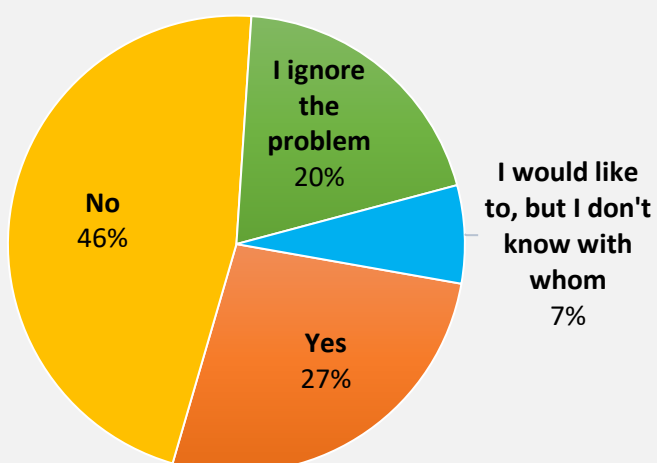
12. If a friend suggested you follow a popular trend, what would you do?



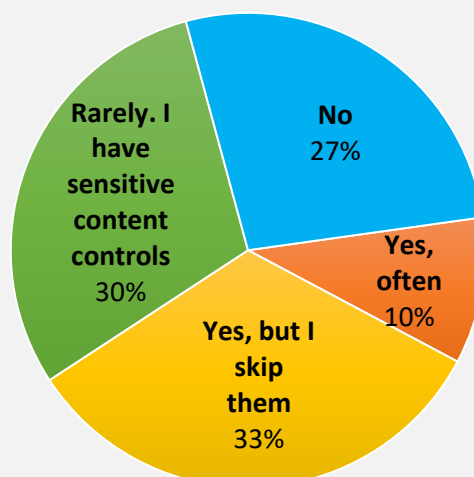
13. You use social networks because...?



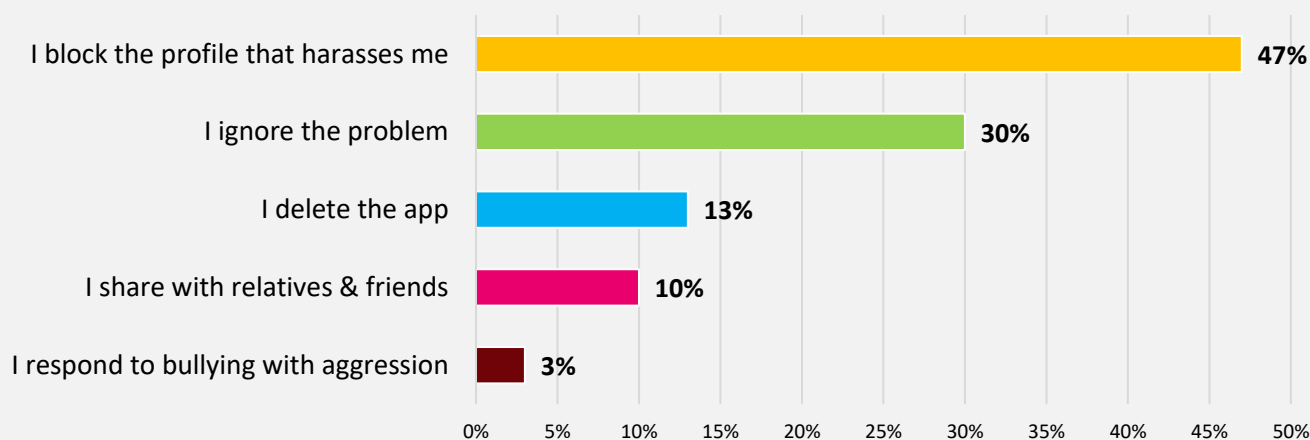
14. Do you share your negative experiences online with anyone?



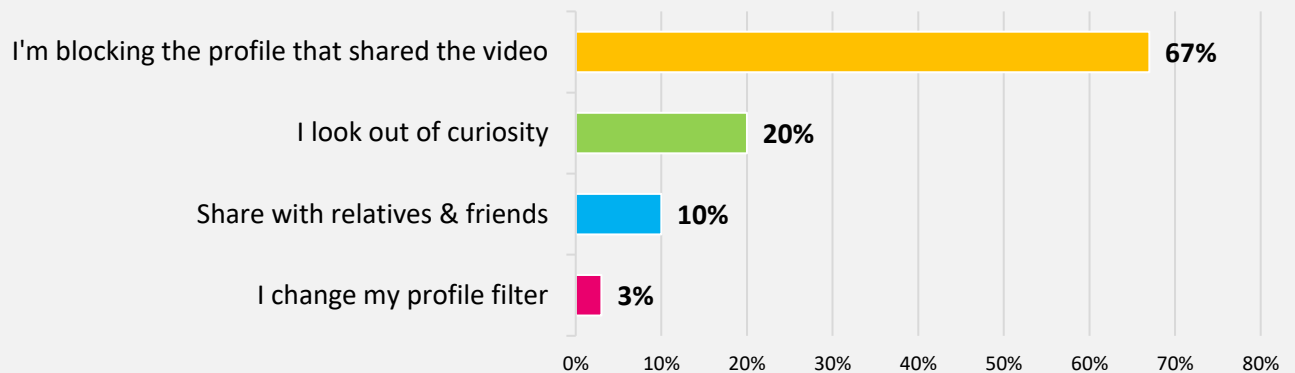
16. Have you come across videos with "sensitive content"?



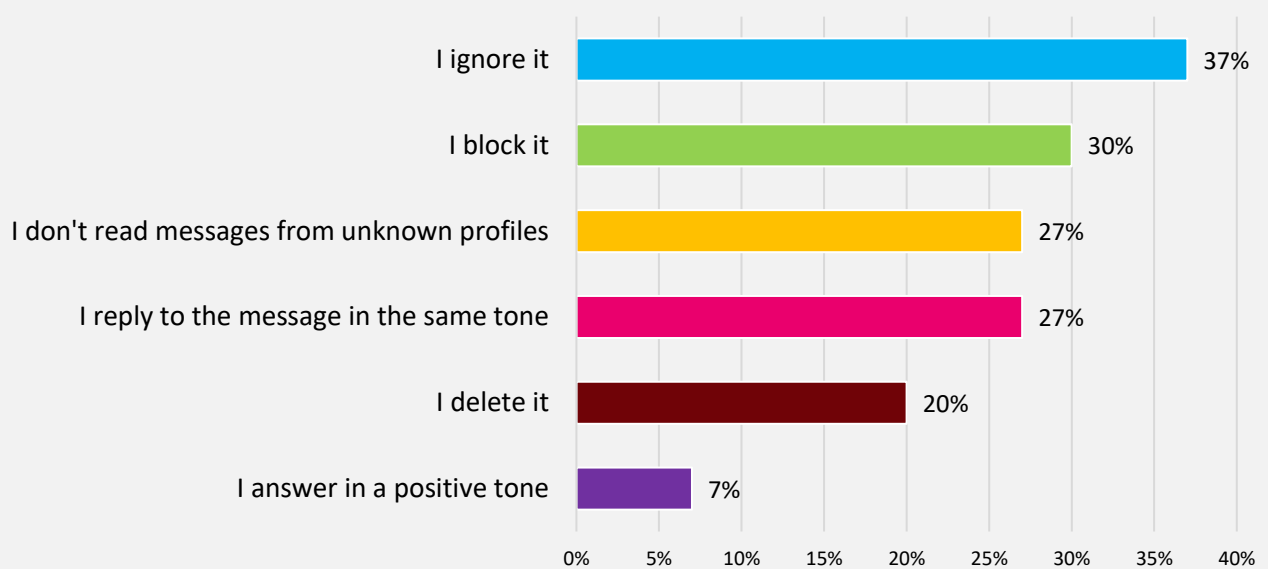
15. How do you deal with bullying on social media?



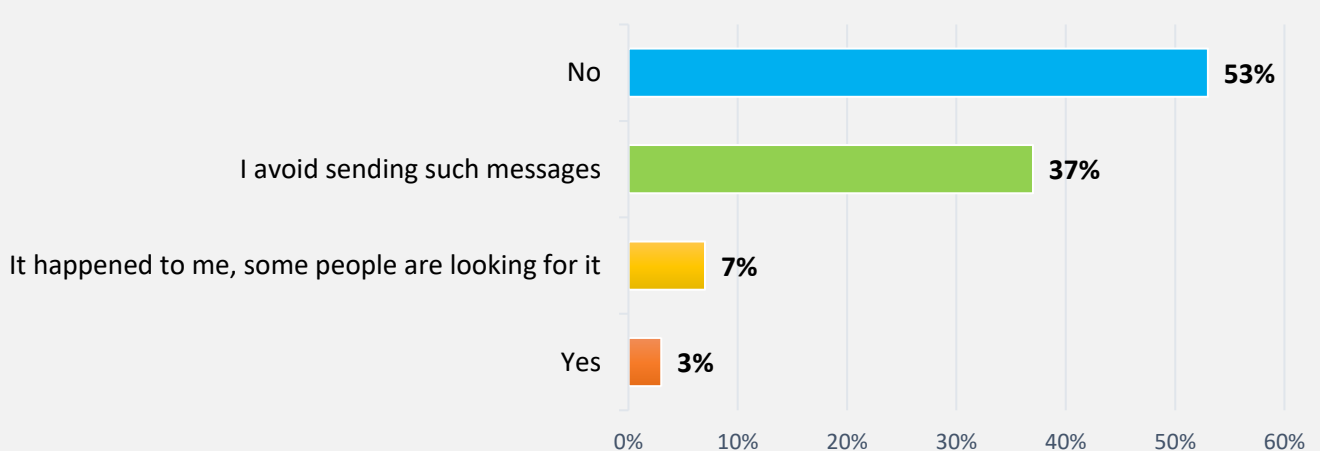
17. How do you protect yourself from videos with "sensitive content" on your social network?



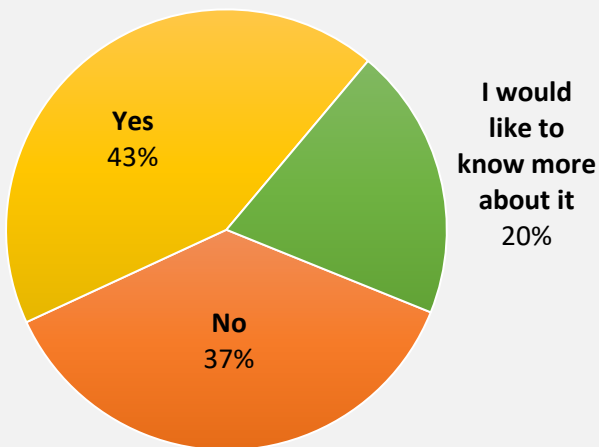
18. When you receive a message with hate language, you...?



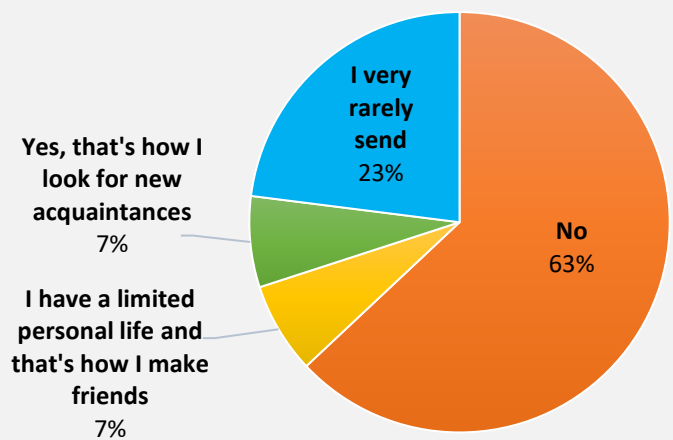
19. Have you personally sent such messages?



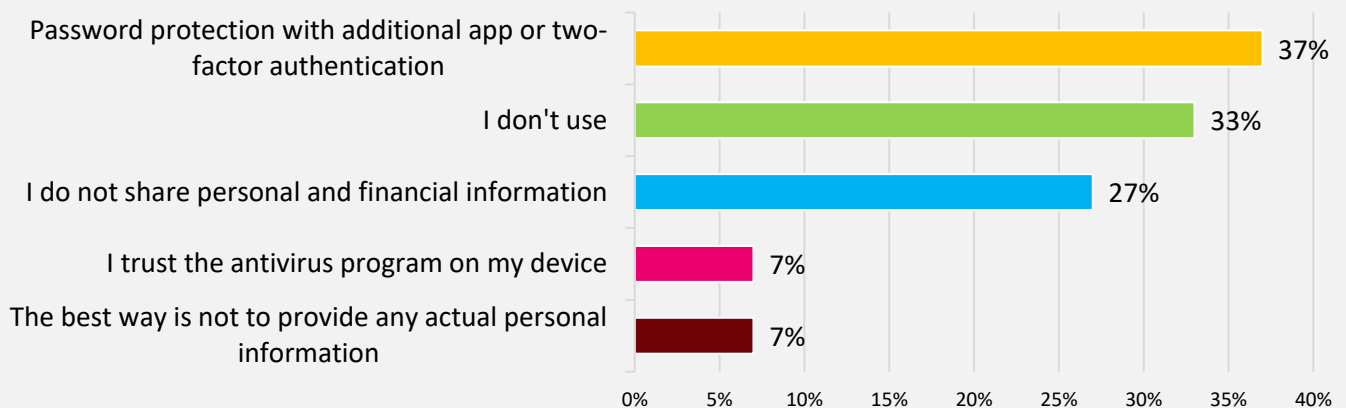
20. Do you know what is misuse of personal and/or financial data on the Internet?



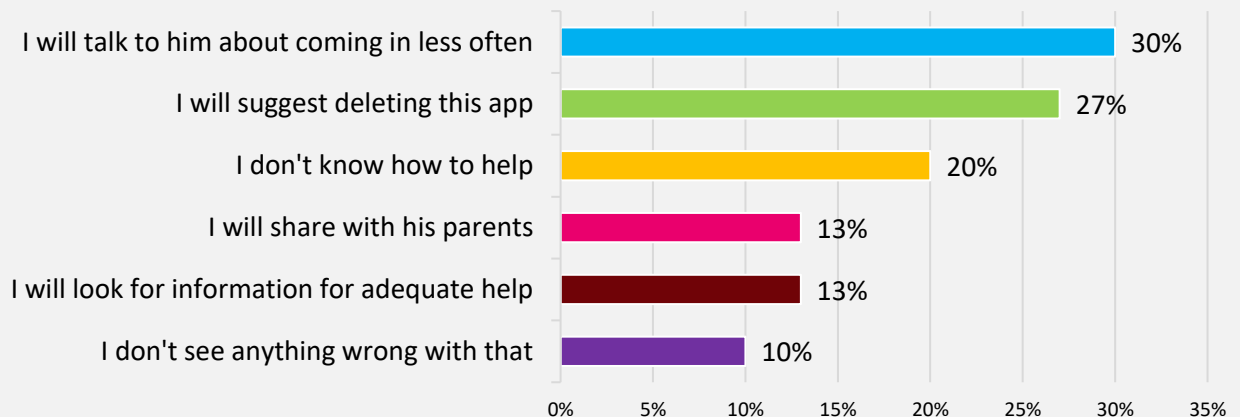
24. Do you personally send meeting invitations to strangers?



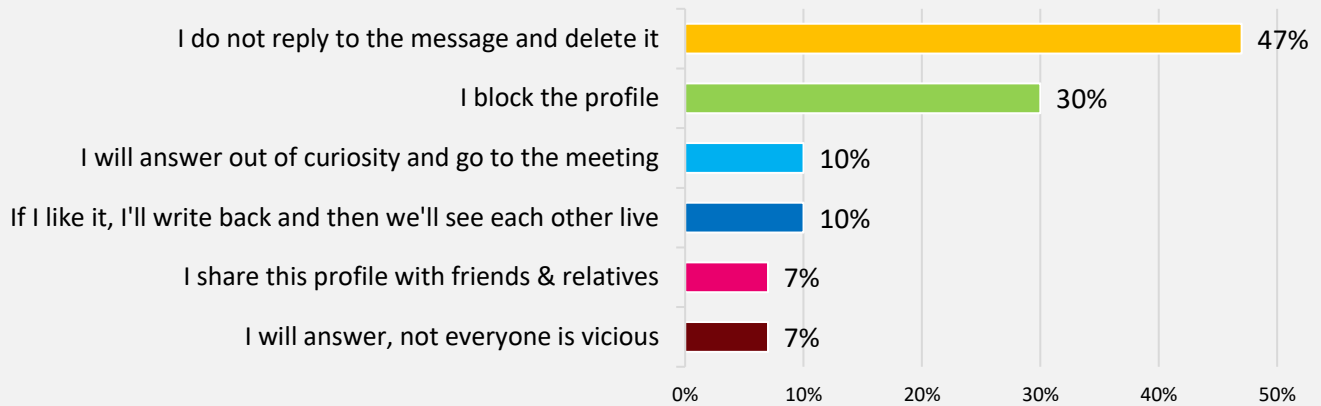
21. What methods of protection against misuse of personal and/or financial data do you know?



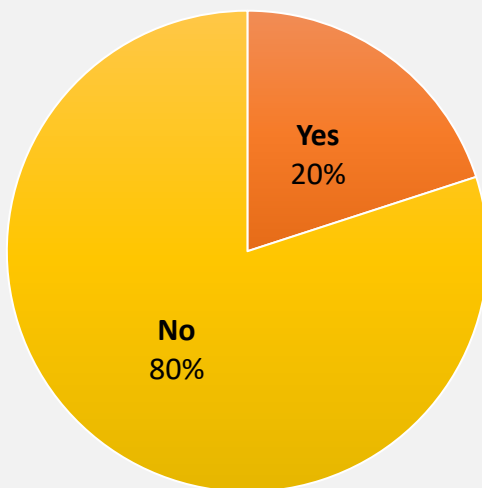
22. If you find out that your friend has an addiction to social networks, how will you help him/ her?



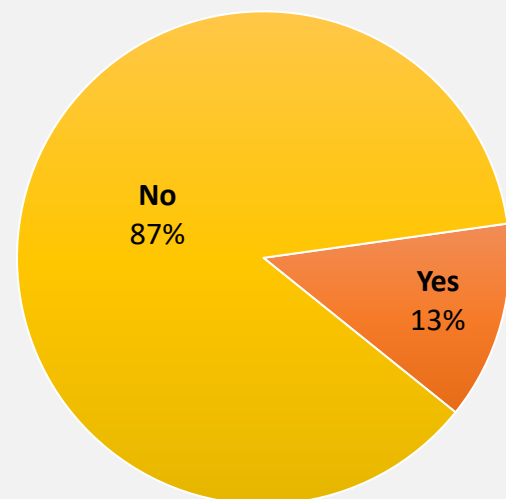
23. How will you protect yourself if an unknown profile writes to you and asks to meet you?



25. Have you ever received provocative photos?



26. Have you sent provocative photos that you wouldn't post on the internet?



3. POLAND

The survey in Poland was initiated in February and March 2023 by the partner organization Urban Forum Association. The sample involved **41 respondents**. The range of respondents was not influenced by gender, race, ethnicity or education. The respondent's characteristics are as follows:

- ☑ **Age:** Around 49% of the respondents were in the age group 14 to 18 years old. The rest of the young people - around 49 % - were in the age group 19-29 years old. The age distribution corresponded to the purpose of the survey since there is a balance between the two groups of respondents.
- ☑ **Gender:** Young people of both sexes participated in the survey without pre-selection according to gender. In the current survey the distribution between male and female is balanced - 46% of the respondents were boys and 54% girls.
- ☑ **Social status:** Most of the respondents are students (73%) and 27% are working. That allows to objectively see the attitudes of the most vulnerable target group regarding methods of protection in social networks.

QUESTION №1: How do you prefer to communicate with your peers? It is interesting fact that 49% of the respondents prefer live communication with their peers. Around 15% prefer online form of contact with their friends and 36% have no preferences and would use both ways to communicate. These results indicate that although young people spend much time on Internet and social media, they prefer to communicate with their peers live. A comparative analysis of the answers to this question and the inclusion of the gender indicator shows that there is no significant difference between both sexes in communication preferences.

QUESTION №2: When you are on vacation, is it mandatory for you to have internet? This question gives information about the lack of skills to disconnect from social networks and the need to be constantly informed. Around 55% of the respondents prefer to have the Internet during their vacation, while 45% don't need it. This corresponds with the answers to the previous question where most respondents answered that they prefer live communication with their peers. There are no gender specific differences in the answers to this question.

QUESTION №3: Do you think there are things on the Internet that can harm you? It is interesting that around 78% of the respondents know about the risks and harms of online media and, respectively, from the previous questions, actively use social networks. The fact that 22% do not know or ignore the risks in the networks is worrying. In a comparative analysis with the gender indicator, the results provide information that there are slight gender related differences – girls are more cautious and 19 claim that there are dangers online, versus 12 boys, who also believe that there is nothing harmful in social media more than girls (6 boys vs. 3 girls).

QUESTION №4: Which social media protection methods do you know? The answers to these questions showed that young people are aware of many social media protection methods. Only 4,9% stated that they don't know any methods of protection. Most respondents - 51,2% don't accept friends request from strangers, 39% always check whether they know or have mutual acquaintances with the person who sent them an invitation. Around 39% also don't post personal information, don't share their real name (34%) and control their personal information online (32%). Around 24% of the respondents don't believe everything posted on the Internet. Around 5% of all the respondents admit that they are not aware about any protection method from the risks and harms of internet. The results of this question indicate some familiarity and awareness among young people about protecting themselves from the risks in social networks but still there are some serious gaps in their knowledge and skills. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №5: Did you know that there is a mobile application (App) that monitors how much time you spend on the Internet? Around 59% of respondents know about such mobile application, while around 24% have no idea about it. It is worrying that around 17% don't care which means that they reject control over their time online. This could also mean that there is a distortion of personal judgment to protect against misuse of time on the Internet. It can be concluded that young people rely on their own personal control over the time spent or that they do not like to be limited. It is a bit surprising that the respondents in the age group 19-29 years are more aware of

this kind of software than the respondents, in the age group 14-18 years (78% vs. 62%), probably because of their longer experience online. No matter of their age most of the respondents are uncritical to the time they spent online no matter what their gender is as well.

QUESTION №6: Can you spot a fake (fake news) from real news? The answer of 49% of the respondents is that they think they can distinguish fake news from real ones. Referring to the above question about methods, knowledge about fake news among youth is based more on accumulated experience than on learned and validated information. Worryingly, 32% share that they wouldn't be able to distinguish fake from real news and 19% ignore the truth of the news which indicate the lack of knowledge and need of further training of specific skills in young people.

QUESTION №7: How will a day without internet access affect you? Access to the Internet is not so important for almost 49% of the respondents, who claim that a day without the Internet will not affect them (29%) and that they will have more time for useful things (20%). The rest of the respondents are not keen on losing the internet connection and would experience a type of social anxiety when are kept away from social media, because:

- 39% say they will lose the touch with their contacts and 27% will not be able to communicate with them;
- Around 20% are worried for not updating their profile;
- Only 2% of the respondents are worried for missing the news and trends they follow.

