



CONSCIOUS YOUTH BEHAVIOURS.
IN EMERGING REALITIES

EU Comparative Report on cyber resiliency and cyber threats

R2.1 Comparative study



Co-funded by
the European Union

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.

Document Information

Grant Agreement #	2023-1-EL01-KA220-SCH-000156982
Acronym	C.Y.B.E.R.
Title	Conscious Youth Behaviours in emerging realities
Start Date:	28/02/2024
Result:	EU Comparative Report
Related Activities:	A2.1 Comparative study on cyber resiliency and threats
Lead Organisation:	PRISM Impresa Social s.r.l.
Contributing Partners:	<ul style="list-style-type: none"> ▪ SIGMA Tournis Symvouleftiki EE, Greece ▪ Centrul Judetean De Resurse Si De Asistenta Educationala Botosani, Romania ▪ CPM-Centrum Prevencie Mladeze, Slovakia ▪ Casa Do Professor, Portugal
Dissemination Level	PU: Public
Disclaimer	<i>The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein</i>

Document History

Date	Submitted by	Reviewed by	Version (Notes)
30/04/2024	PRISM	All Partners	V0.0
22/05/2024	All Partners	PRISM	V0. Peer-review/feedback
31/05/2024	PRISM	All Partners	Final_public



This Document is published under an [Attribution-NonCommercial 4.0 International](https://creativecommons.org/licenses/by-nc/4.0/) license [CC BY-NC].

About CYBER	
Action type	Erasmus+ KA220-SCH - Cooperation partnerships in school education
Priority	<p><i>SCHOOL EDUCATION: Development of key competences</i></p> <ul style="list-style-type: none"> ▪ Addressing digital transformation through development of digital readiness, resilience and capacity ▪ Inclusion and diversity in all fields of education, training, youth and sport
<p><i>The project aims to address a crucial question: How does cyberspace influence human behaviour, particularly among young people? In today's digital age, online behaviour has become deeply embedded in the psychological environment of cyberspace. It offers unique opportunities for shaping human interaction but also raises concerns due to its borderless nature. While the internet brings undeniable social and economic benefits, it has challenged core European values such as equality, human rights, and democracy. To build a safer internet, a collective effort is essential. Sharing best practices and educating young generations, teachers, and parents are pivotal steps toward fostering a safer online environment.</i></p> <p><i>CYBER strives to develop the cyber resilience of European schools by creating tailored EU quality procedures for the school system, and by equipping the professors and students with the tools and knowledge to discuss conscious and unconscious online behaviours of adolescents, cyberpsychology and the downsides of the Internet overuse, to enhance the classrooms understanding of the dangerous emerging behaviours a young user may incur.</i></p> <p><i>CYBER is going to structure a methodology to integrate the crucial topics of cyberthreats and cyberpsychology within the classroom and the school system, fostering dialogue among students on the dangerous emerging behaviours towards themselves and their peers. In addition, the project sets clear procedures on cyber and data protection to have schools obtain the CYBER certification, requirements for establishing, implementing, maintaining and improving information security management at school.</i></p> <p><i>The project results are meant to benefit every adolescent in every European country, especially those who were born in the digital era. The social context in these matters (hacking of profiles, fake news, fake identities, online fraud/scam, online blackmailing, revenge porn, hikikomori, cyberbullying, etc.) holds a stronger value, where the education and awareness of young people on the problem have a way greater impact than a national rule.</i></p>	

The sole responsibility of this publication lies with the author.

The European Union is not responsible for any use that may be made of the information contained therein.



Table of contents

Table of contents.....	4
Introduction.....	5
Methodology	6
MACRO Level - Policy Frameworks.....	8
MESO Level - School Communities.....	10
MICRO Level - Youth Insights	12
Identification of Cyber Threats.....	15
National Perspectives	17
GREECE	18
ITALY	28
PORTUGAL.....	37
ROMANIA.....	45
SLOVAKIA.....	57
SWOT Analysis	68
Conclusions.....	70





Introduction

This report provides a detailed comparative analysis of cyber resilience initiatives across five European countries—Greece, Italy, Portugal, Romania, and Slovakia. The focus is particularly on how these initiatives influence and support school-aged youth, specifically those between 14 to 17 years of age.

This report aims to provide a holistic view of the state of cyber resilience among Europe's youth. It seeks to highlight effective practices, identify gaps in current approaches, and recommend strategies for enhancing cyber resilience that are informed by a nuanced understanding of the varied layers of influence.