The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.

QUESTION №8: What will you do if your social network account is blocked? To this question, there are two prevailing answers indicating:

- ☒ Dependence on their activity and the attention they receive online – a possible reason for limiting social live contacts and voluntary social isolation because: Around 44% of the respondents will create a new profile on the social network and 15% will panic and look for ways to

unblock it. Using another app is the answer given by 15% of the respondents.

- ☒ Relative independence from online activities because around 26% of the surveyed boys and girls answer that they would do nothing (17%) and they would spend the time for social media for something else (9%).

QUESTION №9: If you get an invitation to join a group from a stranger, what will you do? This question responds to the knowledge and skills of young people to protect themselves from the risks in social networks and to what extent they can do it. Around 68% of the respondents would refuse the invitation, which is probably based on a negative previous experience among the youth. It is positive that around 17% of the respondent would accept the invitation. Around 15 % would do something else, which means that they would not accept it blindly.

QUESTION №10: You come across an interesting article on the Internet. How will you verify its authenticity? Predominance of the answers (64%) to this question are related to checking on the Internet the source of the article (22%) and its validity in Google (42%). It means that there is some level of critical thinking among children and young people who participated in the survey. Worryingly around 32% of the respondents will trust the information without any doubt which is a risky behavior. Only around 4% will turn to friends and relatives for advice which means that most of the surveyed young people do not need the authority of the more experienced and trusted people.

QUESTION №11: What are your ways of dealing with cyberbullying? Most of the respondents have some idea about coping with the problem – around 59% stated that they would read about it and 15% that would watch a video about how to manage with cyberbullying. This is a proactive approach and positive attitude. Around 34% would talk to someone close like relatives and friends, which means that trust is important factor for young people. Around 12% admit that they don't know how to deal with cyberbullying which is a clear message for lack of knowledge, skills and specific information about the problem. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №12: If a friend suggested you follow a popular trend, what would you do? The answers to this question show a criticality towards the information that is offered on internet. According to the answers, most of the surveyed young people will look for information about the trend in advance (61%) and would watch TikTok videos about it (10%). This means that 71% of the surveyed young people have a cautious and proactive approach concerning information on internet. Around 27% of the respondents will not follow any trend, recommended by a friend. Only 2% of the responses given by youth provide information on possible risky behavior since they show a readiness to follow a certain trend without preliminary research.

QUESTION №13: You use social networks because...?: To this question, young people mainly answered that they use social networks for fun in their free time (39%) and to connect with friends and relatives (32% and 20%). A small number of respondents have answered that social networks are a way to find out what others think of them (7%) and to compare their life with those of other people (2%).

QUESTION №14: Do you share your negative experiences online with anyone? Most of the respondents do not share negative experience they had in social networks (64%). Around 22% of all the respondents would share with friends and relatives which is a more active approach. Around 7% would ignore the problem and about 7% don't know who to share the negative experience with. The fact that young people do not share about negative experiences on social networks and ignore the problems is very worrying. These results show that young people are not aware of the real risks and underestimate their effects. Since this is a threat for their mental health it requires serious measures to educate young people with skills and knowledge about protection on the Internet.

QUESTION №15: How do you deal with bullying on social media? Most of the respondents stated that blocking the profile is the method they use to deal with bullying online (35%). Deleting the app will be done by 27% of the surveyed. It is worrying that 22% of the respondents would ignore the problem. Only around 3% of the respondents would share with friends and relatives. Around 2% would

respond with aggressive behavior which means that these young people are not skilled to manage harassment online.

QUESTION №16: Have you come across videos with "sensitive content"? The distribution of videos with sensitive content is a network risk that young people fall into (51%). Very often these videos are forwarded by friends or posted in groups where youth have easy access. Around 28% rarely come across sensitive content since they have specific sensitive content controls. Around 21% claim that they didn't come across such videos.

QUESTION №17: How do you protect yourself from "sensitive content" video on your social network? The leading answer here is blocking the profile - 63% of the respondents. Around 20% state that they will look out of curiosity which could be considered as risky behavior. Sharing with friends and relatives is stated in only 10 % of the answers. Changing profile filter is another method mentioned by 7% of the respondents.

QUESTION №18: When you receive a message with hate language (Hate messages), you...?: There is a sharp edge in responses to this question: around 37% of the respondents would not read the message if it is from an unknown profile, 29% would delete the message and around 5% would block the sender. Ignoring the message would be the action of around 27% of the respondents. Only 2% would respond to the message with the same tone which suggests answering to the aggression with aggression and in conclusion – lack of knowledge and skills to manage hate language online.

QUESTION №19: Have you personally sent such messages? Sending messages with hate speech have been confirmed by 7% of the young people surveyed. On the other hand, half of the respondents (51%) have denied sending such messages, and around 42% are avoiding doing it.

QUESTION №20: Do you know what is misuse of personal and/or financial data on the Internet? About 32% of the respondents stated that they are aware of what is misuse of personal and/ or financial data. It is worrying that 42% have no information and 26% are willing to learn more. This means that around 68% of

the young people surveyed realize the lack of knowledge about the topic. Considering the active use of the Internet and social networks, online shopping and risks, related to protecting financial data, young people do need additional and more specific information on how to protect their personal data on the Internet.

QUESTION №21: What methods of protection against misuse of personal and/or financial data do you know? Most popular protection method of personal and financial data online among young people surveyed (65%) is consisting of two similar approaches: not sharing personal and financial data (40%) and not sharing personal data at all (25%). Antivirus program would be the next method chosen by young people according 25% of the respondents. Password protection with additional app and two-factor authentication is mentioned by 20% of the young people surveyed. The distribution of the methods according to the answers suggests a relatively poor knowledge and skills among most of the young people needed to protect themselves from malicious interference in their personal profiles on social networks. What is worrying is that 30% of the surveyed stated that they do not use any protection method of personal or/ and financial data which indicates gaps in knowledge and skills, needed for safe internet life. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №22: If you find out that your friend has an addiction to social networks, how will you help him? Personal support is readily offered from the young people surveyed including: advise for deleting the app (42%), friendly conversation (37%), sharing with the parents of the person affected (27%). Around 26% of the respondents want actively to help and they would look for information how to do it (22%). Around 10% of the respondents stated that they don't know how to do it. It is a good sign that none of the respondents indicated that they don't think addiction is or could be a problem and they claim that there is nothing wrong with dependence on the Internet and social networks. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №23: How will you protect yourself if an unknown profile writes to you and asks to meet you? Caution among young people is seen by most answers about their probable behavior - they will not respond to the message and delete it (44%), would block the profile (32%) and would share with their friends and relatives about the situation (29%). On the other hand, there are some worrying answers - around 9% of the respondents would communicate and meet in real life with the person and 20% would answer to the message since they don't think there could be a risk for them. Not taking any precautions and meeting with a stranger in the real life is a very risky behavior for young people. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

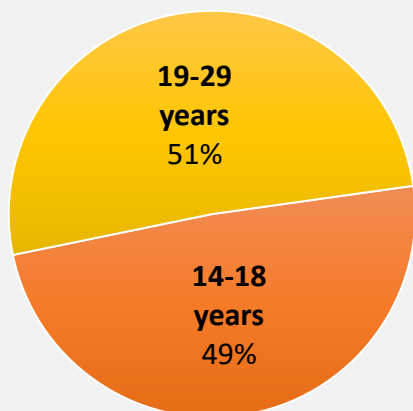
QUESTION №24: Do you personally send such invitations? Most of the respondents (61%) deny sending invitations for communication to strangers. It is worrying that rest of the respondents (39%) do send invitations as an excuse for their limited social life (15%) and as a way for finding new friends (12%). These results prove that Internet and social media are important for young people, because it helps them find new friends. But it is also a signal, that they are quite addicted to social media and internet, and they lack normal communication in real life.

QUESTION №25: Have you received provocative photos? Around 78% of the respondents denied receiving provocative photos, while 22% confirmed such events online. This provides an answer to the extent to which young people in social networks are protected from sensitive and harmful content.

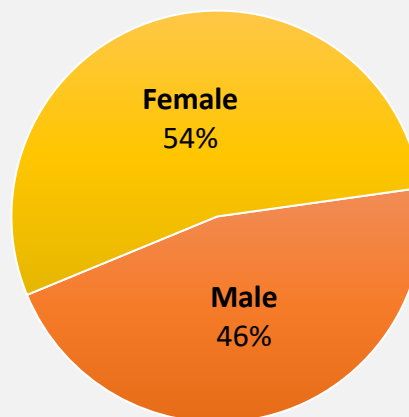
QUESTION №26: Have you sent provocative photos that you wouldn't post on the Internet? Here the answers are unequivocal - 100% of the respondents deny sending provocative photos.

VISUAL REPRESENTATION OF SURVEY RESULTS IN POLAND:

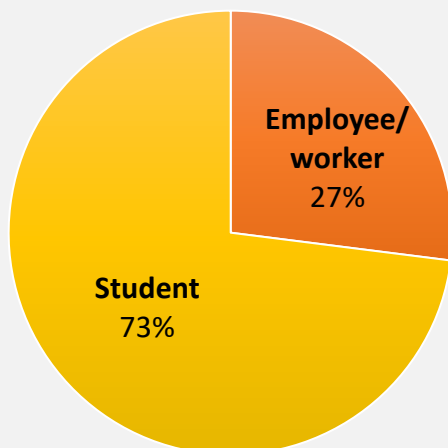
Your age is between...?



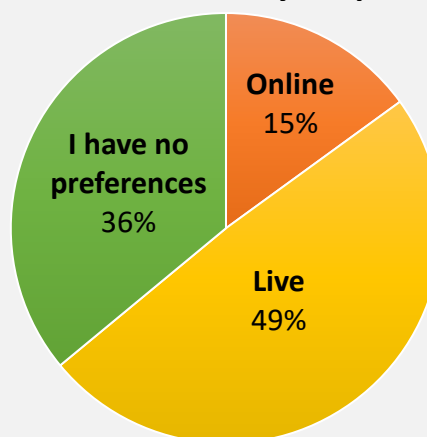
Your gender is...?



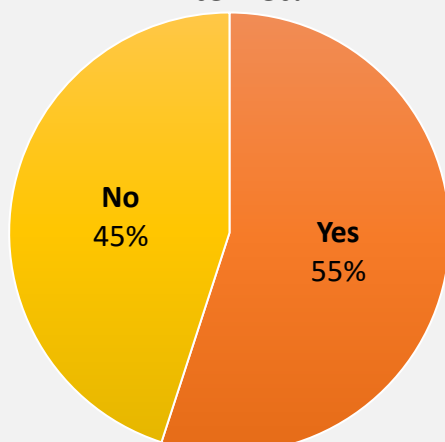
Your status is...?



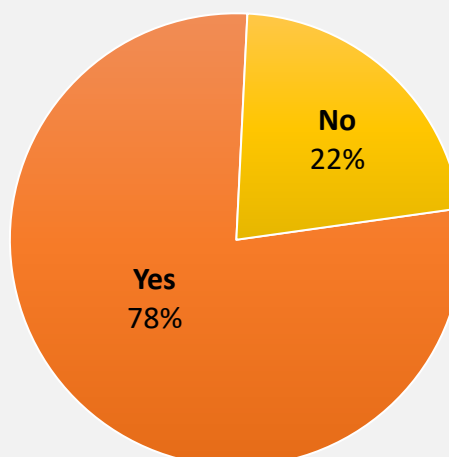
1. How do you prefer to communicate with your peers?



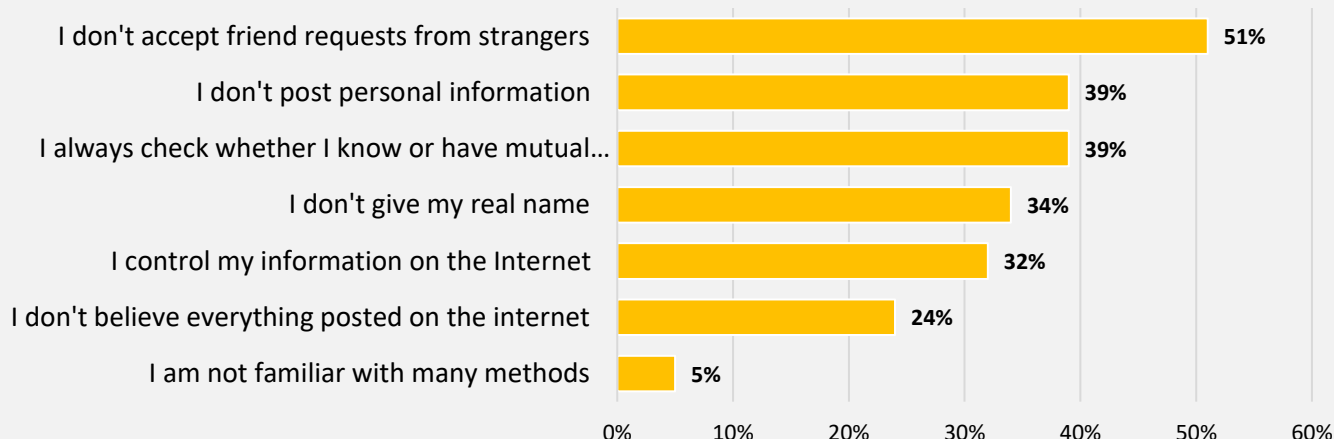
2. When you are on vacation, is it mandatory for you to have internet?



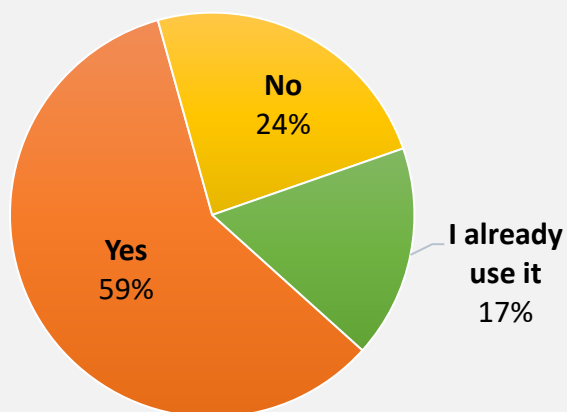
3. Do you think there are things on internet that can harm you?



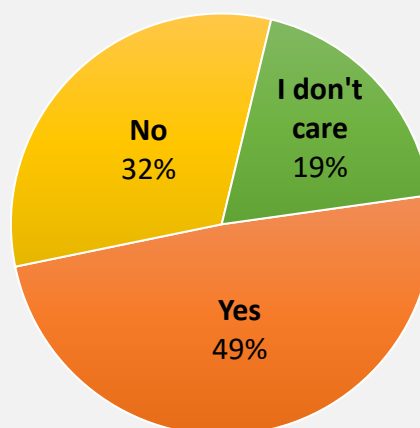
4. Which social media protection methods do you know...?



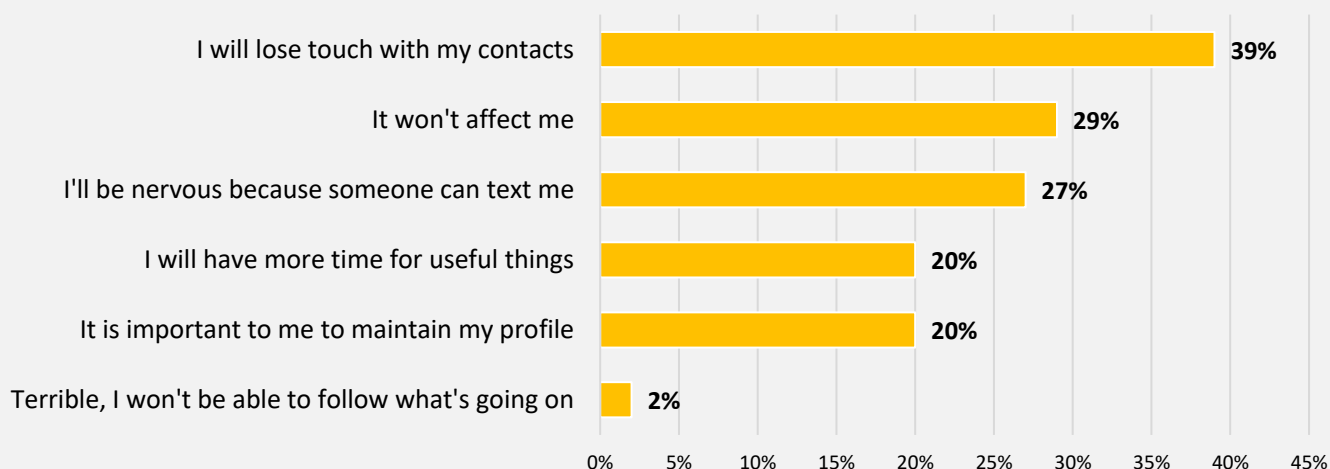
5. Did you know that there is an app that monitors time spent on Internet?



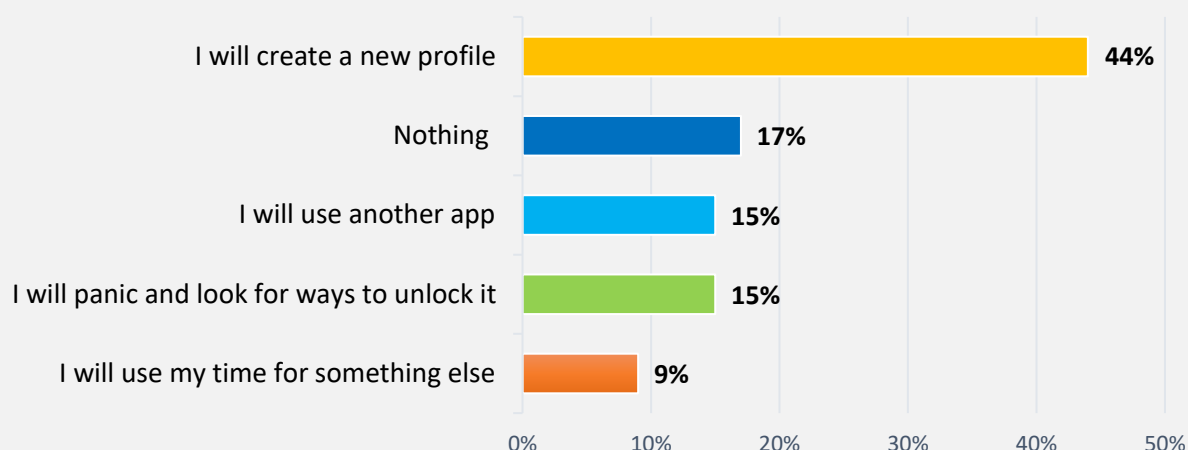
6. Can you tell fake news from real news?



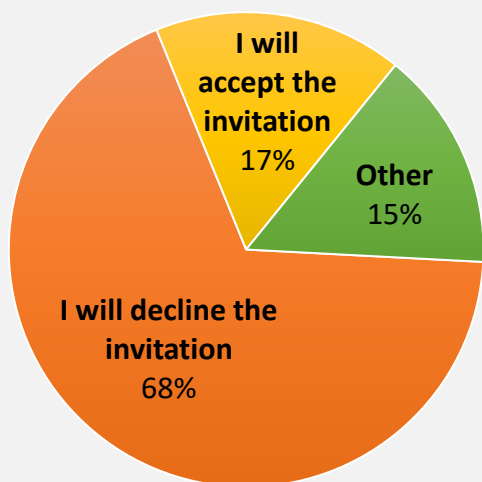
7. How will a day without internet access affect you?



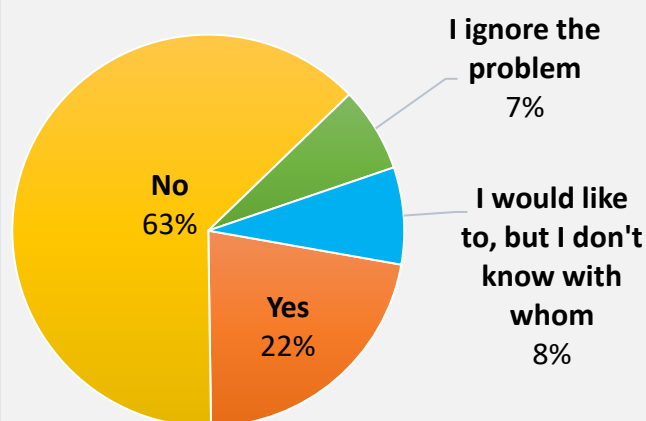
8. What will you do if your social network profile is blocked?



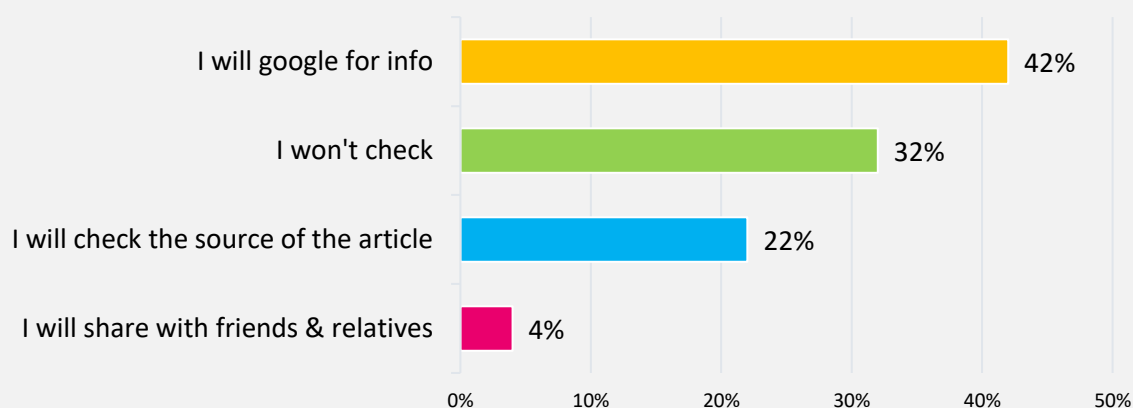
9. If you get an invitation to join a group from a stranger...?



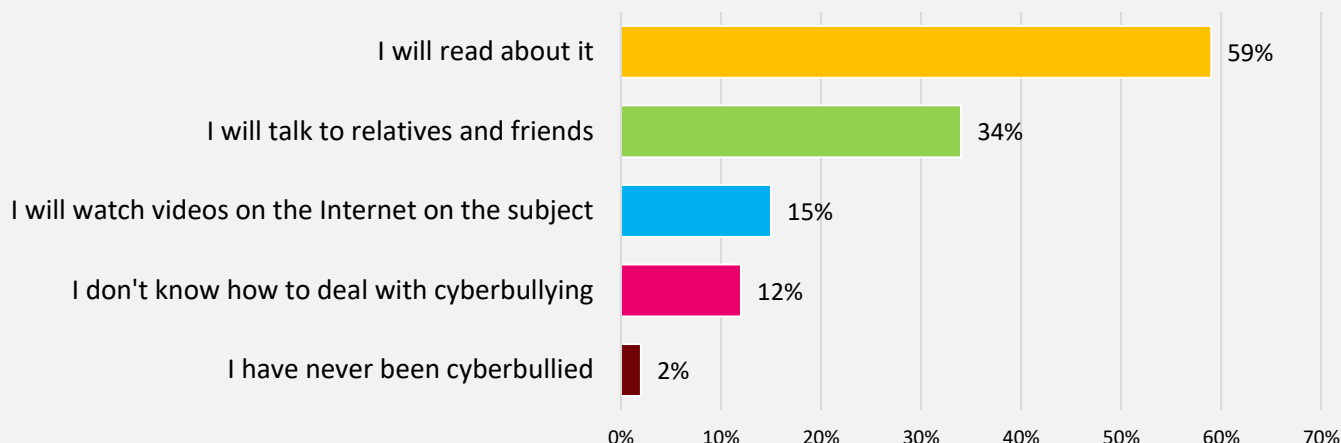
14. Do you share your negative experiences online with anyone?



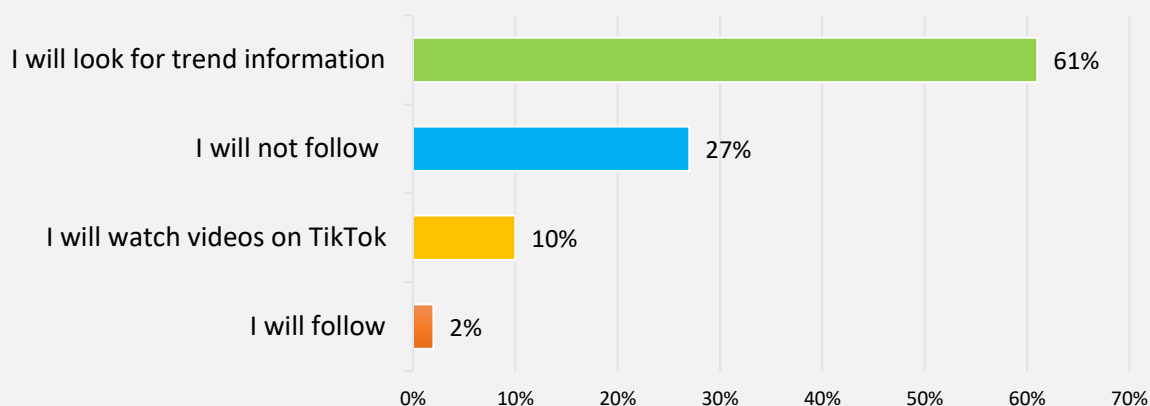
10. You come across an interesting article on the Internet. How will you verify its authenticity?



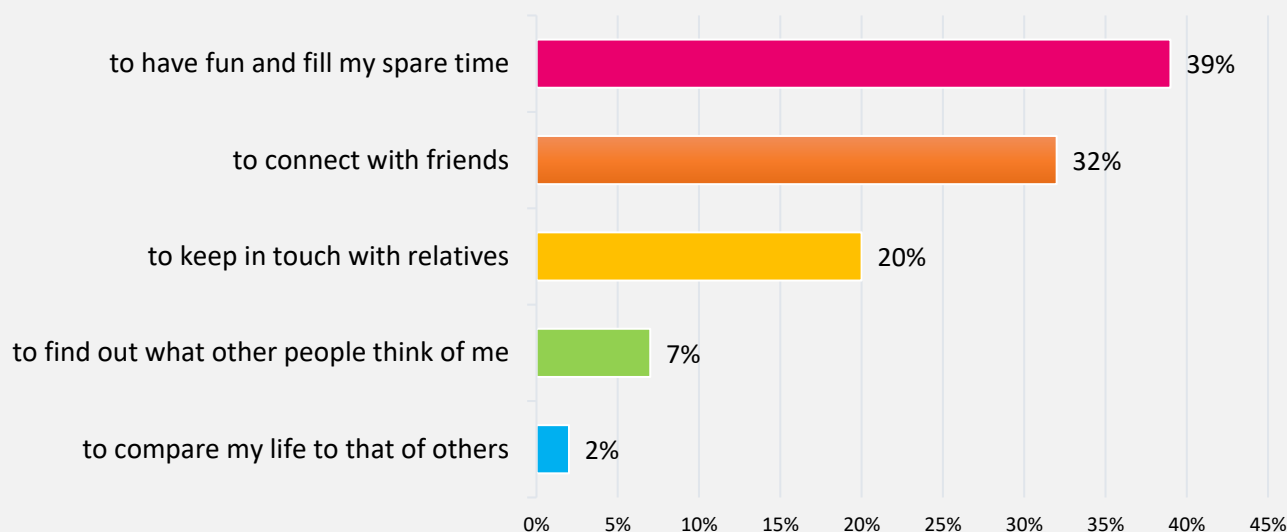
11. What are your ways of dealing with cyberbullying?



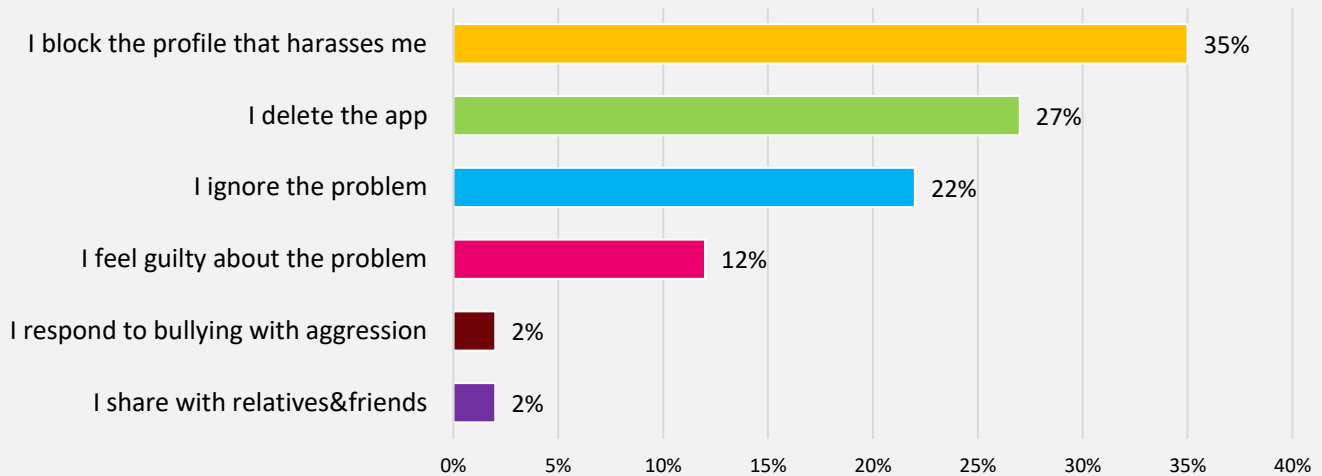
12. If a friend suggested you follow a popular trend...?



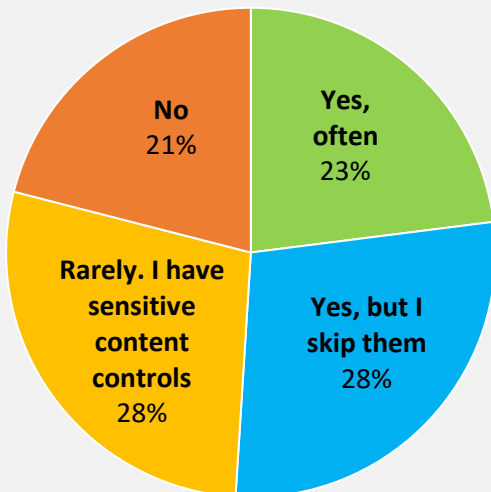
13. You use social networks because...?



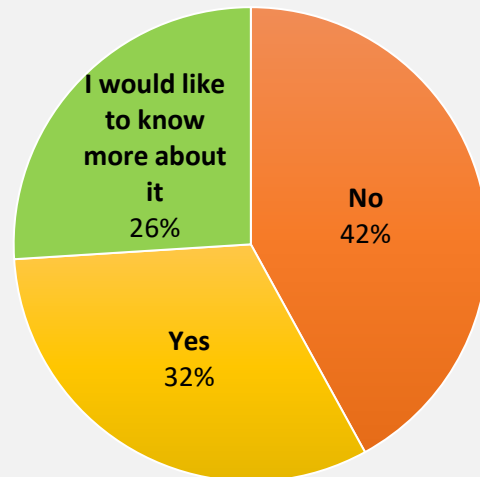
15. How do you deal with bullying on social media?



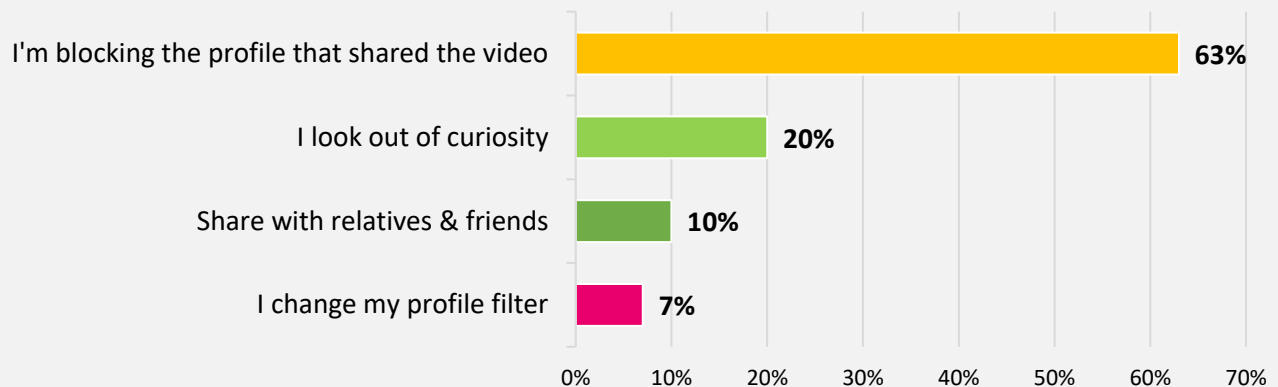
16. Have you come across videos with "sensitive content"?



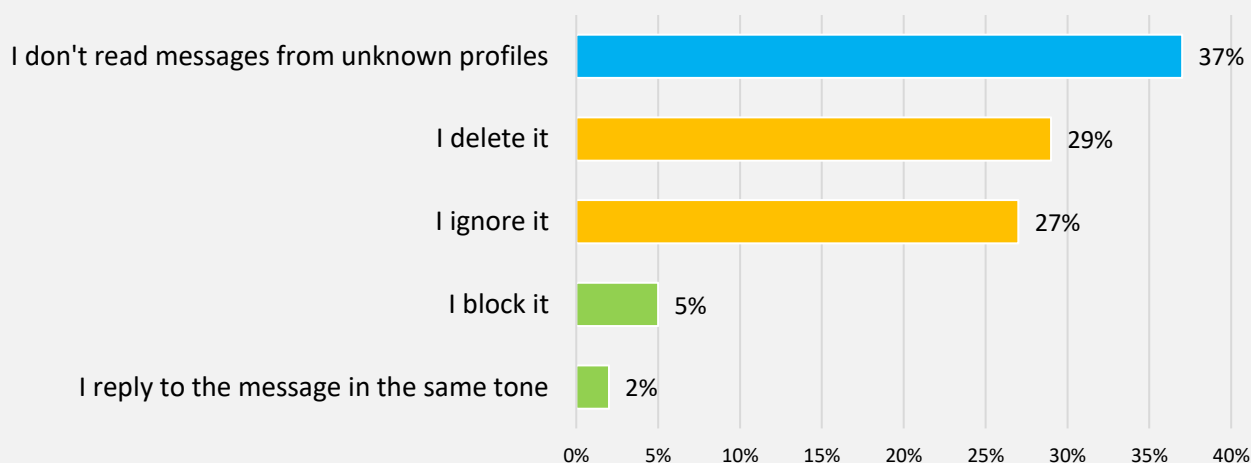
20. Do you know what is misuse of personal and/or financial data?



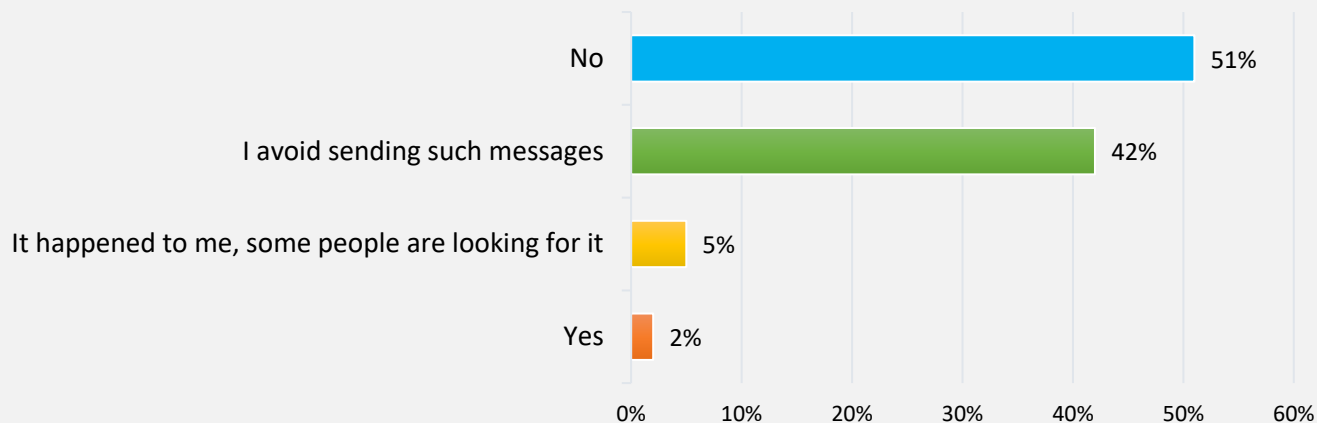
17. How do you protect yourself from videos with "sensitive content" on your social network?



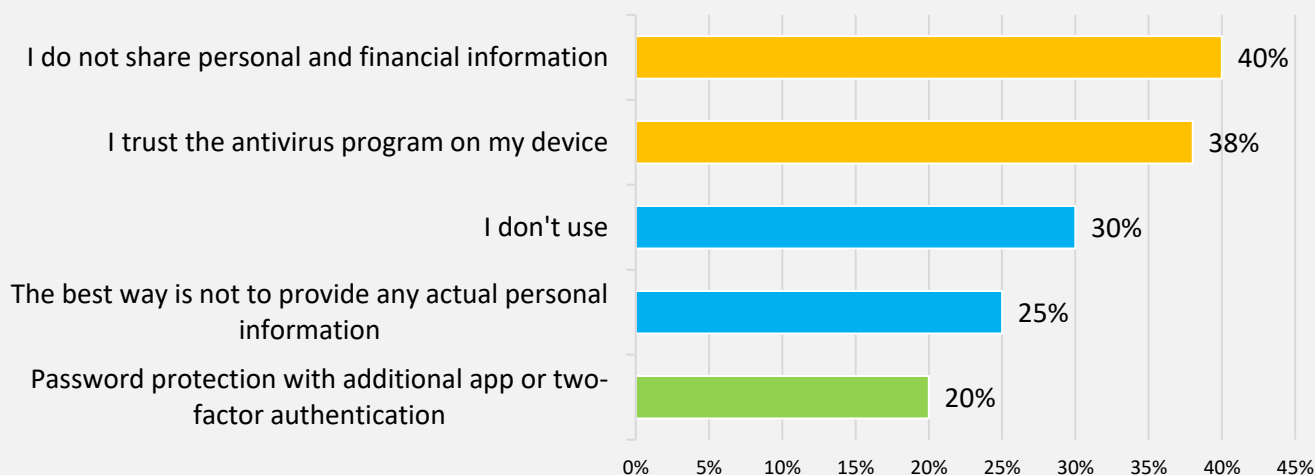
18. When you receive a message with hate language, you...?



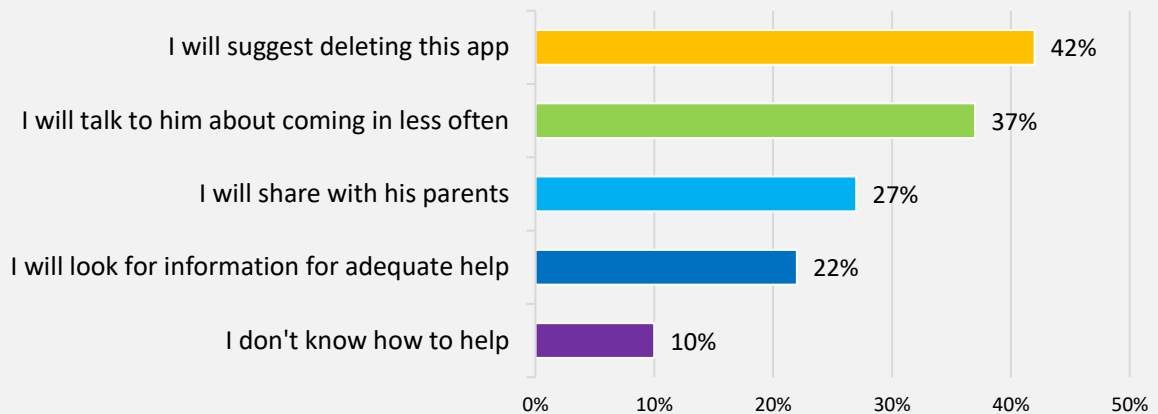
19. Have you personally sent such messages?



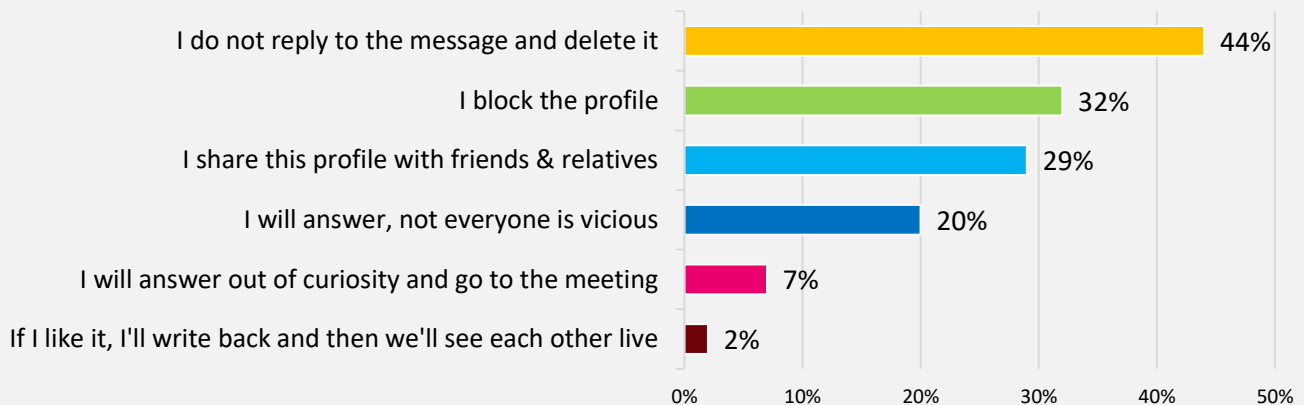
21. What methods of protection against misuse of personal and/or financial data do you know?



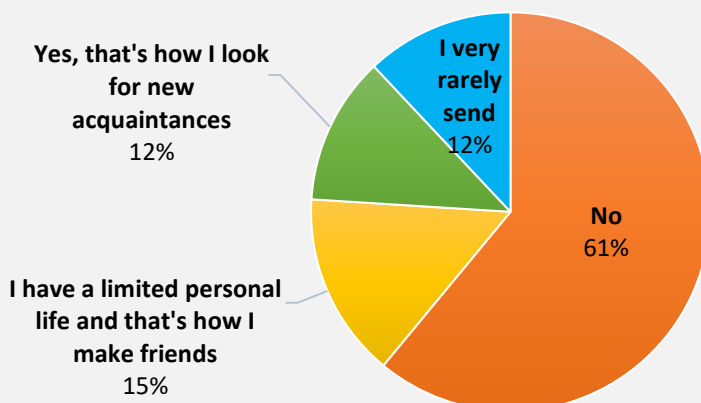
22. If you find out that your friend has an addiction to social networks, how will you help him/ her?



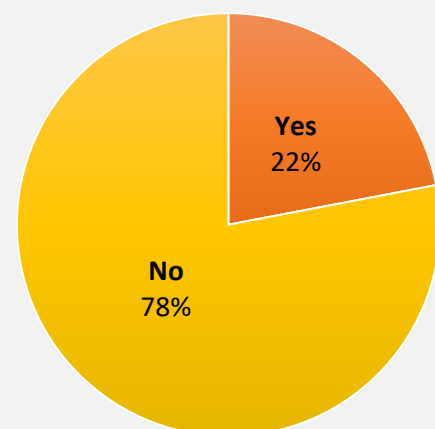
23. How will you protect yourself if an unknown profile writes to you and asks to meet you?



24. Do you personally send such invitations?



25. Have you ever received provocative photos?



4. AUSTRIA

The survey in Austria was initiated in 2023 by the partner organization **Academy for political education and measures to promote democracy, Austria**. The sample involved **46 respondents**, selected from schools in the city of Leonding and the city of Linz in Austria. The respondent's characteristics are as follows:

- ✓ **Age:** Around 59% of the respondents were in the age group 14 to 18 years old. The rest of the young people - around 41% - were in the age group 19-29 years old. The age distribution corresponded to the purpose of the survey since most of the respondents are most active in social networks and are particularly exposed to risks.
- ✓ **Gender:** Young people of both sexes participated in the survey without pre-selection according to gender. In the current survey the distribution between male and female is 57% (26 boys) and 43% (20 girls).
- ✓ **Social status:** Around 76% of the respondents are students. Rest of them (24%) are working. That allows to objectively see the attitudes of the most vulnerable target group regarding methods of protection in social networks.

QUESTION №1: How do you prefer to communicate with your peers? It is interesting fact that 83% of the respondents prefer live communication with their peers. Around 17% prefer online form of contact with their friends. A comparative analysis of the answers to this question and the inclusion of the gender indicator shows that there is no difference between both sexes in communication preferences.

QUESTION №3: Do you think there are things on the Internet that can harm you? It is interesting that around 96% of the respondents know that there are possible risks and harms online. The fact that only 4% do not know or ignore the risks in the networks is a good sign for easy management with a suitable specific training.