The ultimate goal of this comparative study is to equip policymakers, educators, and stakeholders with the knowledge and tools needed to enhance the digital safety landscape. It aims to foster a safer online environment where young people are both aware of and equipped to deal with the cyber challenges they face, thus ensuring they can fully engage with and benefit from the digital world.

This report is structured to examine these measures across three critical levels:

- **MACRO Level - Policy Frameworks:** At the macro level, the report evaluates national cybersecurity strategies and policies. It analyses how these frameworks are designed to protect young netizens and the broader educational ecosystem from cyber threats. This level also considers the alignment of national policies with European Union directives and their effectiveness in fostering a secure and resilient digital environment for youth.
- **MESO Level - School Communities:** The meso level focuses on the implementation of cyber resilience strategies within school communities. It looks at how schools integrate cybersecurity into their curricula, the role of educators in promoting digital safety, and the effectiveness of partnerships between schools and external entities such as law enforcement and cybersecurity firms. This level is crucial for understanding the practical applications of national policies and the direct impact on the student body.
- **MICRO Level - Youth Insights:** At the micro level, the report delves into the perceptions and behaviours of the youth regarding their online safety and digital practices. It includes data from surveys and focus groups that reveal how students perceive the cyber threats they face, their knowledge and practice of safe online behaviours, and the psychological impact of cyber incidents. This level provides insight into the direct outcomes of educational initiatives and policy implementations on individual students.

Methodology

In the pursuit of understanding the intricacies of cyber resilience and digital safety among today's European youth, the CYBER Project Committee carried out a comprehensive international research endeavour across Greece, Italy, Portugal, Romania, and Slovakia, this study draws upon insights from various stakeholders, including engagement with 210 young individuals, 5 schools, and consultations with 5 national/local police departments for cyber protection.

In order to conduct a thorough and effective comparative study on cyber resilience and cyber threats across the five European countries involved in the CYBER project, a variety of research methods and tools were adopted. These methods were designed to capture detailed insights at different levels of analysis—macro, meso, and micro—ensuring a comprehensive understanding of the cybersecurity landscape from policy frameworks to individual youth experiences.

1. Desk Research

At the macro level, desk research played a foundational role in gathering existing data, reports, and documentation on national cybersecurity policies and frameworks. This method involved:

- **Policy Analysis:** Reviewing government documents, legislation, and strategies related to cybersecurity and education.
- **Literature Review:** Examining academic and industry literature to understand the broader context of cyber resilience education and its challenges.

2. Surveys

Surveys were extensively used, particularly at the micro level, to collect data directly from the primary stakeholders—students and educators within school communities. These surveys were designed to:

- **Assess Knowledge and Awareness:** Determine the level of cyber threat awareness and digital literacy among students and teachers.
- **Evaluate Impact:** Understand the personal impact of cyber threats on students, including psychological effects and behavioural changes.

3. Interviews

Structured interviews were conducted with key stakeholders at both the macro and meso levels. These included:

- **Cyber Security Police and Experts:** Interviews with those involved in the development and implementation of national cybersecurity strategies provided insights into the goals and challenges of these policies.
- **School Administrators and Teachers:** These interviews helped to uncover the practical challenges and successes in integrating cyber resilience into the educational curriculum.

4. Best Practices

Best Practices were used primarily at the meso level to provide detailed examples of how specific schools or local communities have successfully implemented cybersecurity measures or faced particular challenges. This method involved:

- **In-depth Analysis:** Detailed exploration of particular instances where cybersecurity education programs were either successful or encountered significant obstacles.
- **Comparative Analysis:** Comparing these instances across different contexts to identify factors that influence outcomes.

The study ensured a holistic understanding of the cyber landscape by aligning research methods to specific objectives:

Country-Specific Analysis:

- To develop in-depth examination of cyber resiliency initiatives and educational methodologies in the participating countries.
- To study existing programs, curricula, and awareness initiatives targeted at online users within the school setting.

Identification of Best Practices:

- To identify and analyse successful approaches utilised by countries with notable levels of cyber resiliency.
- To recognize effective strategies, tools, and techniques employed to educate users about cyber threats and promote critical thinking online.

Consultation with National Police Departments:

- To engage in consultations with national police departments to gather valuable insights on prevalent cyber threats, emerging trends, and challenges encountered by law enforcement.
- To provide a real-world perspective on the cyber landscape, informing the development of educational strategies.