QUESTION №4: Which social media protection methods do you know? The answers to these questions showed that 98% of the young people surveyed are aware of social media protection methods. Only 2% stated that they don't know any methods of protection. Most respondents are sceptic about the information in social media and stated that they don't believe everything posted on the

Internet (33%). Many respondents indicated that they don't post any personal information (30%), don't share their real name (4%) and control their personal information online (7%). Around 20% of the respondents are cautious when it comes to new acquaintances - 9% don't accept friends request from strangers, 11% always check whether they know or have mutual acquaintances with the person who sent them an invitation. The results of this question indicate some familiarity and awareness among young people about protecting themselves from the risks in social networks but still there are some gaps in their knowledge and skills that require additional training. **The sum of the percentages is more than 100% because some of the respondents have given more than one answer to the question.**

QUESTION №5: Did you know that there is a mobile application (App) that monitors how much time you spend on the Internet? Around 78% of respondents know about such mobile application, around 11% use it and around 11% have no idea about it. This is a sign for a relatively good understanding about the control of time online among young people surveyed. Still the little number of boys and girls who use such application means that most of the respondents rely on their own personal control over the time spent or that they do not like to be limited. It is a bit surprising that all the respondents in the age group 19-29 years are aware of this kind of software or use it, while only 81% of the respondents in the age group 14-18 years do the same - probably because of their shorter experience online. No matter of their age most of the respondents are still uncritical to the time they spent online no matter what their gender is as well.

QUESTION №6: Can you spot a fake (fake news) from real news? The answer of 63% of the respondents is that they think they can distinguish fake news from real ones. Referring to the above question about methods, knowledge about fake news among youth is based more on accumulated experience than on learned and validated information. Comparing this question with the dangers of the Internet that can harm the young people who responded and comparing the positive answers, 29 young people are aware of the risks and fake news and confirm that they can distinguish them from reality. Worryingly, 33% share that they wouldn't be able to distinguish fake from real news and 4% ignore the truth

of the news which indicate the lack of knowledge and need of further training of specific skills in young people.

QUESTION №7: How will a day without internet access affect you? Access to the Internet is not so important for 61% of the respondents, who claim that they will have more time for useful things (52%) and that a day without the Internet will not affect them (9%). The rest of the respondents are not keen on losing the internet connection and would experience a type of social anxiety when are kept away from social media, because:

- Around 24% will not be able to communicate with their contacts and 4% say they will lose the touch with them;
- Around 4% of the respondents are worried for missing the news and trends they follow.

QUESTION №8: What will you do if your social network account is blocked? To this question, there are two prevailing answers indicating:

- ☒ Dependence on their activity and the attention they receive online of ...% of the respondents – a possible reason for limiting social contacts in real live and voluntary social isolation because: 28% of the respondents will create a new profile on the social network, 24% will panic and look for ways to unblock it, using another app is the answer given by 9% of the respondents and considering other options by 11%.
- ☒ Relative independence from online activities because around 26% of the surveyed boys and girls answer that they would spend the time for social media for something else (19%), they would or do nothing (9%).
- ☒ The degree of importance of the social network profile depends on gender, indicating that boys are more active on the Internet and undertake more social network activities.

QUESTION №9: If you get an invitation to join a group from a stranger, what will you do? This question corresponds to the knowledge and skills of young people to protect themselves from the risks in social networks and to what extent they can do it. Around 83% of the respondents would refuse the invitation, which is probably based on a negative previous experience among the

youth. Around 17% of the respondent would accept the invitation, which means that they would not accept it blindly – such behavior among young people is worrying. The results by gender show that boys more willing to take such risk in social networks.

QUESTION №10: You come across an interesting article on the Internet. How will you verify its authenticity? Predominance of the answers (64%) to this question are related to checking on the Internet the source of the article (44%) and its validity in Google (37%). It means that there is some level of critical thinking among children and young people who participated in the survey. Worryingly around 13% of the respondents will trust the information without any doubt which is a risky behavior. Friends and relatives will not be contacted about such issue. From gender perspective – around 40% of girls and 46% of boys stated that they would search and check the source of the article. This shows that boys make more critical choices to rate articles, preferring source verification.

QUESTION №11: What are your ways of dealing with cyberbullying? Overall, the answers to this question show that around two-thirds of those questioned do not really know how to handle such situations. Around 31% said that they would obtain information on this with the help of videos on the Internet and 33% stated that they wanted to read something on the subject. In a comparative analysis, there were twice as many girls as boys among those who answered, “ignore the problem”. A high response rate of 13%, ignoring the problem, indicates that the seriousness of the risks on social networks is not accepted. Only a third of young people seek help from friends and relatives, indicating a lack of awareness and support from family and friends about the problem.

QUESTION №12: If a friend suggested you follow a popular trend, what would you do? The answers to this question show a criticality towards the information that is offered on internet. According to the answers, most of the surveyed young people will look for information about the trend in advance (41%) and would watch TikTok videos about it (17%). This means that 58% of the surveyed young people have a cautious and proactive approach concerning information

on internet. Around 35% of the respondents will not follow any trend, recommended by a friend. Only 7% of the responses given by youth provide information on possible risky behavior since they show a readiness to follow a certain trend without preliminary research. From gender perspective girls are more vulnerable online since they would follow the trend blindly more often than boys.

QUESTION №13: You use social networks because...?: To this question, young people mainly answered that they use social networks for fun in their free time (35%) and to connect with friends and relatives (26%). A small number of respondents have answered that social networks are a way to compare their life with those of other people (4%). Girls use social media for fun (45%) more often than boys (35%), while boys use social media for connecting with friends and relatives (27%) more often than girls (15%).

QUESTION №14: Do you share your negative experiences online with anyone? Surprisingly most of the respondents stated that they do share negative experience they had in social networks (55%). Around 30% do not share such experience. Around 13% would ignore the problem and about 2% don't know who to share the negative experience with. The fact that 43% of the young people do not share their negative experiences on social networks and ignore the problem is very worrying. These results show that young people are not aware of the real risks and underestimate their effects. Since this is a threat for their mental health it requires serious measures to educate young people with skills and knowledge about protection on the Internet. From gender perspective girls would share with friends and relatives more often (65%) than boys (46%), but also ignore problem more often (20%) than boys (8%). From the other hand boys are more reluctant to sharing (46%) than girls (10%).

QUESTION №15: How do you deal with bullying on social media? Most of the respondents stated that blocking the profile is the method they use to deal with bullying online (61%). Deleting the app will be done by 11% of the surveyed. It is worrying that 13% of the respondents would ignore the problem. Only around 4% of the respondents would share with friends and relatives. Around 2% would

feel guilty because of the problem which means that these young people are not skilled to manage harassment online. From the perspective of gender boys tend to ignore the problem more often than girls (20% vs. 0%).

QUESTION №16: Have you come across videos with "sensitive content"? The distribution of videos with sensitive content is a network risk that young people fall into (70%). Very often these videos are forwarded by friends or posted in groups where youth have easy access. Around 15% rarely come across sensitive content since they have specific sensitive content controls. Around 15% claim that they didn't come across such videos. There are no significant gender differences in the answers given.

QUESTION №17: How do you protect yourself from "sensitive content" video on your social network? The leading answer here is blocking the profile - 39% of the respondents. Many respondents stated that they will look out of curiosity (37%) which could be considered as risky behavior. Changing profile filter is another method mentioned by 13% of the respondents. From gender perspective boys tend to be more curious online and would look at such videos – something that girls would be more cautious about and therefore take less risks than boys.

QUESTION №18: When you receive a message with hate language (Hate messages), you...?: There is a sharp edge in responses to this question: around 59% would block the sender, 2% of the respondents would not read the message if it is from an unknown profile, 2% would delete the message. Ignoring the message would be the action of around 24% of the respondents. Around 2% would answer to the message with a positive tone and 4% would respond to the message with the same tone suggesting answering to the aggression with aggression and in conclusion – lack of knowledge and skills to manage hate language online. The breakdown of responses by gender shows the following: 7 boys vs. 0 girls would delete the message and 9 boys vs. 0 girls would not read a message from stranger. This means that girls are more prone to take risks online.

QUESTION №19: Have you personally sent such messages? Sending messages with hate speech have been confirmed by 10% of the young people surveyed.

On the other hand, most of the respondents (68%) have denied sending such messages, and around 22% are avoiding doing it. By gender girls are less prompt to sending hate messages (90%) than boys (50%), meaning that boys tend to be more aggressive online.

QUESTION №20: Do you know what is misuse of personal and/or financial data on the Internet? Most of the respondents (61%) stated that they are aware of what is misuse of personal and/or financial data. It is worrying that 11% have no information and 28% are willing to learn more. This means that around 39% of the young people surveyed realize the lack of knowledge about the topic. Considering the active use of the Internet and social networks, online shopping and risks, related to protecting financial data, young people do need additional and more specific information on how to protect their personal data on the Internet. The results are very similar for boys and girls. Still, respondents know it's important to protect personal and financial information, and almost a third would like more information on this.

QUESTION №21: What methods of protection against misuse of personal and/or financial data do you know? Most popular protection method of personal and financial data online is password protection with additional app and two-factor authentication mentioned by 48% of the young people surveyed. Not sharing personal and financial data is practiced by 24% of the respondents and not sharing any personal data online by 22%. Antivirus program is mentioned only by 2% of the respondents. The distribution of the methods according to the answers suggests a relatively good knowledge and skills among most of the young people needed to protect themselves from malicious interference in their personal profiles on social networks. What is worrying is that 4% of the surveyed stated that they do not use any protection method of personal or/ and financial data which indicates gaps in knowledge and skills, needed for safe internet life.

QUESTION №22: If you find out that your friend has an addiction to social networks, how will you help him? Personal support is readily offered from the young people surveyed including: friendly conversation (61%), advise for

deleting the app (9%) and sharing with the parents of the person affected (7%). Around 2% of the respondents stated that they don't know how to do it or that they would need to look for information how to do it (9%). Worryingly around 11% of the respondents indicated that they don't think addiction is or could be a problem and they claim that there is nothing wrong with dependence on the Internet and social networks.

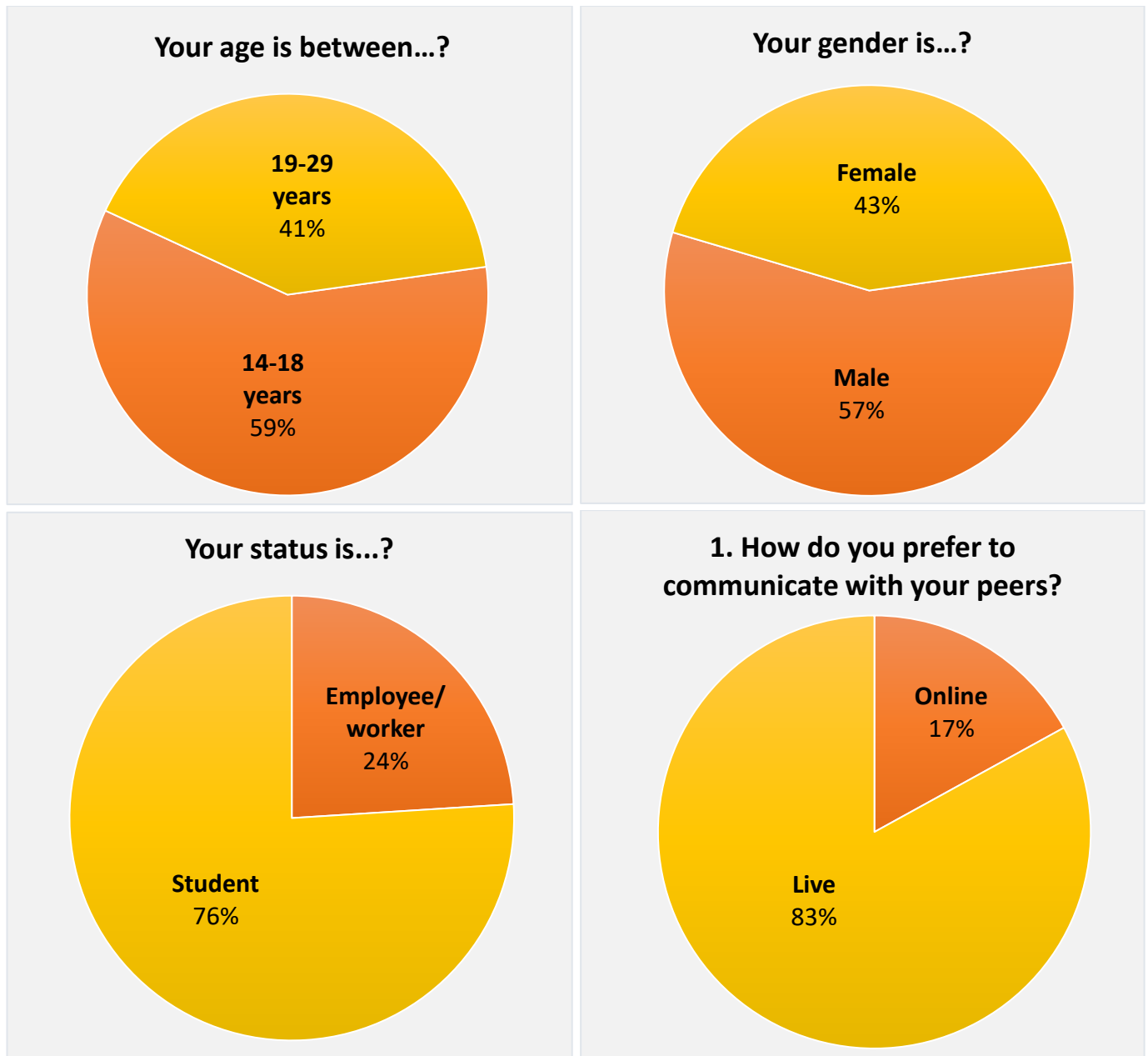
QUESTION №23: How will you protect yourself if an unknown profile writes to you and asks to meet you? Caution among young people is seen by most answers about their probable behavior - they will not respond to the message and delete it (41%), would block the profile (35%). On the other hand, there are some worrying answers - around 22% would answer to the message since they don't think there could be a risk for them and 2% of the respondents would communicate and meet in real life with the person. None of the respondents would share with their friends and relatives about the situation. Not taking any precautions and meeting with a stranger in the real life is a very risky behavior for young people.

QUESTION №24: Do you personally send such invitations? Most of the respondents (81%) deny sending invitations for communication to strangers. It is worrying that rest of the respondents (19%) do send invitations as an excuse for their limited social life (15%) and as a way for finding new friends (4%). These results prove that Internet and social media are important for young people, because it helps them find new friends. But it is also a signal, that they are quite addicted to social media and internet, and they lack normal communication in real life. There are not significant differences related to gender of the respondents.

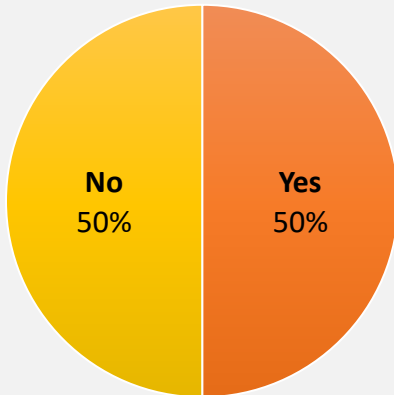
QUESTION №25: Have you received provocative photos? Around 67% of the respondents denied receiving provocative photos, while 33% confirmed such events online. This provides an answer to the extent to which young people in social networks are protected from sensitive and harmful content. There are not significant differences related to gender of the respondents.

QUESTION №26: Have you sent provocative photos that you wouldn't post on the Internet? Here the answers are almost unequivocal - 94% of the respondents deny sending provocative photos, while around 6% confirm doing it. Broken down by gender, the results indicate that boys are a bit more prone to sending such photos online, while girls are more cautious online.

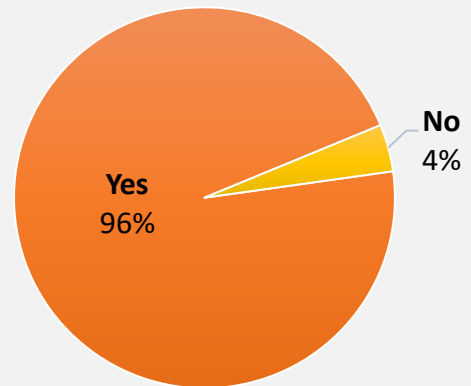
VISUAL REPRESENTATION OF SURVEY RESULTS IN AUSTRIA:



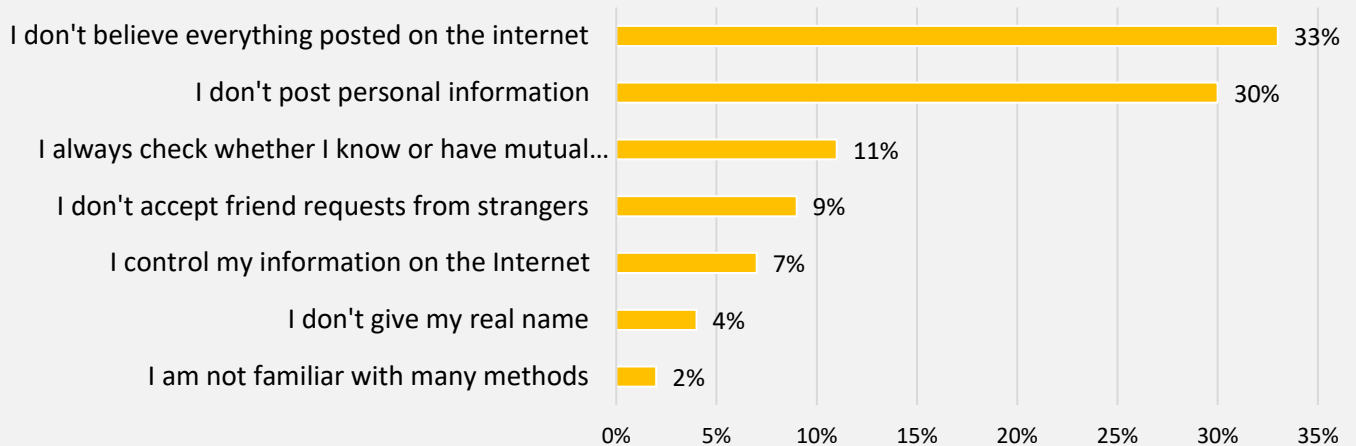
2. When you are on vacation, is it mandatory for you to have internet?



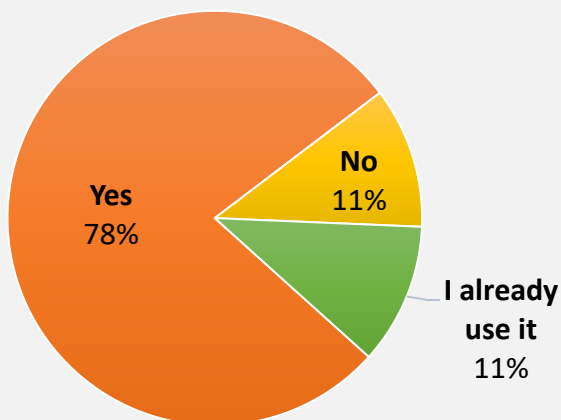
3. Do you think there are things on the internet that can harm you?



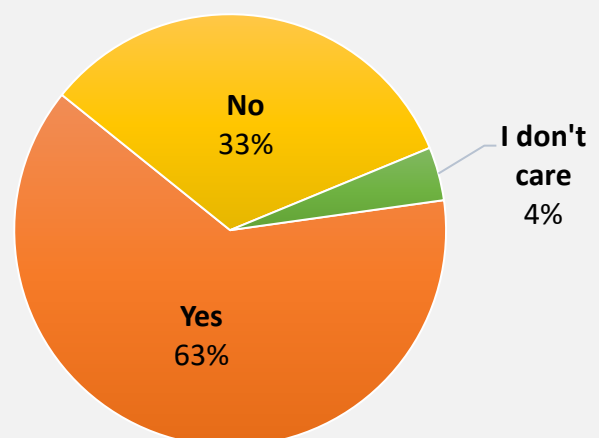
4. Which social media protection methods do you know...?



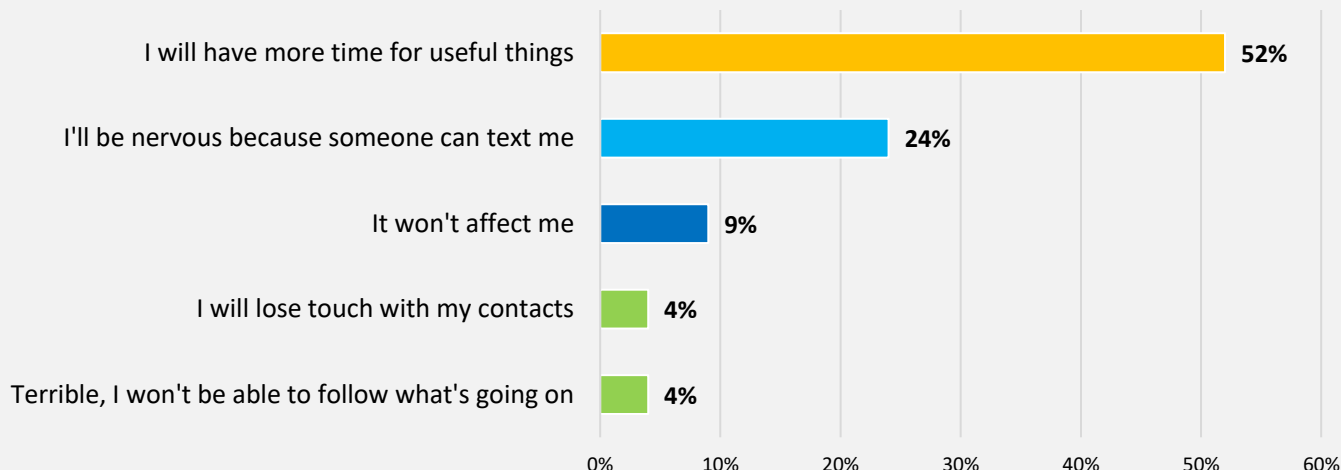
5. Did you know that there is an app that monitors your time on Internet?



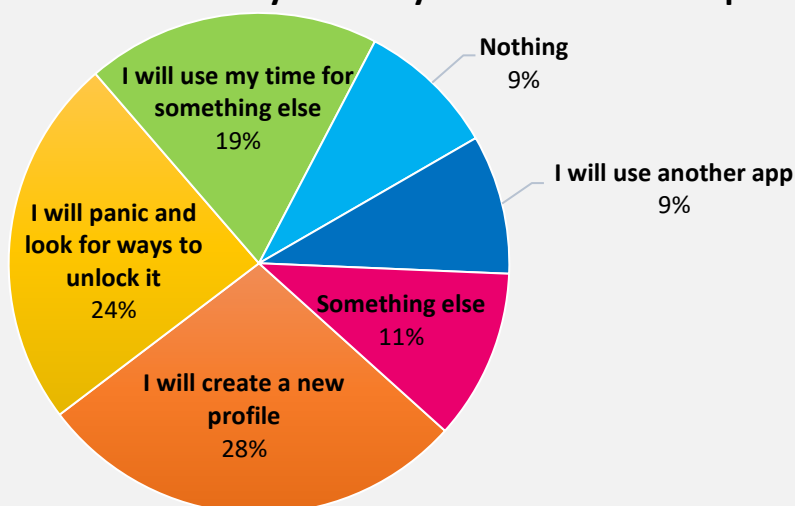
6. Can you tell fake news from real news?



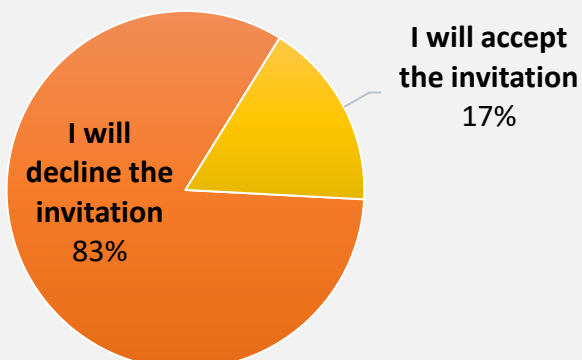
7. How will a day without internet access affect you?



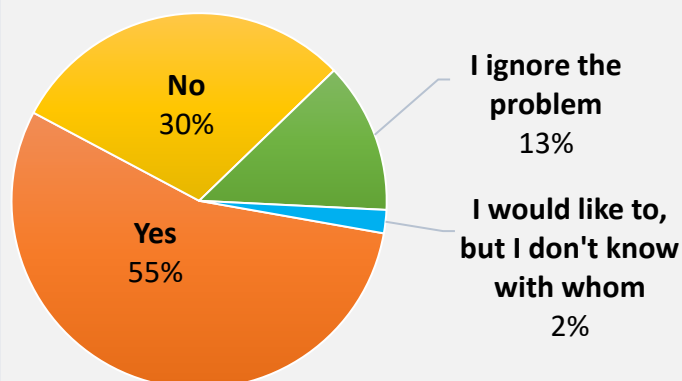
8. What will you do if your social network profile is blocked?



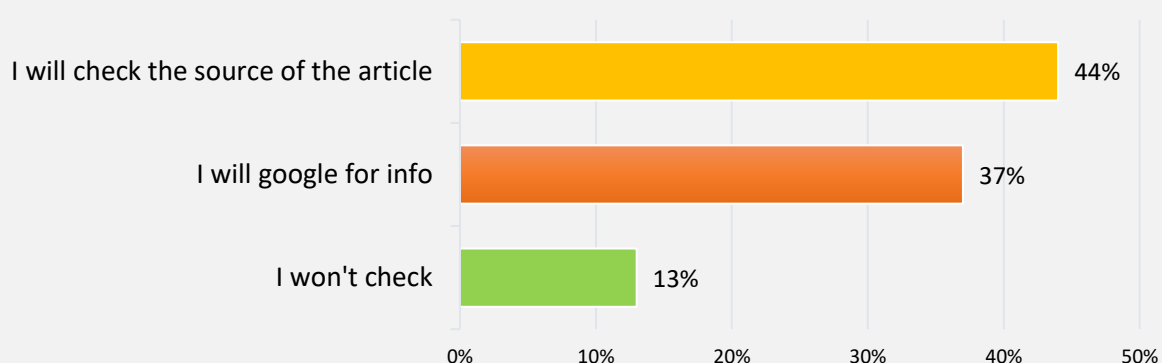
9. If you get an invitation to join a group from a stranger, what will you do?



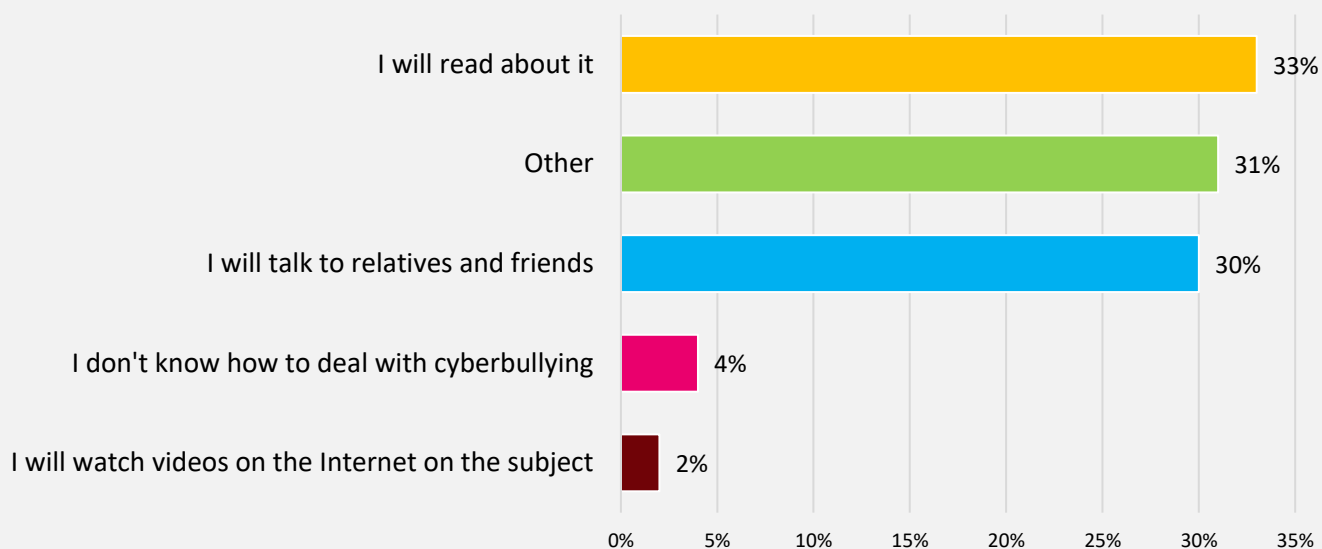
14. Do you share your negative experiences online with anyone?



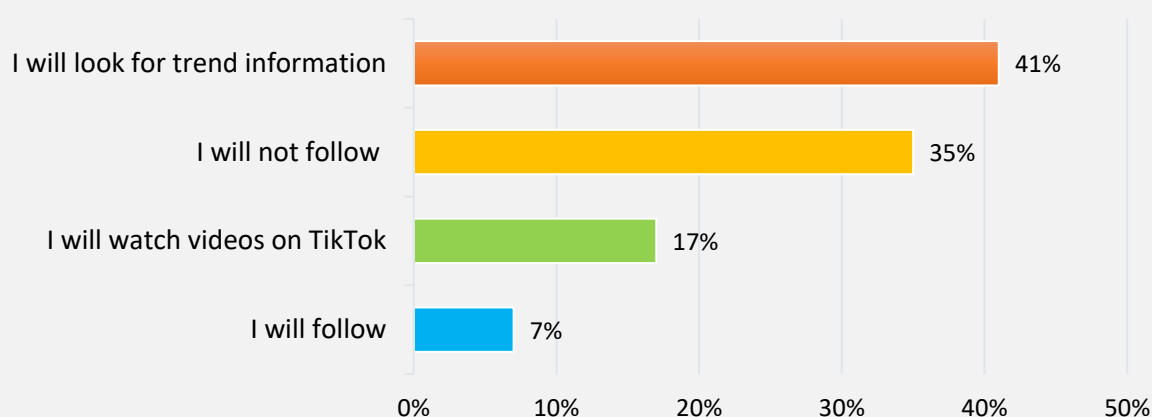
10. You come across an interesting article on the Internet. How will you verify its authenticity?



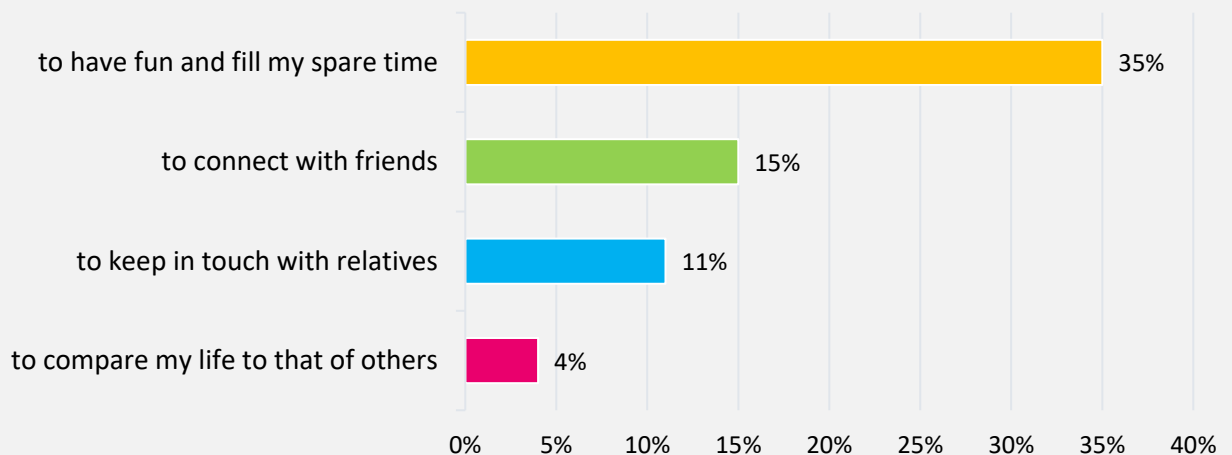
11. What are your ways of dealing with cyberbullying?



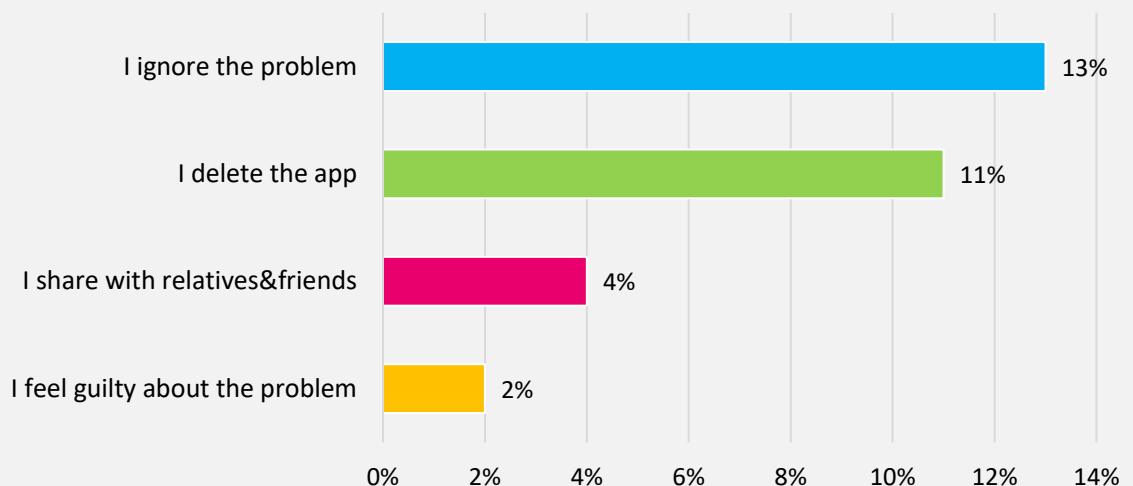
12. If a friend suggested you follow a popular trend...?



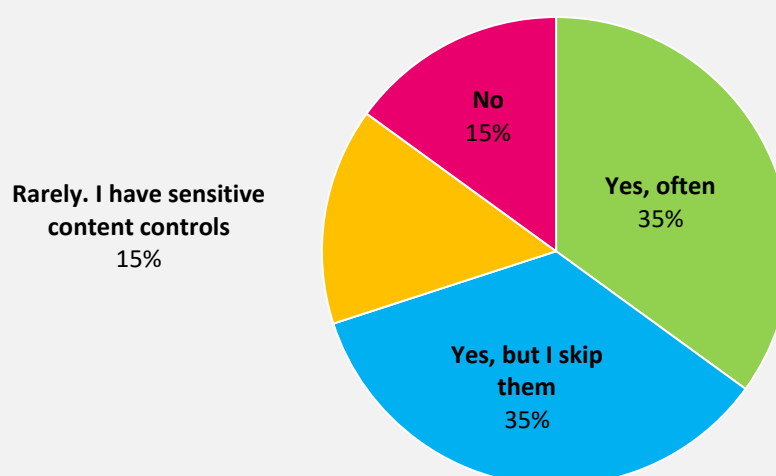
13. You use social networks because...?



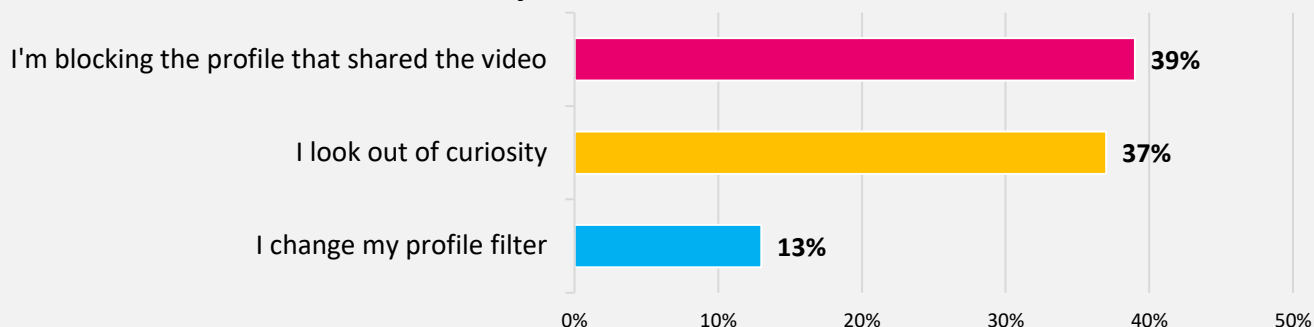
15. How do you deal with bullying on social media?



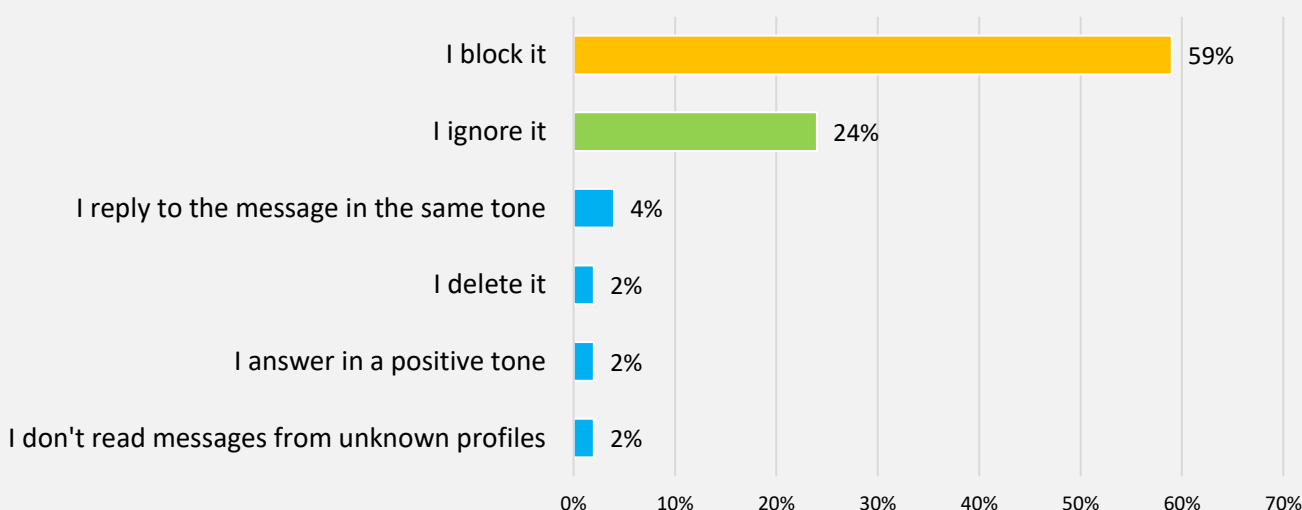
16. Have you come across videos with "sensitive content"?



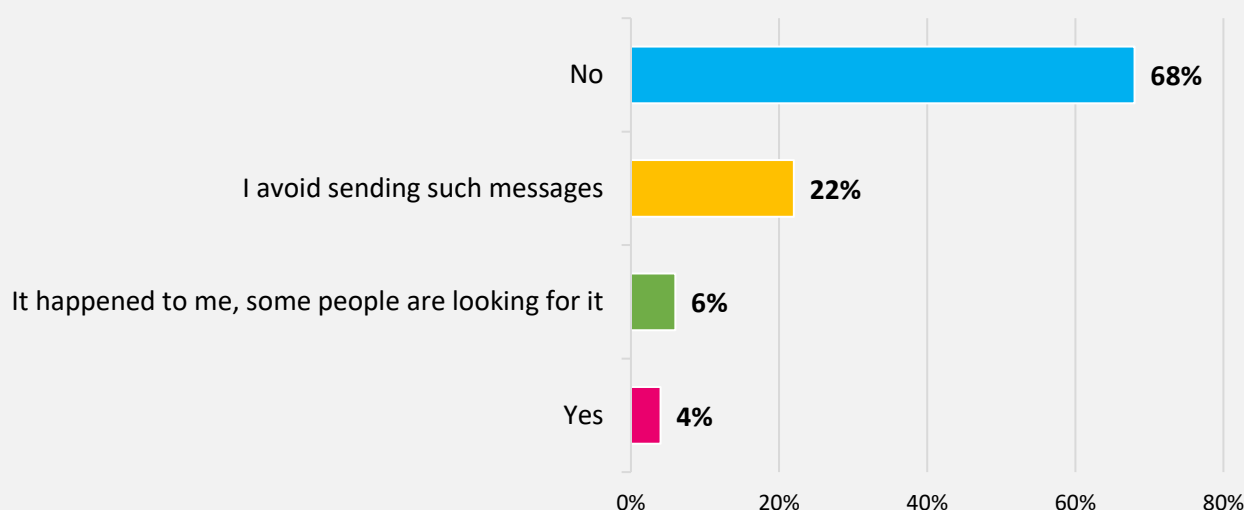
17. How do you protect yourself from videos with "sensitive content" on your social network?



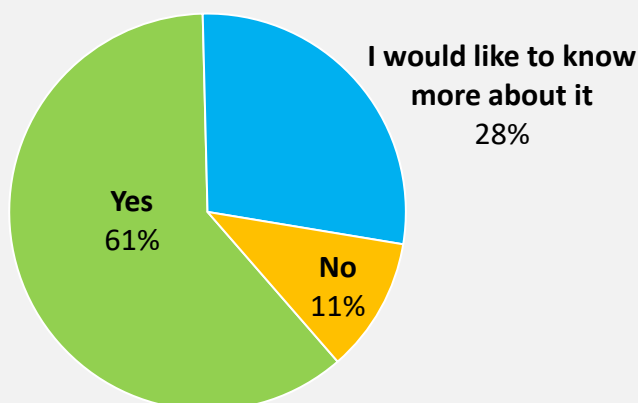
18. When you receive a message with hate language (Hate messages), you...?



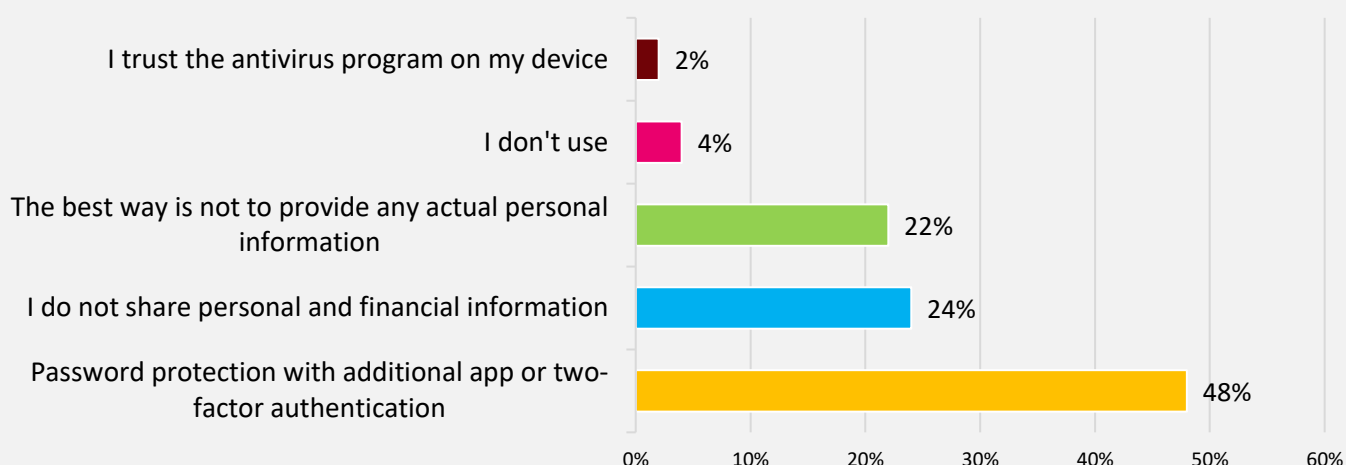
19. Have you personally sent such messages?



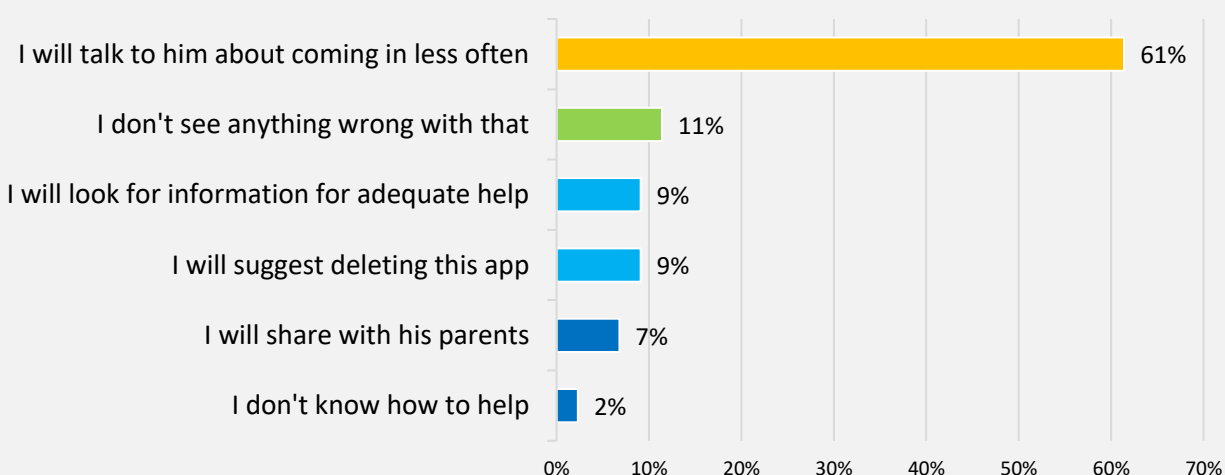
20. Do you know what is misuse of personal/ financial data on Internet?