Consultation with Schools:

- To engage with schools and understand their approach to cyber resiliency education and digital literacy.
- To identify specific challenges faced by schools in implementing digital safety measures and recommending improvements or additional resources.

Youth survey:

- To assess the level of digital literacy among youth, including their understanding of online safety measures, their engagement with digital safety education, and their confidence in recognizing and responding to cyber threats.
- To gain insight into how young individuals perceive and experience digital safety issues, including cyberbullying, online conduct, and awareness of potential online threats.



MACRO Level - Policy Frameworks

In the comparative analysis of national cybersecurity strategies, the aim was to develop an international-level understanding while focusing on strengths and commonalities across the five countries. By synthesising insights from police department interviews and in-depth research conducted in Greece, Italy, Slovakia, Portugal, and Romania, it provides a macro-level perspective on the cybersecurity landscape. Representatives from the 5 National/local police departments for cyber protection have been interviewed to gather valuable information and insights. This approach enriched the study by incorporating real-world perspectives and expertise from law enforcement agencies, enhancing the comprehensiveness and relevance of findings.

Greece has implemented robust cybersecurity measures anchored by the Law 4577/2018, which aligns with the EU's NIS Directive. The General Directorate of Cyber Security, established in 2018, oversees the strategic implementation of these policies. Educational initiatives are significant, with the Greek Safer Internet Center and the Hellenic Police providing resources and programs to enhance digital literacy and safety awareness among the youth. These efforts reflect Greece's commitment to creating a secure digital culture that extends from governmental agencies to classroom settings.

Italy established the National Cybersecurity Agency (ACN) in 2021, marking a pivotal step in centralising and strengthening the country's cybersecurity initiatives. The agency is tasked with implementing Italy's National Cybersecurity Strategy, emphasising resilience and safety in cyberspace. Educational efforts are robust, incorporating digital citizenship into school curriculums through initiatives like CyberChallenge.IT, which is aimed at nurturing young cybersecurity talents. Italy's approach is comprehensive, integrating cutting-edge training and awareness programs within its educational framework.

Portugal established the National Cybersecurity Center (CNCS) in 2014 and the Portuguese cybersecurity strategy is exemplified by its forward-thinking in digital rights, as encapsulated in the Portuguese Charter of Human Rights in the Digital Age, adopted in 2021. This charter underpins the country's legislative approach to cybersecurity, emphasising the protection of personal data and privacy online. Collaborative efforts between law enforcement and educational institutions underscore the national commitment to promoting cyber awareness and safety, particularly among students.

Romania coordinates its cybersecurity efforts through the National Cyber Security Directorate, which ensures compliance with EU regulations while addressing domestic cyber threats (Government Decision no 1321/2021 - Romania's Cybersecurity Strategy for the period 2022-2027). The country has focused on integrating cybersecurity awareness into the educational sector (by implementing the violence procedure, as defined in Order 6235/2023, issued by the Ministry of Education), partnering with national police units to deliver programs that educate and protect young internet users. Romania's approach is comprehensive, ensuring that cybersecurity measures are interwoven with national education policies.

Slovakia's National Cyber Security Strategy underscores the integration of cybersecurity into educational initiatives, with a strong emphasis on public-private partnerships to enhance digital skills among the youth. The strategy includes engaging local law enforcement in educational roles to provide real-world insights into cybersecurity threats, which is crucial for developing practical and effective cyber resilience skills among students.

Legislative Frameworks:

- All five countries have established legislative frameworks to address cybersecurity concerns, often aligning with EU directives and regulations.
- These frameworks typically include laws, decrees, or strategies aimed at ensuring network security, incident reporting, data protection, and compliance with international cybersecurity standards.

National Cybersecurity Agencies or Authorities:

- Each country has designated a national cybersecurity agency or authority responsible for coordinating cybersecurity efforts, setting standards, and implementing strategies.
- These agencies serve as central hubs for cybersecurity planning, response, and cooperation, playing a vital role in safeguarding national interests in cyberspace.

Digital Education and Awareness:

- Digital education and awareness campaigns are common across all countries, with a strong emphasis on promoting safe online practices and fostering digital literacy.
- Initiatives targeting youth, schools, and communities aim to raise awareness about cyber threats, educate individuals on cybersecurity best practices, and promote responsible digital behaviour.