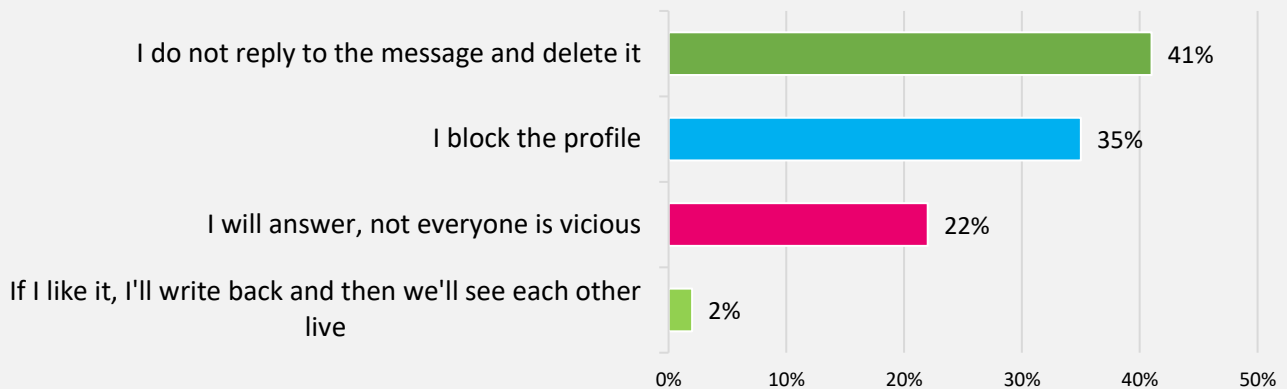
21. What methods of protection against misuse of personal and/or financial data do you know?



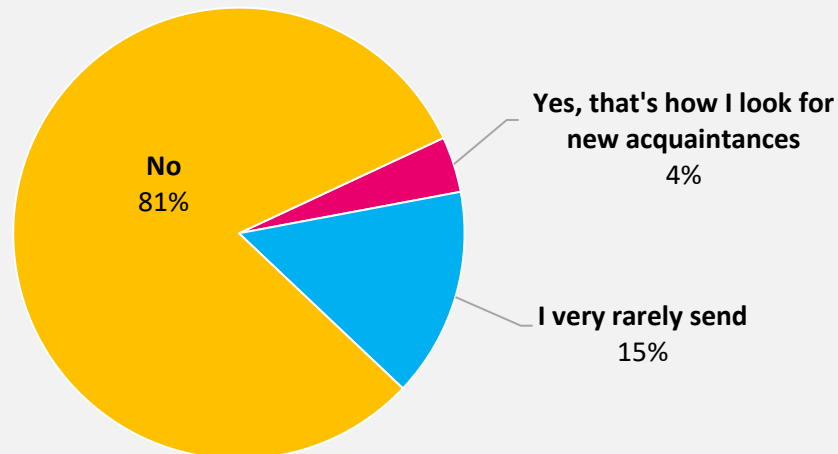
22. If your friend has an addiction to social media, how will you help?



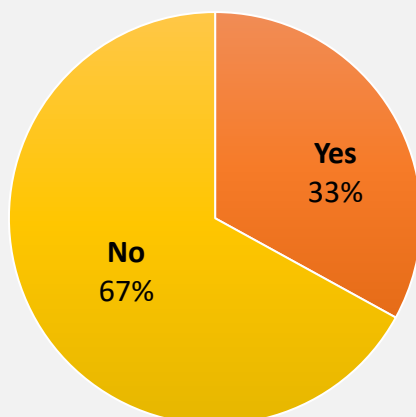
23. How will you protect yourself if an unknown profile writes to you and asks to meet you?



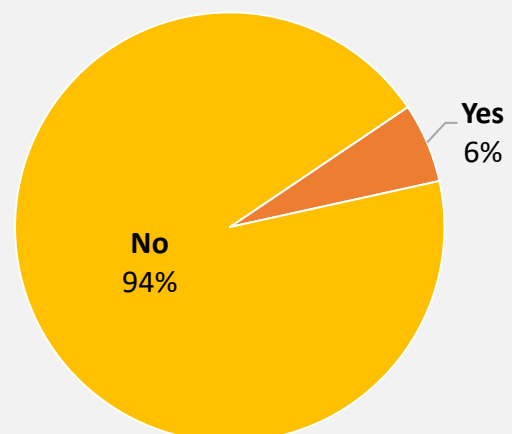
24. Do you personally send such invitations?



25. Have you ever received provocative photos?



26. Have you ever sent provocative photos?



V. RECOMMENDATIONS FOR PREVENTION OF SOCIAL MEDIA THREATS IN PARTNER COUNTRIES

Social media and internet offer unlimited possibilities to young people. At the same time, social networks abound of risks that can cause real harm to young users. Therefore, a multifaceted prevention is needed, combining knowledge and evidence from:

- A. Classification of online risks**, associated to social networks in partner countries according to their type and significance.
- B. Literature review** on the existing prevention methods in the partner countries and worldwide.
- C. Empirical data** from studies, projects and surveys on prevention methods in the partner countries.

As a result, a strong foundation with the best methods for prevention of social media risks in partner countries must be build. Its complexity allowed developing a specific methodology for overcoming the problems, associated with social networks, creating appropriate educational materials for young workers and youth and organizing successful trainings for young people, users of social media.

A. CLASSIFICATION OF ONLINE RISKS

Research of risks among young people as users of social networks defined the most significant online risks in partner countries⁸⁷ according to:

- ☒ literature review on the topic;
- ☒ results of studies, projects and surveys on the topic;
- ☒ survey about social media risks among young people.

Current risks, associated with social networks for young people in partner countries are divided into five groups, according to the European classification of online risks for children (CO:RE)⁸⁸ and the revised typology of risks for children in the digital environment of the Organization for Economic Co-operation and Development (OECD)⁸⁹:

CURRENT RISKS FOR YOUNG PEOPLE ONLINE IN PARTNER COUNTRIES, 2024:

- 1. CONTACT RELATED RISKS (when a child experiences or is targeted by potentially harmful adult contact) (mark 2,67)**
 - a. Harassment, stalking, hateful behavior, unwanted or excessive surveillance;
 - b. Online dating & extortion, cyber sexual grooming, sexual harassment, sexual exploit, sexual trafficking, generation and sharing of child sexual abuse material;
 - c. Ideological persuasion or manipulation, radicalization & extremist recruitment.
- 2. CROSS-CUTTING RISKS (including Privacy risks, Physical & mental health risks, Inequalities & discrimination and Advanced Technologies Risks) (mark 2,56)**
 - a. Privacy violations;
 - b. Physical and mental health risks (incl. isolation, FOMO, negative effect on concentration and attention, self-esteem and worth, critical thinking, distortion of value system, addictions);
 - c. Inequalities and discrimination.
- 3. CONDUCT RELATED RISKS (when a child witnesses, participates in or is a victim of potentially harmful peer conduct) (mark 2,44)**
 - a. Cyberbullying, cyberstalking, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming;
 - b. Sexual harassment, non-consensual sexual messaging (sexting), adverse sexual pressures;
 - c. Potentially harmful user communities e.g. self-harm, anti-vaccine, adverse peer pressures (incl. online challenges and trends, influencers and bad role models).
- 4. CONTENT RELATED RISKS (when a child engages with or is exposed to potentially harmful content) (mark 2)**
 - a. Violent, gory, graphic, racist and other materials with sensitive content, hateful or extremist information and communication;
 - b. Pornography (harmful or illegal), sexualization of culture, oppressive body image norms;
 - c. Mis/disinformation, fake news, age-inappropriate marketing or user-generated content.
- 5. CONTRACT RELATED RISKS (when a child is party to or exploited by potentially harmful contract) (mark 1,25)**
 - a. Identity theft, fraud, phishing, scams, hacking, doxing, blackmail, security risks;
 - b. Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse;
 - c. Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase.

B. LITERATURE REVIEW ON THE EXISTING PREVENTION METHODS IN THE PARTNER COUNTRIES AND WORLDWIDE – more and more countries around the world are recognizing that social media risks require scientific approach in order to help prevent harm to youngest users. Publications from all continents were reviewed in order to find the current prevention methods and best way for their implementation. Successful practices and prevention initiatives worldwide are presented in chapter “III. METHODS FOR PREVENTION OF SOCIAL MEDIA THREATS – THEORETICAL PERSPECTIVE” in this document.

C. EMPIRICAL DATA FROM STUDIES, PROJECTS AND SURVEYS ON PREVENTION METHODS IN THE PARTNER COUNTRIES – current empirical data was taken into consideration when preparing the list of methods below. Doing so allowed the project team to scope the most popular and effective prevention methods in partner countries and also to check the awareness of 392 young users of social media about the possibilities to protect themselves from online risks, related to social networks that can harm them.

- **The purpose of the survey:** to check the knowledge and information that the respondents have about the risks and protection methods in social networks and whether they can adequately manage themselves safely online, based on their own experience and knowledge;
- **Attitude to survey:** In general, the respondents welcomed the survey provided to them with interest and positively. The filling did not cause any difficulties because the questions were formulated clearly and taking into account the age group of the respondents. The respondents treated the filling with the necessary seriousness and attention. We believe that the achieved results are representative within the formulated questions and provide enough material for further analyses and work in the direction of ensuring the safety of young people on the Internet;
- **Awareness about online risks and harm:** Young people surveyed in Bulgaria, North Macedonia, Austria and Poland are generally aware that there are things on the Internet that can harm them. While young people may be aware of these threats, their level of caution and understanding can still vary. Young people surveyed have information that is not sufficient, regarding online safety measures, they do not know how to apply it and how to adequately protect themselves in social networks. These results show that young people rely mainly on information gained from experience and sharing from friends. Very often as a protection method respondents indicated “ignoring the problem” which shows

disregard of the seriousness of the fact that social networks, no matter how interesting and fun they are, carry risks;

- **Sharing with friends and relatives:** a response that is often given by youth indicating what is their awareness level of the need for help. Based on the study, it can be concluded that this relationship regarding how much parents know what their child is doing online is not stable. The majority of young people do not share what they do on the Internet or only share a small part with their parents;
- **Culture of work in the virtual environment:** Growing up in the digital age makes them more technologically savvy and connected than previous generations. Most of the young people demonstrate a sufficiently high culture of work in the virtual environment. They have an understanding of the most common security measures, such as using different passwords and changing them, updating software, not sharing personal information. They are aware that photos or material with inappropriate content should not be uploaded. In the area of Internet security, considering the nature of the risks for young people. However, the level of awareness and understanding vary from country to country;
- **Social media behavior:** Based on the survey responses boys are more aggressive in social networks and are more predisposed to risks, their behavior is riskier, and they are not inclined to provide support when needed to a friend with addiction to social networks, while girls are more active in social networks and non-aggressive in their communication. The difference in the behavior of the two sexes is due to the different stages of development and the level of knowledge about methods of protection in social networks;
- **Recommendations:** young people need to have access to information about prevention methods, to be taught how to communicate non-aggressively, to understand hate speech messages and act correctly. This presents the need of Methodology for training young people how to protect themselves against risks in social networks and targeted trainings on Internet issues. Such efforts will contribute to educating risk-free behavior and building awareness of responsibility among young people. Continuous education and open discussions about online safety with parents, teachers, and other trusted adults can further enhance their awareness and help them navigate the internet safely;
- **Detailed results:** in chapter “IV. METHODS FOR PREVENTION OF SOCIAL MEDIA THREATS - SURVEY PERSPECTIVE”.

PREVENTION OF SOCIAL MEDIA THREATS

Online risks for young people in social media in partner countries are many, diverse and difficult to tackle. It must be emphasized that preventing possible harm and long-term negative consequences for adolescents would require a multidimensional effort and a shared responsibility. According to UNICEF, the task of keeping children & teens safe online is not for a single sector or actor; collaboration and cooperation between parents, educators, schools, governments, law enforcement, civil society, private sector and the young people themselves is essential⁹⁰.

Therefore, here below methods for prevention of risks, related to social media for young people in partner countries are presented in several perspectives:

- A. TARGETED PROGRAMS AND ACTIONS FOR YOUNG PEOPLE**
- B. TARGETED PROGRAMS AND ACTIONS FOR PARENTS & FAMILY**
- C. TARGETED PROGRAMS AND ACTIONS FOR SUPPORT COMMUNITY**
- D. TARGETED PROGRAMS AND ACTIONS FOR DIGITAL COMMUNITY**

Each perspective includes methods that would help prevent risk and harm for young people in different ways and would result in achieving synergy effect if applied together. Based on the study of the current risks and available methods and practices for prevention of risks, related to social networks, the following can be summarized as recommendations:

A. TARGETED PROGRAMS AND ACTIONS FOR YOUNG PEOPLE

Most people use social media in one form or another. While there is nothing inherently wrong with that, and while social media can sometimes be beneficial, it's important to be aware that social media is associated with many issues and potential dangers, including stress, anxiety, loneliness, and depression. Social networks can be particularly challenging for young people, as they may be more vulnerable to the risks associated with these platforms. Therefore, prevention and overcoming the consequences of using social networks by youth is an important topic in today's digital age.

The research shows that in many ways teens are mostly at risk. On the one hand, parental intervention and control significantly decreases compared to younger children. At the same time, a natural curiosity and desire to experiment and explore both the real and the virtual world can expose these children to potentially dangerous situations. Therefore, young people need special attention in the form of training and awareness campaigns. These concepts should be tied to the needs and interests of children, as communication with them needs to be conducted in an accessible language.

To reduce the risks connected with using social media, **education and awareness are essential**. Educational institutions can have a big impact on spreading knowledge about potential risks associated with social media use and how to avoid them. Lessons and trainings on social media use and safety can be incorporated into the curriculum starting from elementary school. This can be accomplished by having group projects, class discussions, and inviting guest lecturers who have expertise in online safety and security.

The processes of teaching and awareness-raising must be continual. Due to the ongoing changes and innovative approaches of social media platforms, new risks and threats can always appear. As a result, it is critical to be educated on the most recent trends in social media usage as well as any potential risks. The promotion of awareness of the dangers of social media can also involve NGOs and government organizations. To inform the public on the usage and safety of social media, these groups can host workshops, conferences, and seminars. To encourage safe and responsible usage of social media, they can work with the various platforms⁹¹.

Peer learning programs are especially effective and useful nowadays. Some of the most common risks related to the use of digital technologies are related to the relationships on the Internet between children or young people themselves (the various forms of online bullying, sexting, sharing illegal or inappropriate content, etc.). Practice shows that the most effective way to teach children how to use digital technologies in a safe and responsible way is through the mediation of their own peers. The training of young trainers should be carried out in partnership between NGOs, schools, government institutions and corporate players to achieve the best and long-lasting result.

1. DIGITAL MEDIA LITERACY EDUCATION

Media literacy is the ability to apply critical thinking skills to the messages, signs, and symbols transmitted through mass media. We live in a world that is saturated with media of all kinds, from newspapers to radio to television to the internet. Media literacy enables us to understand and evaluate all of the media messages we encounter on a daily basis, empowering us to make better choices about what we choose to read, watch, and listen to. It also helps us become smarter, more discerning members of society⁹².

Media literacy is seen as an essential 21st-century skill by educators and scholars, including media psychologists⁹³. Despite this, many people still dismiss media as harmless entertainment and claim they aren't influenced by its messages. However, research findings consistently demonstrate that people are impacted by the media messages they consume⁹⁴.

The share of children who use the Internet before they enter first grade is constantly increasing. Therefore, the need to build their digital skills is a task of increasing importance. It is vital to introduce elements of early learning in digital literacy with a special focus on online safety as early as preschool. Introductory ICT teaching currently emphasizes technical skills, while internet safety, critical understanding and evaluation of information, online etiquette and other social skills are underrepresented – thus neglecting the potential for constructive and fruitful inclusion of digital technologies. It is critical to promote digital media literacy programs that educate young people about the potential risks and consequences of social media use. They must know how to critically evaluate online content, identify fake news, protect their privacy, and maintain positive digital footprint. Fostering digital media literacy skills among young people to help them discern between credible and unreliable sources of information is also

a must. Young people must know how to fact-check before sharing or reposting content. Critical thinking and skepticism must be encouraged to avoid spreading misinformation. By teaching media skills, young people can be better prepared for the risks in social networks and learn to recognize and avoid them. Media literacy also means that young people learn how to handle personal data safely and responsibly, how to protect their privacy and how to react to inappropriate online behavior. Improving the digital literacy of young people can help their mental development and the ability to distinguish between the real and digital worlds.

Emerging science offers preliminary support for the efficacy of Digital Citizenship and Digital Literacy⁹⁵ to increase the frequency of positive interactions online; however, more research is needed in this area⁹⁶. Additional competencies could also include⁹⁷:

- questioning the accuracy and representativeness of social media content;
- understanding the tactics used to spread mis- and disinformation;
- limiting “overgeneralization” and “misestimation” errors that lead users to incorrectly estimate others’ behaviors or attitudes based on social media content (or reactions to content);
- signs of problematic social media use;
- how to build and nourish healthy online relationships;
- how to solve conflicts that can emerge on social media platforms;
- how to refrain from excessive social comparisons online and/or better understand how images and content can be manipulated;
- how to recognize online structural racism and critique racist messages;
- how to safely communicate about mental health online.

Media scholar W. James Potter observes that all media messages include four dimensions⁹⁸:

- Cognitive: the information that is being conveyed
- Emotional: the underlying feelings that are being expressed
- Aesthetic: the overall precision and artistry of the message
- Moral: the values being conveyed through the message

EXAMPLE:

Media psychologist Karen Dill-Shackleford suggests that these four dimensions could be used to improve media literacy skills. For example, while streaming videos online a young person is exposed to an advertisement for a miracle weight loss drug. In order to better evaluate what the ad is really trying to tell it could be broken down as follows:

On the cognitive dimension we can assess what information the ad is conveying to us by asking some of the following questions: What does the ad promise the drug will do? Does it seem likely the drug can deliver on those promises? Who would need this kind of drug?

On the emotional dimension, we can evaluate the feelings the creator of the ad wants us to feel: Do they want us to feel insecure about our weight? Do they want us to imagine the positive ways this drug could change our lives? Do they want us to envision the satisfaction we would feel after the drug delivers its quick fix?

On the aesthetic dimension, we can determine how the ad employs messages and images to make us believe the product will deliver on its promises: Does the ad show "before" and "after" images of someone who supposedly took the drug? Does the "before" image look sad and the "after" image happy? Does the ad offer testimonials from people that are identified as experts?

On the moral dimension, we can examine what the ad makers wanted to say: Are they equating thinness with happiness? Are they sending the message that it's a moral failing when someone is overweight? Are they saying that one has to be thin to be loved and respected?

The purpose of media literacy isn't to enjoy media less, it's to give people the tools to be active media consumers. Not only will media literacy enable young people to detect, analyze, and evaluate negative or false media messages, it will actually enable them to enjoy media more because it puts control over the media back into their hands. And research shows this is likely to increase their health and happiness⁹⁹.

2. CRITICAL THINKING

Media and critical thinking in today's digital world go hand in hand and are built into learning together. As a combination of knowledge, skills, information dissemination practices and knowledge in a new innovative way solve socially significant tasks that arise from real situations in everyday public life. That is why special training is important, which aims to master the basic rules and norms for using information in various life situations. Critical thinking has different dimensions:

- basic skills in critical argumentation – reasoning and drawing conclusions;
- critical judgments;
- critical thinking attitudes;
- critical being and critical actions;
- social and ideological criticism;
- critical creativity and critical openness.

Critical thinking among young people, as active users of social networks, is of high importance for their safety on the networks. Critical thinking skills protect against unmeasured risky behavior and conflict. Social media literacy and critical thinking can be understood as a specific set of technical, cognitive, and emotional competencies that are required when using social media. Having these competencies, young people will be more cautious on social networks and risk-taking will be at lower levels.

3. REPORTING AND BLOCKING

Reporting and blocking are crucial methods for limiting risks on social media. Users could alert the platform's administrators to objectionable content, harassment, and other transgressions of community rules. Users can limit the chance of continued harassment or cyberbullying by blocking undesired users to stop further interactions with them.

To protect their users, social media networks have added banning and reporting features. For instance, Facebook offers users the option to report abusive content, cyberbullying, hate speech, and other transgressions of community standards through its reporting system. Similar types of breaches can also be reported on Twitter. Users have the option to report spam, offensive content, and abusive behavior on Instagram. Users of TikTok have the option to report offensive content and conduct using the platform's reporting mechanism.

Users may also report abuses of their right to privacy under North Macedonia's legal framework for data protection. The Agency for Personal Data Protection, which oversees implementing the law and looking into violations, is established by the Law on the Protection of Personal Data. Users can notify the agency of privacy rights infractions, and the organization will then take legal action against the violators^{100,101}.

Furthermore, while mentioning some of the methods to prevent the risks in social networks that young people face daily, it is important that people who have already been through different risks to be able to overcome the consequences and continue their lives normally.

4. PROTECTION OF PERSONAL INFORMATION

One of the most important steps in reducing dangers on social media platforms is modifying the privacy settings. Social media platforms have become an integral part of daily life, and their use involves sharing personal information and data online. To reduce the privacy concerns connected with utilizing social media, users must be aware of these dangers and take appropriate action. By modifying their privacy settings, individuals can control how much personal information they disclose online, block unauthorized access to their accounts, and safeguard themselves against identity theft, cyberbullying, and other threats. The importance of privacy settings can be highlighted through awareness campaigns and educational initiatives, which can also motivate users to take precautions for their online safety.

Young people must be educated about the importance of using strong and unique passwords, changing them regularly to minimize the risk of hacking and data theft, as well as the potential risks associated with sharing sensitive information online. They must be reminded to regularly review and update their privacy settings on social media platforms to prevent unwanted people from gaining access to private information. Children and teens must be aware to only accept friend requests or connect with people they know in real life, how to keep personal information private and avoid interactions with strangers online.

5. ONLINE HARASSMENT AWARENESS AND EDUCATION

Young people should be aware and educated about the components of online harassment experience (see figure below). There are variety of actors, tactics, mediums, locations and harms that they must be prepared for if using social networks for communication with other people online. In educational programs

it is important to pay attention to the most vulnerable children & young people to online harms including^{102, 103}:

- girls, women, black women, women of color, LGBTQAI+ individuals;
- children from poor households;
- children in communities with a limited understanding of different forms of sexual abuse and exploitation of children;
- children who are out of school;
- children with disabilities;
- children who suffer depression or mental health problems;
- children from marginalized groups;
- children with unguided digital access;
- children with lack of awareness.



Figure 1. Online components of online harassment experience¹⁰⁴

There are different types of harassment online that should be focused on trainings and most popular include:

- **Sexual harassment** - educating young people about the signs of sexual harassment and emphasizing the importance of reporting any incidents to the social media is important. It includes methods like: improving children's knowledge about sexual abuse and how to protect themselves against it; life and social skills trainings in schools; providing adolescent intimate partner violence prevention programs; where support and advice can be accessed online, etc.;
- **Cyberbullying** - awareness must be raised about cyberbullying and its impact on mental health. There must be a promotion of environment of empathy and respect online, encouraging young people to report instances of cyberbullying and provide them with resources for help.

6. EDUCATION ABOUT DIGITAL REPUTATION

There must be an effort to educate teens about their digital reputation. Whenever teen visits a website, shares content, posts something on a blog or uploads information, they're adding to their digital footprint.

7. RAISING AWARENESS OF FAKE NEWS AND DISINFORMATION

Users should be careful about the information they share and be aware that not everything shared on social media is true. Training in dealing with fake news and disinformation can be helpful.

8. VERIFICATION OF FRIENDS AND FOLLOWERS

Before accepting friend requests from new users, users should confirm the identities of their friends and followers. They should also be cautious when adding new friends and avoid adding strangers. Additionally, users should be mindful of fake profiles and avoid sharing any personal information with them.

9. BALANCE ONLINE AND OFFLINE ACTIVITIES

A healthy balance between online and offline activities must be promoted amongst young people. Youth must be encouraged to participate in physical activities, hobbies, and face-to-face interactions. They need help to understand the importance of setting limits on screen time and avoiding excessive reliance on social media for validation. Children and young people should be

strengthened in their personality development and develop a healthy self-confidence. Sports, art and music can also help.

10. POSITIVE ONLINE ENGAGEMENT

Young people need to be encouraged to use social media platforms for positive purposes, such as connecting with friends, pursuing hobbies, or engaging in meaningful discussions. In this regard a promotion of online communities that foster support, creativity, and personal growth would be beneficial.

Young people should learn how to use social media in a positive way so they can benefit from it. They should be able to reconsider which aspects of social media are causing issues, and which aspects are beneficial, and then modify their use of social media accordingly. There are two notable things that young people should likely focus on, as they have been shown to lead to a more positive experience with social media:

- **Use social media in an active way:** Active use of social media, which involves things such as meaningful communication with others, is generally preferable to passive use of social media, which revolves primarily around consuming information;
- **Use social media in an authentic way:** Authentic use of social media, which involves honest self-expression, is generally preferable to self-idealized use of social media, which involves presenting an idealized and therefore disingenuous version of oneself.

11. SUPPORT AND MENTAL HEALTH RESOURCES

Young people must have access to mental health resources and support systems both online and offline. They need education about the potential negative effects of excessive social media use and the importance of seeking help when needed.

12. DIGITAL CITIZENSHIP EDUCATION & RESPONSIBLE SOCIAL MEDIA USE

The promotion of appropriate social media use can be aided by educating people about their digital rights. The ability to traverse the online world securely and ethically can be learned through digital citizenship education, which can also assist users understand their rights and obligations as digital citizens. Digital citizenship instruction can be provided through community-based groups, non-formal educational settings, and integration into formal education curricula^{105,106}.

13. SCREENING OF YOUNG PEOPLE FOR PROBLEMATIC SOCIAL MEDIA USE

Adolescents should be routinely screened for signs of “problematic social media use” that can impair their ability to engage in daily roles and routines and may present risk for more serious psychological harms over time¹⁰⁷. Indicators of problematic social media use include¹⁰⁸:

- a tendency to use social media even when adolescents want to stop, or realize it is interfering with necessary tasks;
- spending excessive effort to ensure continuous access to social media;
- strong cravings to use social media, or disruptions in other activities from missing social media use too much;
- repeatedly spending more time on social media than intended;
- lying or deceptive behavior to retain access to social media use;
- loss or disruption of significant relationships or educational opportunities because of media use.

Social media use should not restrict opportunities to practice in-person reciprocal social interactions, and should not contribute to psychological avoidance of in-person social interactions.

B. TARGETED PROGRAMS AND ACTIONS FOR PARENTS & FAMILY

1. ENCOURAGING AND SUPPORTING PARENTAL INVOLVEMENT AND MEDIATION

As digital-born children struggle to find the right balance between the opportunities and dangers of the digital world, many of their parents feel powerless, incompetent or too busy to help them. In addition to efforts aimed at helping children master digital and media literacy skills, special attention needs to be paid to helping and supporting parents so that they can fully participate in guiding children through the turbulent waters of the digital ocean.

Schools could inform parents about the potential risks of social media use and how to protect their children, schools can also host seminars or workshops for them. Parents can understand the value of setting privacy controls, keeping an eye on their kids' social media activity, and training their kids to behave responsibly online.

2. STRENGTHENING PARENT EDUCATION AND SKILLS IN DIGITAL MEDIA

Parents can support their children in recognizing and avoiding the risks in social networks. Parent education can also help parents better understand the opportunities and risks associated with using social media and how they can help their children develop healthy and safe online behaviors. To protect safety and wellbeing of young people it is crucial that we all educate parents on the possible consequences of using social media.

Parents should be educated about the possible risks of oversharing information about their children online. However, today's digital lifestyle can take it to a new level, turning parents into "potentially the distributors of information about their children to mass audiences"¹⁰⁹. Such behavior is called "sharenting"^{110, 111, 112} and it is used to simplify the actions of parents when posting or sharing their children's personal information on social networks. "Sharenting" is becoming more and more common¹¹³ and it is considered that it can harm a child's reputation.

Example:

A potential source of abuse of children's data comes from their own parents. A 2010 survey found that 81% of children under 2 years old in 10 high-income countries (Australia, Canada, France, Germany, Italy, Japan, New Zealand, Spain, the United Kingdom and the United States) had a digital footprint, meaning that they had a profile or images of them posted online¹¹⁴.

Parents' lack of awareness can cause damage to a child's well-being when these digital assets depict a child without clothing, as they can be misused by child sex offenders. It can also harm child well-being in the longer term by interfering with children's ability to self-actualize, create their own identity¹¹⁵ and find employment¹¹⁶.

3. OPEN COMMUNICATION BETWEEN PARENTS AND CHILDREN

Communication in the family and the authority of the parent is a key moment in the choice of a person in critical situations by the young person. Improving communication between youth and their families could strengthen the position of authority and trust of the youth in the family. As a result, from the constant communication between the young people themselves and their families, a civic awareness among young people will be build.

It is important for children and young people to be able to speak openly about their experiences online and on social media without being ashamed or punished. Parents should encourage open communication and offer support when needed. Open communication between parents and children can help ensure that problems related to social networks and Internet use can be identified and dealt with in a timely manner. Parents should set their children clear rules for using social networks and explain the risks involved.

4. CREATE A FAMILY MEDIA PLAN

Agreed-upon expectations can help establish healthy technology boundaries at home – including social media use. A family media plan can promote open family discussion and rules about media use and include topics such as balancing screen/online time, content boundaries, and not disclosing personal information.

5. PARENTAL GUIDANCE

Parents should engage in open and ongoing conversations with their children about social media risks. They must educate them about potential dangers and help them develop critical thinking skills to navigate the online world safely. An important step in navigating the risks of social networking is to have ongoing conversations about social media use with the youth especially the teens. If parents are engaged in their teen's online world, it will be easier to have conversations about some of the risks and ways to manage them.

6. ATTENTION, MONITORING AND LIMITING SCREEN TIME

Parents should pay close attention to the Internet use of children and young people and intervene if they see risks. However, the privacy of the children and young people should also be respected.

Social media usage should be monitored by parents and screen time should be limited. The American Academy of Pediatrics advises against allowing toddlers under the age of two to spend more than one hour a day in front of a screen, and against allowing kids over the age of six to spend more than two hours a day. Parents can also install parental control software.

And parents must also focus on factors known to have a stronger impact than screen time, such as family functioning, social dynamics and socio-economic conditions¹¹⁷.

Parents should think about "**media diet**" of children¹¹⁸. What children watch on screens is just as important – If not more important – than how much time they spend in front of screens. Parents need to be mindful of what their children see and what games they play. To the extent that it's possible, parents should try to watch and play with their children. With older children, especially those with computers and smart phones, it's important to talk about what they are seeing and doing.

7. MODEL PARENTING

Adults should be role models themselves in dealing with social networks and use them responsibly. Social media use can have positive and negative effects on family connectedness – but it depends on how families use it and talk about it. Research has shown that¹¹⁹:

- Kids are likely to pick up on parents' problematic media use behaviors, including distraction from responsibilities and family time, emotional difficulties and irresponsible posting behaviors. This could influence the kid's own developing relationship with digital media;
- Teens benefit from parents' transparency with their own struggles with managing their social media use;
- Youth may be more receptive to household technology rules that are followed by parents.

8. TECH-FREE ZONES AND IN-PERSON FRIENDSHIPS

Since electronics can be a potential distraction after bedtime and can interfere with sleep, parents should consider restricting the use of phones, tablets, and computers for at least 1 hour before bedtime and through the night. Keeping family mealtimes and in-person gatherings device-free could be a good tradition to build social bonds and engage in a two-way conversation. Children must be encouraged to maintain their in-person relationships by unstructured and offline connections with others and making unplugged interactions a daily priority¹²⁰.

9. WORK WITH OTHER PARENTS

Working with other parents can help establish shared norms and practices and to support programs and policies around healthy social media use. Such norms and practices among parents facilitate collective action and can make it easier to set and implement boundaries on social media use for children.

C. TARGETED PROGRAMS AND ACTIONS FOR SUPPORT COMMUNITY

Support community here includes educators, researchers, social workers, youth workers, youth service organizations, helplines and hotlines in partner countries.

1. SUPPORT AND ASSISTANCE FOR VICTIMS OF ONLINE RISKS

When a child or young person become a victim of bullying, harassment or other risks on social media, they should be offered immediate support and assistance. Specialized counselling centers, psychologists, school pedagogical advisors can help with this issue.

Providing victims of cyberbullying and other forms of online abuse with legal and judicial support is crucial, in addition to counselling programs and helplines. Sexual harassment and cyberbullying is illegal in many countries, and those who have been the victim of it may file a lawsuit. Some victims might not be aware of their legal rights, though, or they might lack the funds to file a lawsuit. Because of this, it's critical to give victims access to legal resources and assistance. To efficiently investigate and pursue cases of internet harassment, law enforcement organizations need also receive proper training.

There are various counselling centers that can help with problems related to social networks and internet use. These include, for example, the online advice from the youth information centers, parent service initiatives and telephone advice hot lines and help lines.

2. INTRODUCTION OF PEER LEARNING PROGRAMS

Designing programs for dealing with most common risks, related to the use of digital technologies and social networks could be highly effective if implemented by young workers. The training of young trainers should be carried out in partnership between NGOs, schools, government institutions and corporate players to achieve the best and long-lasting result.

3. BETTER RESEARCH OF ONLINE HARMS

There are still challenges in the field of online risk research. Studies looking at mental, social or physical well-being have often been correlational or drawn from cross-sectional samples (where the data are taken at only one point in time). From these types of studies, it is difficult to determine what is cause and what is effect; it is also hard to estimate long-term consequences of the use of

digital technology. To assess causality and long-term effects reliably will require longitudinal studies and other improvements in research methodology¹²¹.

Special attention must be paid to young people from marginalized racial, ethnic, sexual, gender, socioeconomic backgrounds, those who are differently abled, and/or youth with chronic developmental or health conditions since relatively few studies have been conducted with marginalized populations of youth, including those¹²².

D. TARGETED PROGRAMS AND ACTIONS FOR DIGITAL COMMUNITY

1. IMPROVING REGULATION OF SOCIAL MEDIA PLATFORMS

Enhancing social media platform regulation is necessary in addition to tougher sanctions for cyberbullying and other types of online abuse. This may entail steps to stop the propagation of hate speech and false information as well as greater openness on the gathering and use of user data. Both holding social media platforms accountable for their deeds and promoting improved regulation of these platforms can be done by governments and civil society organizations.

2. DEVELOPMENT OF SOCIAL NETWORKS INTENDED FOR THE YOUTH

Even though the age limit for users of the most popular social network is 13 years, a significant number of children under this age have their own profile on such a network. The current debate over whether to raise the age limit to 16 only exacerbates the problem. Without a doubt, the restrictions will not prevent children from pursuing their most popular activity. Instead, they should be provided with affordable and attractive alternatives with enhanced security settings that preserve the privacy of young people's and their friends' personal information. Social media sites can help to educate their members. Social media platforms like Facebook and Twitter offer information and tutorials on how to utilize their services properly and safely. Facebook, Instagram and Twitter offer safety centers where users may find out how to safeguard their accounts, report offensive information, and ban individuals who behave inappropriately.

Social media use, functionality, and permissions/ consenting should be tailored to youths' developmental capabilities. Designs created for adults may not be appropriate for children. Specific features (e.g., the "like" button, recommended content, unrestricted time limits, endless scrolling) and notices/ alerts (e.g., regarding changes to privacy policies) should be tailored to the social and cognitive abilities and comprehension of adolescent users¹²³.

Example:

Adolescents should be informed explicitly and repeatedly, in age-appropriate ways, about the manner in which their behaviors on social media may yield data that can be used, stored, or shared with others, for instance, for commercial (and other) purposes.

Other useful actions are:

- **Enforce age limits and age-checking measures¹²⁴** in order underage children to be kept off social media platforms - social media companies set the age limits on their platforms and many of them say children under 13 years of age are not allowed, but many younger children have accounts. Different technologies can be used to check people's ages online - these are called age assurance technologies.
- **Remove illegal content quickly or prevent it from appearing in the first place¹²⁵** – it includes applying measures to prevent social media services to be used for illegal activity and remove illegal content when it does appear. Social media platforms will have to remove illegal content, stopping children and adults from seeing it. Some content that promotes self-harm is already declared for illegal in UK and platforms will need to remove this. Illegal content that platforms will need to remove includes:
 - ☒ child sexual abuse;
 - ☒ controlling or coercive behavior;
 - ☒ extreme sexual violence;
 - ☒ fraud;
 - ☒ hate crime;
 - ☒ inciting violence;
 - ☒ illegal immigration and people smuggling;
 - ☒ promoting or facilitating suicide;
 - ☒ promoting self-harm;
 - ☒ revenge porn;
 - ☒ selling illegal drugs or weapons;
 - ☒ sexual exploitation;
 - ☒ terrorism.
- **Remove content that is harmful or age-inappropriate to children¹²⁶** - some content is not illegal but could be harmful or age-inappropriate for children. Platforms will need to protect children from it. The categories of harmful content that platforms will need to protect children from encountering include:
 - ☒ pornographic content;
 - ☒ content that does not meet a criminal threshold, but which promotes, encourages or provides instructions for suicide, self-harm or eating disorders;
 - ☒ content that depicts or encourages serious violence;

☒ bullying content.

- **Offer to parents tools so they can have greater control over the kinds of content their kids see and who they engage with online¹²⁷** - this includes option of filtering out unverified users, which will help stop anonymous trolls from contacting them and reduce the likelihood that they will encounter certain types of content that promotes or encourages eating disorders or self-harm, or is racist, antisemitic or misogynistic.
- **Provide parents and children with clear and accessible ways to report problems online¹²⁸** when they do arise;
- **The introduction of a pop-up heavy usage warning on social media¹²⁹** - The social media platform would track usage and provide the user with a pop-up warning when they breach a set level of usage deemed potentially harmful. It is then up to the user to decide if they carry on using the platform or stop, although the warning may provide links to information and advice on social media addiction.
- **Social media platforms to highlight when photos of people have been digitally manipulated¹³⁰** - This may be in the form of a small icon or watermark at the bottom of someone's photo that indicates an airbrush or filter has been used that may have significantly altered their appearance. Young people, and in particular young women, are bombarded with images that attempt to pass off the edited as the norm. This practice is contributing to a generation of young people with poor body image and body confidence. Fashion brands, celebrities and other advertising organizations may sign up to a voluntary code of practice where the small icon is displayed on their photos to indicate an image may have been digitally enhanced or altered to significantly alter the appearance of people in it.
- **Social media platforms to identify users who could be suffering from mental health problems by their posts and other data, and discreetly signpost to support¹³¹** – If social media is contributing to poor mental health in young people, we should be utilizing the various platforms to reach and help those who are suffering. The existing stigma around mental health issues, particularly in young people, may make it difficult for those suffering to come forward or even know where to look for help. We would like to see technology used to identify those young people who could be suffering from mental health conditions on social media, and provide

them with discreet information about where they can find help and advice should they wish to receive it.

Technology companies must design, develop, and evaluate platforms, products, and tools that foster safe and healthy online environments for youth, keeping in mind the needs of girls, racial, ethnic, and sexual and gender minorities. The platform design and algorithms should prioritize health and safety as the first principle, seek to maximize the potential benefits, and avoid design features that attempt to maximize time, attention, and engagement.

To reduce the risks of psychological harm, adolescents' exposure to content on social media that depicts illegal or psychologically maladaptive behavior, including content that instructs or encourages youth to engage in health-risk behaviors, such as self-harm (e.g., cutting, suicide), harm to others, or those that encourage eating-disordered behavior (e.g., restrictive eating, purging, excessive exercise) should be minimized, reported, and removed¹³²; moreover, technology should not drive users to this content. Evidence suggests that exposure to maladaptive behavior may promote similar behavior among vulnerable youth, and online social reinforcement of these behaviors may be related to increased risk for serious psychological symptoms, even after controlling for offline influences¹³³. In this respect, reporting structures should be created to easily identify harmful content, and ensure it is deprioritized or removed.

The entertainment industry (and news industry) should be more responsible about how it portrays violence. It should limit gratuitous violence and glamorization of violence, and when violence is portrayed, the pain and loss suffered should be portrayed as well¹³⁴.

3. TRANSPARENT AND INDEPENDENT ASSESSMENTS

Technology companies play a central role and have a fundamental responsibility in designing safe online environments and in preventing, minimizing, and addressing the risks associated with social media. In this respect they should conduct and facilitate transparent and independent assessments of the impact of social media products and services on children and adolescents. Assuming responsibility for the impact of products on different subgroups and ages of children and adolescents, regardless of the intent behind them would be the best strategy for keeping children and young people safe online. This may include¹³⁵:

- Transparent assessment findings and underlying data with independent researchers and the public in a privacy protecting manner;
- Assessment of the potential risks of online interactions and taking active steps to prevent potential misuse, reducing exposure to harms;
- Establish scientific advisory committees of independent experts and members of user subgroups, including youth to inform approaches and policies aimed at creating safe online environments for children.

VI. CONCLUSIONS

Social media could offer both benefits and harms to young people. How teens use social media also might determine its impact:

- **Social media benefits** - social media allows teens to create online identities, communicate with others and build social networks. These networks can provide teens with valuable support, especially helping those who experience exclusion or have disabilities or chronic illnesses. Teens also use social media for entertainment and self-expression. And the platforms can expose teens to current events, allow them to interact across geographic barriers and teach them about a variety of subjects, including healthy behavior. Social media that is humorous and distracting, that provides meaningful connection to peers and a wide social network might even help teens avoid depression.
- **Social media harms** - however, social media use can also negatively affect teens, distracting them, disrupting their sleep, and exposing them to bullying, rumor spreading, unrealistic views of other people's lives and peer pressure. Because of teens' impulsive natures, experts suggest that teens who post content on social media are at risk of sharing intimate photos or highly personal stories. This can result in teens being bullied, harassed or even blackmailed. Teens often create posts without considering these consequences or privacy concerns.

Risks experienced by children are not always easily separated and frequently coincide, with some children more vulnerable to potential harms than others. Significant policy, legal and regulatory initiatives must be developed to provide children's protection and empowerment. In this chapter series of recommendations address the importance of: safety of social networks; suitability of social media content, age-appropriate design and functionality for stage of development of the child; continued policy development in children's privacy; and sustained research in the form of longitudinal studies.

Recommended actions are concluded based on theoretical research and empirical evidence, as well as recent results from international survey, conducted in the partner countries – Bulgaria, North Macedonia, Poland and Austria in 2023.

VII. APPENDIX A: SURVEY QUESTIONNAIRE

W2/A1 SURVEY ON METHODS OF PREVENTION AND OVERCOMING NEGATIVE CONSEQUENCES AMONG YOUNG PEOPLE AS USERS OF THE INTERNET AND SOCIAL NETWORKS

Mark the correct answer with ☒ or ☐

Your name and surname:

You are aged between: ☐ 14-18 ☐ 19-29

Country: City:

Your gender:	<input type="checkbox"/> A man.	<input type="checkbox"/> A woman.
Your status:	<input type="checkbox"/> Study at	<input type="checkbox"/> I'm working.
How do you prefer to communicate with your peers?	<input type="checkbox"/> Online.	<input type="checkbox"/> Live.
When you are on vacation, is it mandatory for you to have internet?	<input type="checkbox"/> Yes .	<input type="checkbox"/> No.
Which social media protection methods do you know?	<input type="checkbox"/> I am not familiar with many methods. <input type="checkbox"/> I don't give my real name. <input type="checkbox"/> I don't accept friend request from strangers. <input type="checkbox"/> I always check whether I know or have mutual acquaintances with the person who sent me an invitation. <input type="checkbox"/> I do not post personal information. <input type="checkbox"/> I don't believe everything posted on the internet. <input type="checkbox"/> I control my information on the Internet. <input type="checkbox"/> Something else.....	
Do you think there are things on the Internet that can harm you?	<input type="checkbox"/> Yes.	<input type="checkbox"/> No.
Did you know that there is a mobile application (App) that monitors how much time you spend on the Internet?	<input type="checkbox"/> Yes.	<input type="checkbox"/> No.
Can you tell fake news from real news?	<input type="checkbox"/> Yes.	<input type="checkbox"/> No.
How will a day without internet access affect you?	<input type="checkbox"/> Terrible, I won't be able to follow what's going on. <input type="checkbox"/> I will have more time for useful things. <input type="checkbox"/> I will be nervous because someone can text me. <input type="checkbox"/> I will lose touch with my contacts. <input type="checkbox"/> It's important to me to maintain my profile.	

	<input type="checkbox"/> It won't affect me. <input type="checkbox"/> Something else.....
What will you do if your social network profile is blocked?	<input type="checkbox"/> I will use another app. <input type="checkbox"/> I will use the time I spend on social media for something else. <input type="checkbox"/> I will panic and look for ways to unblock it. <input type="checkbox"/> I will make a new profile. <input type="checkbox"/> Nothing. <input type="checkbox"/> Something else.....
If you get an invitation to join a group from a stranger, what will you do?	<input type="checkbox"/> I will decline the invitation. <input type="checkbox"/> I will accept the invitation. <input type="checkbox"/> Something else.....
You come across an interesting article on the Internet. How will you verify its authenticity?	<input type="checkbox"/> I won't check. <input type="checkbox"/> I will google for info. <input type="checkbox"/> Will share with friends/relatives. <input type="checkbox"/> I will check the source of the article. <input type="checkbox"/> Something else.....
What are your ways of dealing with cyberbullying?	<input type="checkbox"/> I will watch videos on the Internet on the subject. <input type="checkbox"/> I will talk to relatives and friends. <input type="checkbox"/> I will read about it. <input type="checkbox"/> I don't know how to deal with cyberbullying. <input type="checkbox"/> Something else.....
If a friend suggested you follow a popular trend, what would you do?	<input type="checkbox"/> I will follow. <input type="checkbox"/> I will look for trend information. <input type="checkbox"/> I will watch videos on TikTok . <input type="checkbox"/> I will not follow.
You use social networks because:	<input type="checkbox"/> To find out what others think of me. <input type="checkbox"/> To compare my life with that of others. <input type="checkbox"/> I have fun and fill my spare time. <input type="checkbox"/> I connect with friends. <input type="checkbox"/> I keep in touch with relatives. <input type="checkbox"/> Something else.....
Do you share your negative experiences online with anyone?	<input type="checkbox"/> Yes, with..... <input type="checkbox"/> I don't share. <input type="checkbox"/> I would like to, but I don't know with whom. <input type="checkbox"/> I ignore the problem.
How do you deal with bullying on social media?	<input type="checkbox"/> I'm deleting the app. <input type="checkbox"/> I ignore the problem. <input type="checkbox"/> I block the profile that harasses me. <input type="checkbox"/> I feel guilty about the problem. <input type="checkbox"/> I respond to bullying with aggression. <input type="checkbox"/> Share with..... <input type="checkbox"/> Something else.....