Public-Private Partnerships:

- Collaboration between government entities, law enforcement agencies, private organisations, and NGOs is evident in cybersecurity initiatives.
- Public-private partnerships play a crucial role in enhancing cyber resilience, sharing threat intelligence, and coordinating response efforts to mitigate cyber threats effectively.

Compliance with EU Regulations:

- All countries demonstrate a commitment to complying with EU regulations and directives related to cybersecurity, data protection, and digital rights.
- Compliance with EU standards ensures interoperability, fosters cross-border cooperation, and strengthens cybersecurity resilience at both national and international levels.

Capacity Building and Training:

- Efforts to build cybersecurity capacity and provide training are evident across all countries, with a focus on equipping individuals, organisations, and institutions with the necessary skills to address cyber threats.
- Training programs, workshops, and educational resources aim to enhance cybersecurity awareness, develop technical expertise, and empower stakeholders to respond effectively to evolving cyber challenges.

MESO Level - School Communities

As the educational landscape undergoes a significant transformation, integrating digital technologies into traditional pedagogy, the imperative to protect students from cyber threats has become increasingly critical for policymakers and educators across Europe. In nations such as Greece, Italy, Portugal, Romania, and Slovakia, concerted efforts are being made to strengthen the educational framework against the challenges posed by the online environment.

Through collaboration with five schools, this activity has provided valuable insights into the actual practices and challenges encountered in the realm of cybersecurity within educational systems. These insights highlight the realities schools face in protecting youth from digital dangers.

Additionally, this report explores various effective strategies and initiatives implemented across these countries. These efforts collectively underscore the importance of cybersecurity education and illustrate successful approaches to enhancing digital safety. Key strategies include comprehensive teacher training, collaboration with external partners, and active parental involvement.

Common Approaches:

Integration of Cybersecurity Education: All five countries recognize the importance of integrating cybersecurity education into school curricula. Whether through legislative measures, training programs, or dedicated initiatives, there is a shared emphasis on equipping students with the knowledge and skills to navigate the digital landscape safely.

Teacher Training and Professional Development: Each country acknowledges the pivotal role of teachers in delivering cybersecurity education. Efforts to train and empower educators through in-service training, workshops, and online resources are evident across the board, reflecting a commitment to enhancing teacher competency in cybersecurity matters.

Collaboration with External Partners: Collaboration with external stakeholders, including law enforcement agencies, cybersecurity experts, and non-governmental organisations, is a common strategy. Partnerships facilitate the development and implementation of comprehensive cybersecurity initiatives, leveraging collective expertise and resources to address cyber threats effectively.

Parental Engagement: While challenges exist, such as limited parental involvement and awareness, all countries recognize the importance of parental engagement in cybersecurity education. Initiatives aimed at raising parental awareness and providing resources for supporting their children's online safety are emerging trends across the board.

Impactful Initiatives:

In-Service Training Programs: In-service training programs for teachers, such as Italy's "Future Labs" and Slovakia's teacher training sessions, have demonstrated significant impact by equipping educators with the necessary skills and knowledge to effectively integrate cybersecurity concepts into their teaching practices. By providing hands-on training, resources, and ongoing support, these initiatives empower teachers to address cybersecurity challenges proactively and engage students in meaningful learning experiences.

Student-Focused Initiatives: Student-focused initiatives, such as cybersecurity scholarships and training courses offered by organisations like Cisco, play a crucial role in nurturing a cyber-resilient generation. By providing students with access to specialised training, mentorship, and career opportunities in cybersecurity,

these initiatives not only enhance students' digital skills but also inspire them to pursue careers in the field, thus contributing to the long-term resilience of the workforce.

Awareness Campaigns and Workshops: Awareness campaigns and workshops aimed at students, teachers, and parents are instrumental in raising awareness about cybersecurity risks and promoting responsible online behaviour. Initiatives like Romania's "Net Hour" and Slovakia's "Turn on the Brain in the Online World" leverage interactive activities, educational resources, and community partnerships to foster digital literacy and resilience among participants. By engaging stakeholders in dialogue and practical learning experiences, these initiatives empower individuals to make informed decisions and navigate the digital landscape safely.

Partnership-Based Approaches: Collaborative initiatives involving partnerships between government agencies, educational institutions, and private sector organisations demonstrate the potential for collective action in addressing cybersecurity challenges. By leveraging diverse expertise, resources, and networks, these partnerships contribute to the development of comprehensive cybersecurity strategies and initiatives that are responsive to the evolving threat landscape. Examples include joint awareness campaigns, research collaborations, and industry-sponsored educational programs that bridge the gap between theory and practice in cybersecurity education.



MICRO Level - Youth Insights

The survey findings underscore the critical need for targeted interventions to enhance capacities in digital safety and cyber resiliency among European youths and educators. Despite a good level of awareness in certain areas, the persistent prevalence of cyber threats and their emotional impact call for a coordinated response involving educational authorities, parents, and community stakeholders to foster a safer digital environment for adolescents.

Survey Summary: Digital Safety and Cyber Resiliency Among Youths Aged 14-17

Participant Demographics

- **Total Respondents:** 210, with detailed responses from 164 individuals.
- **Gender Distribution:** 59% female, 40% male, 1% described as non-binary.
- **Average Age:** 16.13 years.
- **Active Online Presence:** Initiation ages vary with 17,8% under 10 years, 52,2% between 10-12 years, 27,2% between 13-15 years, and a minimal 2,3% starting at 15-17 years.
- **Average Daily Social Media Usage:** Less than 1 hour (3%), 1-2 hours (22%), 2-3 hours (26%), more than 3 hours (49%).

Key Findings on Digital Safety Education and Awareness

- **Structured Digital Literacy and Cyberbullying Education:** The average rating across the EU is moderate (2.98 out of 5), indicating a need for enhanced curriculum integration.
- **Awareness of Online Conduct Guidelines:** Generally higher awareness (3.51 out of 5), with Slovakia and Romania noting more substantial engagement.
- **Cybersecurity Incident Reporting:** Awareness of protocols is average (3.07), suggesting room for improvement in educating students on reporting mechanisms.
- **Parental Measures and Involvement:** Both are relatively low (2.46 and 2.44 respectively), pointing towards a need for greater parental engagement in digital safety practices.

Experiences with Cyber Threats

- **Prevalence of Cyberbullying:** Reported by 42% of respondents, indicating it as a significant issue.
- **Other Online Threats:** Fake identities (40%), online hoaxes (35%), and sexting (31%) are notably prevalent, showcasing diverse challenges that youth encounter online.

Emotional Impact and Response to Cyber Threats

- The emotional impact of online bullying and cybercrimes is significant, with feelings of anger, sadness, and irritability being prominent.
- **Recognition and Avoidance of Cyber Threats:** A high confidence level (3.89 out of 5) among youths in recognizing and avoiding threats, suggesting effective awareness but highlighting the persistent impact of these threats.

Common trends

The comparative data highlights significant trends in youth online behaviour and exposure to cyber threats. With 52% of participants initiating their online presence between the ages of 10 to 12, and a considerable portion spending over 3 hours online daily, it underscores the early and extensive immersion of youth in the digital realm.

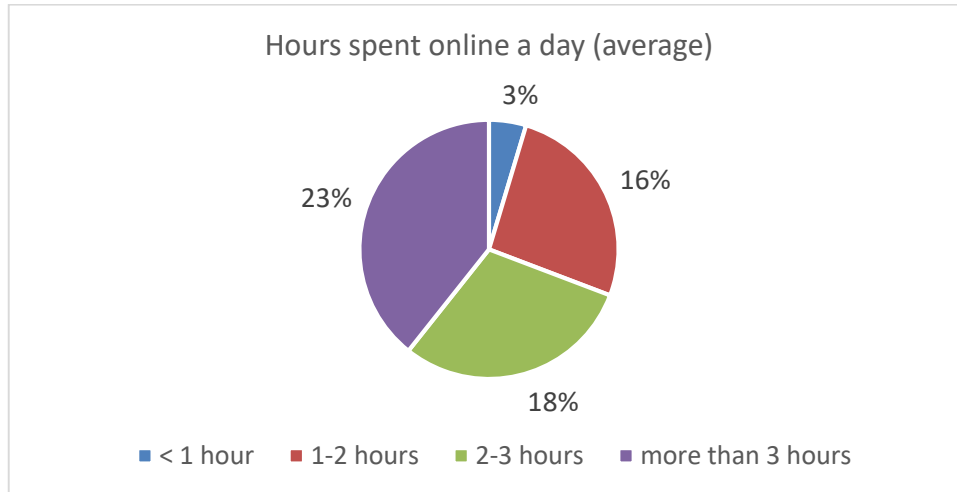


Figure 1: Hours spent online by youth 14-17

Across the surveyed countries, cyberbullying, fake identities on social media, and online hoaxes emerge as prevalent cyber threats, affecting a significant portion of the youth population. Sexting and over-gaming also feature prominently among the experienced cyber threats. The comparative data reveals that cyberbullying is experienced by 42% of participants, followed closely by fake identities on social media (40%) and online hoaxes (35%). Sexting and over-gaming are reported by 31% of respondents each, highlighting their significance in the cyber threat landscape.