Have you come across videos with "sensitive content"?	<input type="checkbox"/> Yes, often. <input type="checkbox"/> Yes, but I skip them. <input type="checkbox"/> Rarely. I have sensitive content controls. <input type="checkbox"/> No. <input type="checkbox"/> Something else.....
How do you protect yourself from "sensitive content" video on your social network?	<input type="checkbox"/> I'm changing my profile filter. <input type="checkbox"/> I'm blocking the profile that shared the video. <input type="checkbox"/> I look out of curiosity. <input type="checkbox"/> Share with <input type="checkbox"/> Something else.....
When you receive a message with hate language (Hate messages) , You:	<input type="checkbox"/> I reply to the message in the same tone. <input type="checkbox"/> I ignore it. <input type="checkbox"/> I don't read messages from unknown profiles. <input type="checkbox"/> I answer in a positive tone. <input type="checkbox"/> I delete it. <input type="checkbox"/> I block the sender. <input type="checkbox"/> Something else.....
Have you personally sent such messages?	<input type="checkbox"/> Yes. <input type="checkbox"/> It has happened to me, some people are provoking it. <input type="checkbox"/> I avoid sending such messages. <input type="checkbox"/> I haven't had to.
Do you know what is misuse of personal and/or financial data on the Internet?	<input type="checkbox"/> Yes, I am familiar. <input type="checkbox"/> I have no information. <input type="checkbox"/> I would like to know.
What methods of protection against misuse of personal and/or financial data do you know?	<input type="checkbox"/> Password protection with additional app or two-factor password. <input type="checkbox"/> The best way is to not provide actual personal information. <input type="checkbox"/> I do not share personal and financial information. <input type="checkbox"/> Antivirus program on the device. <input type="checkbox"/> I do not use. <input type="checkbox"/> Something else.....
If you find out that your friend has an addiction to social networks, how will you help him?	<input type="checkbox"/> I don't see anything wrong with that. <input type="checkbox"/> I will suggest them to delete the app. <input type="checkbox"/> I will talk to them about using them less often. <input type="checkbox"/> I will share with their parents. <input type="checkbox"/> I will look for information for adequate help. <input type="checkbox"/> I don't know how to help. <input type="checkbox"/> Something else.....
How will you protect yourself if an unknown profile writes to you and asks to meet you?	<input type="checkbox"/> If I like it, I'll text them for a while and then we'll see each other live. <input type="checkbox"/> I block the profile. <input type="checkbox"/> I don't reply to the message and delete it. <input type="checkbox"/> I will share with

	<input type="checkbox"/> I will answer, not everyone is malicious. <input type="checkbox"/> I will answer out of curiosity and go to the meeting.
Do you personally send such invitations?	<input type="checkbox"/> Yes, that's how I look for new acquaintances. <input type="checkbox"/> I have a limited personal life and that's how I find friends. <input type="checkbox"/> Very rarely. <input type="checkbox"/> No.
Have you received provocative photos?	<input type="checkbox"/> Yes. <input type="checkbox"/> No.
Have you sent provocative photos that you wouldn't post on the Internet?	<input type="checkbox"/> Yes. <input type="checkbox"/> No.

VIII. REFERENCES

1. Ilieva, D., Law and Internet Foundation, How to overcome digital addiction?, <https://www.netlaw.bg/bg/a/digitalna-zalgalka> Digital pacifier
2. Cambridge Dictionary, <https://dictionary.cambridge.org>, 2024
3. Online experiences of children in Bulgaria: risks and safety, <https://www.safenet.bg/wp-content/uploads/2015/05/risks-and-harm.pdf>
4. International Telecommunication Union, Guidelines for policy-makers on Child Online Protection, 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.POL_MAKERS-2020-PDF-E.pdf
5. Digistress.eu/wp-content/uploads/2021/03/best-practice-bg.pdf Examples of project practice: "Digital stress skills training in the form of a web-based application"
6. <https://www.newportacademy.com/resources/empowering-teens/positives-of-social-media/> What Are the Positives of social media for teens?
7. <https://www.fulbright.bg/en/media-literacy-for-teachers/>, (<https://www.irex.org/program/opportunity-international-teachers-fulbright-teaching-excellence-and-achievement-program-1>)
8. Media Literacy in the Classroom, Handbook of the "Association of European Journalists in Bulgaria", jointly with the "America for Bulgaria" Foundation
9. <https://www.safenet.bg/bg/>
10. Digital Scouts 2023, <https://www.yettel.bg/digital-scouts>, 2024
11. Project "BE SAFE ON THE INTERNET", <https://narpbg.com/?p=91>, 2024
12. КАИРОС, Журнал за медиуми и комуникации, https://respublica.edu.mk/wp-content/uploads/2022/06/kairos-zhurnal-za-mediumi-i-komunikacii-br1-juni-2022_mk.pdf
13. Republic of Macedonia national cyber security strategy 2018 – 2022, https://www.itu.int/en/itu-d/cybersecurity/documents/national_strategies_repository/ns%20cyber%20security%202018-2022_eng.pdf
14. КАИРОС, Журнал за медиуми и комуникации, https://respublica.edu.mk/wp-content/uploads/2022/06/kairos-zhurnal-za-mediumi-i-komunikacii-br1-juni-2022_mk.pdf
15. University of Pittsburgh, Safety Tips for Social Networking, <https://services.pitt.edu/TDClient/33/Portal/KB/ArticleDet?ID=42>, 2024
16. Tabea Bork-Hüffer, Belinder Mahlknecht, Katja Kaufmann: (Cyber)Bullying in schools – when bullying stretches across cON/FFlating spaces. In: children's geographies. 2021, VOL. 19, NO.2, page 241 – 253.
17. S. Wójcik, Children count 2022. Report on threats to the safety and development of children in Poland, Threats to children and youth related to the use of the Internet, Foundation "Dajemy dzieciom siłę".
18. M. Bochenek, Z. Polak, K. Silicki, A.Wrońska, Guide for Parents „How to keep children safe on the Internet”, Research Institute Nask.
19. M. Bochenek, Z. Polak, K. Silicki, A.Wrońska, Guide for Parents „How to keep children safe on the Internet”, Research Institute Nask.
20. Lehrende, saferinternet.at, <https://www.saferinternet.at>, 2023
21. Media education, mediamanual.at, <https://www.mediamanual.at>, 2023
22. Youth Media and Information - Federal Chancellery of Austria, <https://www.bundeskanzleramt.gv.at>
23. Klicksafe.de: Die EU-Initiative für mehr Sicherheit im Netz, <https://www.klicksafe.de>, 2023
24. Net Nanny: Parental Control Software & Website Blocker, <https://www.netnanny.com>
25. SaferKid, <https://www.saferkid.com>, 2023
26. Home, saferinternet.at, <https://www.saferinternet.at>, 2023
27. Federal Chancellery of Austria, Youth Media and Information, <https://www.bundeskanzleramt.gv.at>
28. Die EU-Initiative für mehr Sicherheit im Netz, <https://www.klicksafe.de>, 2023
29. Die EU-Initiative für mehr Sicherheit im Netz, <https://www.klicksafe.de>, 2023
30. Eltern-Medien-Beratung, Medienpädagogik, <https://www.bpb.de>
31. Die EU-Initiative für mehr Sicherheit im Netz, <https://www.klicksafe.de>, 2023
32. BEE SECURE, <https://www.bee-secure.lu/fr/>, 2023
33. Internet-ABC, <https://www.internet-abc.de>, 2023
34. Die Projekteplattform von netbridge, www.jugendserver.at, 2023

35. EduGroup, Medienfit 2020 - YouTube, <https://www.edugroup.at/praxis/portale/medienfit-in-der-volksschule/die-initiative/medienfit-2020-youtube.html>, 2023
36. Ratgeber - Sicheres-Netz.com
37. Digitales Lernen (oad.at)
38. Sicher im Netz | Tiroler Bildungsservice tibs.at
39. Medien.werkstatt: Medienbildung und -kompetenz in Salzburg - FS1
40. University of Graz, <https://www.uni-graz.at/de/>, 2023
41. #Hass im Netz, Land Kärnten, ktn.gv.at, 2023
42. DigiPros: Junge digitale Expertinnen und Experten, JugendService OÖ
43. #makelTsafe2.0 - Regionales Jugendmanagement Steirischer Zentralraum (jungimzentralraum.at)
44. Antenne macht Schule | Antenne Steiermark
45. Best practice heft 2020.pdf mediamanual.at
46. Volksschule Liezen - Projekte - Aktiv gegen Cyber – Mobbing
47. International Telecommunication Union, Measuring digital development, Facts and figures 2019, <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf>
48. The Council of Europe, Lanzarote Convention, <https://www.coe.int/en/web/children/lanzarote-convention>, 2024
49. European Crime Prevention Network, A TABBY (Threat assessment of bullying behavior in youth) in internet and TABBY trip in EU, <https://rb.gy/u0exy3>, 2024
50. UNICEF Albania, Safer and better internet for children and youth in Albania, <https://www.end-violence.org/grants/unicef-albania>, 2024
51. The Bulletin, New game may decrease bullying, <https://www.thebulletin.be/new-game-may-decrease-bullying>, 2024
52. Croga.fi. I take the responsibility initiative. <https://eucpn.org/document/croga-fi-i-take-the-responsibility-online-self-help-material>, 2024
53. Preventing child sexual abuse, <https://eucpn.org/sites/default/files/document/files/finlandecpa2015.pdf>
54. DigiCAMP project, <https://www.digicamp-project.eu/en/>, 2024
55. Verklückt! Der Gesamtfilm. <https://www.youtube.com/watch?v=E6H5t7gr75w>, 2024
56. Opfer, Schlampe, Hurensohn - Gegen Mobbing. <https://jugendhilfeportal.de/material/opfer-schlampe-hurensohn-gegen-mobbing>, 2024
57. Das Programm Medienhelden, <https://www.medienhelden.info/das-programm.html>, 2024
58. Italian Safer Internet Centre - Generazioni Connesse, <https://www.saferinternetday.org/in-your-country/italy>, Last updated: 2024-01-25, 2024
59. <https://www.positiveonlinecontentforkids.eu/examples/article?id=4981536>
60. Juvenile Inspectors of The State Police, https://eucpn.org/sites/default/files/document/files/LV_1.pdf
61. The Cyber Mobbing Guide, <https://police.public.lu/fr/prevention/cyber-mobbing.html>
62. European Crime Prevention Network, The White Dot Tolerance Project, <https://shorturl.at/cjuNU>, 2024
63. <https://stopline.sk/sk/uvod/>
64. <http://www.workbasedtraining.eu/en/partners/the-partners/rcr-regionalni-center-za-razvoj-d-o-o/>
65. Rosario Ortega-Ruiz, Rosario Del Rey, José A. Casa, Knowing, Building and Living Together on Internet and Social Networks: The ConRed Cyberbullying Prevention Program, International Journal of Conflict and Violence, 2012, 6(2):303-313, <https://rb.gy/rcv62j>, accessed Apr 04 2024
66. Rosario Ortega-Ruiz, Rosario Del Rey, José A. Casa, Knowing, Building and Living Together on Internet and Social Networks: The ConRed Cyberbullying Prevention Program, International Journal of Conflict and Violence, 2012, 6(2):303-313, <https://rb.gy/rcv62j>, accessed Apr 04 2024
67. <https://www.bbc.com/news/technology-49726844>
68. <https://www.internetmatters.org/resources/bbc-own-it/>
69. <https://projectevolve.co.uk/>
70. <https://360safe.org.uk/>
71. <https://360safe.org.uk/overview/>
72. UNICEF, Children's experiences online - building global understanding and action, <https://www.unicef-irc.org/publications/1065-childrens-experiences-online-building-global-understanding-and-action.html>

-
73. Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online. October 2019 Dr. Joanna Rubinstein
74. <https://inhope.org/EN/articles/what-is-the-international-child-sexual-exploitation-icse-database>
75. <https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database>
76. <https://www.dqinstitute.org/wp-content/uploads/2020/02/2020COSIReport.pdf>
77. <https://safeonline.global/a-major-victory-for-children-in-peru-as-country-brings-in-new-law-to-tackle-online-csea/>
78. <https://krmangalam.com/blogs/how-to-save-kids-from-social-media-addiction/>
79. <https://www.dqinstitute.org>
80. <https://www.end-violence.org/grants/plan-international-vietnam>
81. Child Online Protection in Rwanda, <https://5rightsfoundation.com/uploads/cop-in-rwanda-report.pdf>
82. eSafety Commissioner, <https://www.esafety.gov.au>
83. DigitalCitizenship, eSafety Toolkit for Schools, <https://www.digitalcitizenship.nsw.edu.au/resources/esafety-toolkit-for-schools#:~:text=Key%20message&text=The%20eSafety%20Toolkit%20for%20schools,support%20online%20safety%20and%20wellbeing>
84. New Zealand Parliamentary Counsel Office, New Zealand Legislation, Harmful Digital Communications Act 2015, <https://www.legislation.govt.nz/act/public/2015/0063/latest/versions.aspx>, 2023
85. Facebook, Reporting a violation or infringement of your rights, <https://www.facebook.com/help/181495968648557>, 2021
86. Instagram, Reporting a violation or infringement of your rights, <https://help.instagram.com/165828726894770>, 2021
87. Georgieva M., et al, 2024, "Research on current risks among young people as users of social networks", Project 2022-1-BG-01-KA220-YOU-000085174, Prevention of youth risky viral trends, Erasmus+
88. The CO:RE classification of online risk to children, Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung, Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence
89. OECD, Children in the digital environment - revised typology of risks, https://www.oecd-ilibrary.org/science-and-technology/children-in-the-digital-environment_9b8f222e-en;jsessionid=4zJInbcr2m-dEbDh40st6AEv.ip-10-240-5-100about:blank, 2021
90. United Nations Children's Fund (UNICEF), The state of the world's children, Children in a Digital World, <https://www.unicef.org/bulgaria/media/421/file/State%20of%20the%20world's%20children%20-%20children%20in%20a%20digital%20age.pdf>, 2017, p.104
91. Social Media Security Tools and Tips to Mitigate Risks, <https://blog.hootsuite.com/social-media-security-for-business/>, 2024
92. Cynthia Vinney, Media Literacy in the Modern Age, How to understand the messages we observe all day every day, <https://www.verywellmind.com/what-is-media-literacy-5214468>, October 26, 2023
93. Society for Media Psychology & Technology, About the Society for Media Psychology & Technology, Division 46 of the American Psychological Association, <https://www.apadivisions.org/division-46/about>, 2013, accessed 2024
94. Dill-Shackleford KE. *How Fantasy Becomes Reality*. New York: Oxford University Press; 2009
95. Common Sense Media. Digital citizenship, Common Sense Education, <https://www.commonsense.org/education/digital-citizenship>, 2019, May 10.
96. Magis-Weinberg, L., Muñoz Lopez, D. E., Gys, C. L., Berger, E. L., & Dahl, R. E. (2022). Short research article: Promoting digital citizenship through a school-based intervention in early adolescence in Perú (a pilot quasi-experimental study). *Child and Adolescent Mental Health*. Advance online publication. <https://doi.org/10.1111/camh.12625>
97. Balt, E., Mérelle, S., Robinson, J., Popma, A., Creemers, D., van den Brand, I., van Bergen, D., Rasing, S., Mulder, W., & Gilissen, R. (2023). Social media use of adolescents who died by suicide: Lessons from a psychological autopsy study. *Child and Adolescent Psychiatry and Mental Health*, 17(1), 48. <https://doi.org/10.1186/s13034-023-00597-9>

-
98. Potter WJ. Media Literacy. 4th ed. Los Angeles: SAGE; 2008.
99. Dill-Shackleford KE. How Fantasy Becomes Reality. New York: Oxford University Press; 2009.
100. Gaudin, S. (2019). Social media privacy: A comparison of current privacy settings across various social media platforms. *Journal of Technology Research*
101. Jensen, C., Potts, C., Jensen, K. B., & Christensen, L. T. (2015). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Communication*
102. Risks and Harms for Children in the Digital Age.... Cited in United Nations Children's Fund (UNICEF), THE STATE OF THE WORLD'S CHILDREN 2017, Children in a Digital World, <https://www.unicef.org/bulgaria/media/421/file/State%20of%20the%20world's%20children%20-%20children%20in%20a%20digital%20age.pdf>,
103. Harel, T. 7 Best Practices for Coping With Online Sexual Harassment, <https://msmagazine.com/2020/10/08/7-best-practices-for-coping-with-online-sexual-harassment/>, 10/8/2020
104. TERRI HAREL, Seven Best Practices for Coping With Online Sexual Harassment, <https://msmagazine.com/2020/10/08/7-best-practices-for-coping-with-online-sexual-harassment/>, 10/8/2020
105. Radesky, J. S., Christakis, D. A., Hill, D. A., Mendelsohn, A. L., & Committee on Public Education. (2016). Media and Young Minds. *Pediatrics*
106. American Academy of Pediatrics. (2016). Media and Young Minds. *Pediatrics*
107. AMERICAN PSYCHOLOGICAL ASSOCIATION, Health Advisory on Social Media Use in Adolescence, <https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use>, MAY 2023
108. Boer, M., Stevens, G. W. J. M., Finkenauer, C., & van den Eijnden, R. J. J. M. (2022). The course of problematic social media use in young adolescents: A latent class growth analysis. *Child Development*, 93(2), e168–e187. <https://doi.org/10.1111/cdev.13712>
109. LaFrance, Adrienne, 'The Perils of "Sharenting"', *The Atlantic*, 6 October 2016
110. Lisa Belkin. 2013. Humiliating Children in Public: A New Parenting Trend? In HUFFINGTON POST.
111. Stacey. B Steinberg. 2017. Sharenting: Children's Privacy in the Age of Social Media. In *Emory Law Journal*, 66(4), 839-884.
112. University of Michigan Health System. 2015. Sharenting' trends: Do parents share too much about their kids on social media? In *ScienceDaily*. DOI: www.sciencedaily.com/releases/2015/03/150316092805.htm
113. Steinberg, Stacey B., 'Sharenting: Children's privacy in the age of social media', University of Florida Levin College of Law Legal Studies Research Paper Series, vol. 66, 839, 2016
114. AVG Technology. 2010. Digital Birth: Welcome to the Online World. In *Business Wire*, cited in United Nations Children's Fund (UNICEF), THE STATE OF THE WORLD'S CHILDREN 2017, Children in a Digital World, <https://www.unicef.org/bulgaria/media/421/file/State%20of%20the%20world's%20children%20-%20children%20in%20a%20digital%20age.pdf>, p.92
115. Steinberg, Stacey B., 'Sharenting: Children's privacy in the age of social media', University of Florida Levin College of Law Legal Studies Research Paper Series, vol. 66, 839, 2016
116. Organisation for Economic Co-operation and Development, 'The Protection of Children Online: Risks faced by children online and policies to protect them', OECD Digital Economy Papers No. 179, OECD Publishing, Paris, 2011, p. 37.
117. United Nations Children's Fund (UNICEF), THE STATE OF THE WORLD'S CHILDREN 2017, Children in a Digital World, <https://www.unicef.org/bulgaria/media/421/file/State%20of%20the%20world's%20children%20-%20children%20in%20a%20digital%20age.pdf>, p.109
118. Claire McCarthy, MD, Protecting children from the dangers of virtual violence, Harvard Health Publishing, <https://www.health.harvard.edu/blog/protecting-children-dangers-virtual-violence-2016080210036>, October 6, 2021
119. American Academy of Pediatrics, Healthy Parenting and Digital Media Use, <https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/qa-portal/qa-portal-library/qa-portal-library-questions/healthy-parenting-and-digital-media-use/>, Last Updated 10/18/2023
120. Morgan Stanley Alliance For Children's Mental Health & Child Mind Institute. (2022, May). How to set limits on screen time and internet use. Retrieved from <https://www.morganstanley.com/assets/pdfs/setting-limits-on-screen-time-tip-sheet.pdf>

- 121.** United Nations Children's Fund (UNICEF), THE STATE OF THE WORLD'S CHILDREN 2017, Children in a Digital World,
<https://www.unicef.org/bulgaria/media/421/file/State%20of%20the%20world's%20children%20-%20children%20in%20a%20digital%20age.pdf>, p.110
- 122.** AMERICAN PSYCHOLOGICAL ASSOCIATION, Health Advisory on Social Media, Use in Adolescence,
<https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use>, MAY 2023
- 123.** Introduction to the Age appropriate design code, ICO. (n.d.), <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>, Retrieved April 20, 2023
- 124.** Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport, UK, A guide to the Online Safety Bill, <https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill>, Last updated 30 August 2023
- 125.** Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport, UK, A guide to the Online Safety Bill, <https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill>, Last updated 30 August 2023
- 126.** Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport, UK, A guide to the Online Safety Bill, <https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill>, Last updated 30 August 2023
- 127.** Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport, UK, A guide to the Online Safety Bill, <https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill>, Last updated 30 August 2023
- 128.** Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport, UK, A guide to the Online Safety Bill, <https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill>, Last updated 30 August 2023
- 129.** Royal Society for Public Health, Status of Mind: Social media and young people's mental health and well-being, 2017, <https://www.rsph.org.uk/our-work/campaigns/status-of-mind.html>,
<https://www.rsph.org.uk/static/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf>
- 130.** Royal Society for Public Health, Status of Mind: Social media and young people's mental health and well-being, 2017, <https://www.rsph.org.uk/our-work/campaigns/status-of-mind.html>,
<https://www.rsph.org.uk/static/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf>
- 131.** Royal Society for Public Health, Status of Mind: Social media and young people's mental health and well-being, 2017, <https://www.rsph.org.uk/our-work/campaigns/status-of-mind.html>,
<https://www.rsph.org.uk/static/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf>
- 132.** Tools and tips to help communicate safely online about suicide - #chatsafe - Orygen, Revolution in Mind. (n.d.). Retrieved April 20, 2023, from <https://www.orygen.org.au/chatsafe>.
- 133.** Nesi, J., Rothenberg, W. A., Hussong, A. M., & Jackson, K. M. (2017). Friends' alcohol-related social networking site activity predicts escalations in adolescent drinking: Mediation by peer norms. *Journal of Adolescent Health*, 60(6), 641–647. <https://doi.org/10.1016/j.jadohealth.2017.01.009>
- 134.** Claire McCarthy, MD, Protecting children from the dangers of virtual violence, Harvard Health Publishing, <https://www.health.harvard.edu/blog/protecting-children-dangers-virtual-violence-2016080210036>, October 6, 2021
- 135.** Social Media and Youth Mental Health, The U.S. Surgeon General's Advisory, 2023, accessed on 20 feb 2024, <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf>

Follow me Association, Bulgaria, 2024

ISBN 978-619-92834-2-4(print edition) ISBN 978-619-92834-3-1 (e-book PDF)

For more information about the project:

e-mail: follow.me.association@gmail.com

web: <https://followmebg.com>

Social media: <https://www.facebook.com/PreventionYouthRiskyViralTrends>