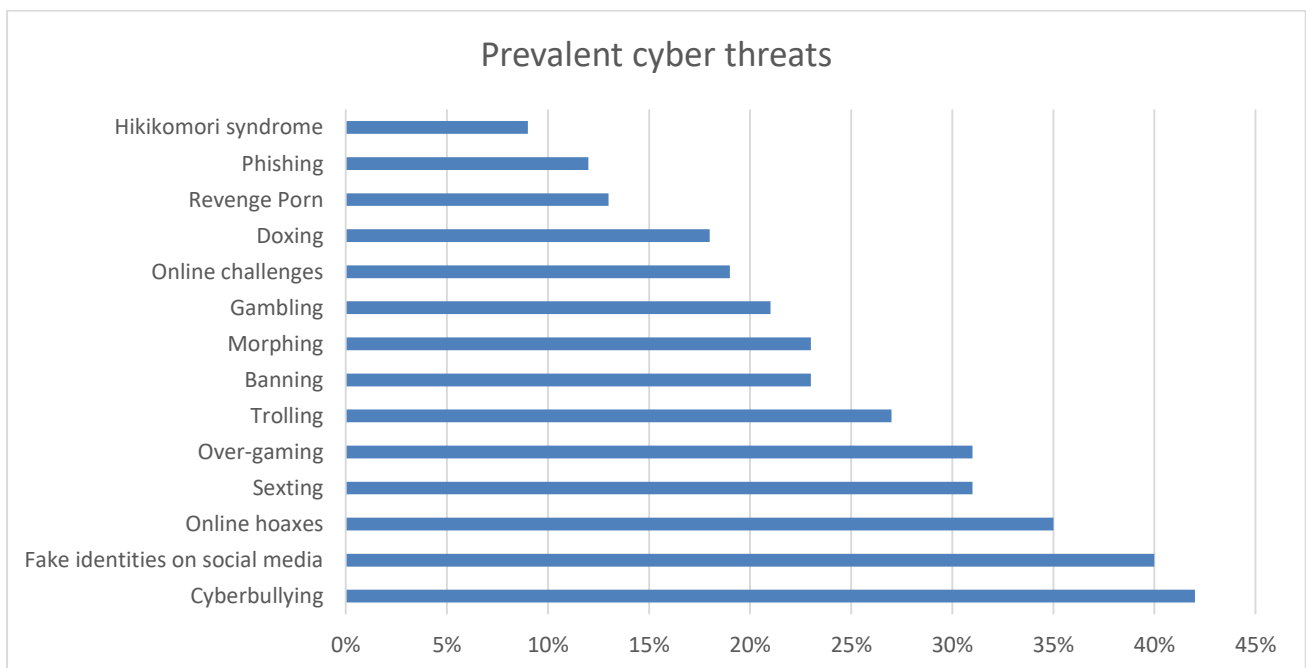


Figure 2: Prevalent Cyber threats detected by youth 14-17



The data on platforms where cyberbullying or cybercrime occurs reveals Instagram as the primary platform for both personal experiences and witnessing others' experiences. This is followed by WhatsApp, Snapchat, Facebook, and gaming platforms, indicating the need for targeted interventions on popular social media platforms.

Despite differences in response mechanisms and cultural contexts, there are commonalities in the prevalence of cyber threats and the emotional impacts experienced by youth, such as anxiety, depression, and social isolation. This underscores the universal challenges faced by youth in navigating the digital landscape and emphasises the need for targeted interventions and support services.



Identification of Cyber Threats

CYBER's approach to categorization considers both the direct targets (individuals or communities) and the nature of the threat ([A] Psychological and Behavioural Impact on Individuals; [B] Social and Community Impact; [C] Technical and Security Threats):

[A] Psychological and Behavioural Impact on Individuals

Focusing on threats that directly affect individuals' mental health, self-esteem, and personal behaviour acknowledges the profound personal consequences of online harassment, addiction, and exploitation. This category highlights the need for interventions that support mental health, promote digital literacy, and foster resilience among internet users. It recognizes the individual as the primary target and emphasises personal safety and well-being.

- **Cyberbullying and Body Shaming:** Affects individuals by targeting their self-esteem and mental health through negative comments or images.
- **Over-gaming or Gaming Addiction:** Focuses on individuals developing unhealthy gaming habits that can impact their daily functioning and mental health.
- **Hikikomori Syndrome:** Characterised by severe social withdrawal, often exacerbated by digital technology use.
- **Gambling:** Targets individuals with the lure of easy wins, leading to potential addiction and financial ruin.
- **Sexting:** Involves individuals sharing explicit content, which can lead to privacy violations and emotional distress.
- **Grooming and Fake Identities on Social Media:** Predators target individuals, often minors, for exploitation through deception.
- **Revenge Porn:** Individuals are victimised through the non-consensual sharing of intimate images, leading to psychological trauma.

[B] Social and Community Impact

This categorization acknowledges that certain threats, while targeting individuals, have broader implications for social dynamics, community norms, and collective behaviour online. By grouping threats like online radicalization, hate speech, and social media challenges, this approach underscores the role of digital platforms in shaping societal values and behaviours. It highlights the importance of fostering positive online communities, encouraging respectful discourse, and combating misinformation. This category calls for community-oriented strategies and educational efforts that build collective digital citizenship skills.

- **Hoaxes and Scam:** Affect wider audiences by spreading misinformation or fraud, eroding trust in information sources.
- **Social Media Challenges:** Engage communities in activities that can range from benign to dangerous, influencing group behaviour.
- **Online Radicalization and Hate Speech:** Target or emanate from groups, promoting extremist views and disrupting social harmony.
- **Banning:** Impacts individuals' ability to participate in online communities, affecting the social dynamics of those platforms.

[C] Technical and Security Threats

Separating technical and security threats acknowledges the specialised nature of these challenges, which often require specific technical knowledge to both execute and combat. This categorization emphasises the need for robust cybersecurity measures, awareness of digital threats, and the development of technical skills among users to protect their information and navigate the digital landscape safely. It also points to the necessity for ongoing research, development, and policy-making focused on enhancing digital infrastructure and user protection against sophisticated cyber-attacks.

- **Phishing:** Uses deceptive techniques to steal sensitive information, targeting individuals but requiring technical knowledge to execute and counter.
- **Morphing and Deepfakes:** Involve the technical manipulation of images and videos to create believable falsehoods, affecting both individuals' reputations and broader societal trust.
- **Trolling:** While often targeting individuals, the disruptive nature of trolling impacts the wider community atmosphere and online discourse.
- **Doxing:** The act of publicly revealing private information about an individual without their consent, combining both technical means for information gathering and a psychological impact on the victim.

The criteria driven methodological approach guiding the selection process for the strategic development of addressing cyber threats ensures that the educational content is not only relevant but also impactful for the target audience. The criteria employed identify the threats that pose the greatest risk and relevance to students, thus optimising the educational interventions for maximum effectiveness. These criteria include:

- I. **Potential Harm Caused:** This criterion evaluates the severity and scope of the negative impact a cyber threat could have on an individual's mental, emotional, or physical well-being, as well as its potential consequences on their social and professional lives. By prioritising threats based on the extent of harm they can inflict, the curriculum can focus on the most damaging risks, ensuring students are well-equipped to protect themselves against significant dangers.
- II. **Frequency of Occurrence:** Understanding the commonality of a threat within the digital environment is crucial. This criterion assesses how often a particular threat is encountered by the target audience, thereby gauging its prevalence in the daily digital interactions of young users. By focusing on the most frequently occurring threats, the educational content remains highly relevant and timely, addressing the issues students are most likely to face in their online activities.
- III. **Relevance to the Target Audience:** This criterion examines the applicability of a cyber threat to the specific demographic of the educational initiative, considering factors such as age, digital literacy levels, and common online behaviours of the target audience. By tailoring the content to the unique experiences and vulnerabilities of young users, the education provided can directly address the threats that are most pertinent and impactful to their digital lives.

National Perspectives

Across these five European countries, a pattern emerges of integrating cybersecurity deeply into national strategies, educational systems, and public awareness initiatives. Each country, while tailored in its approach, shares common goals: enhancing digital literacy, protecting citizens' digital rights, and fostering a collaborative environment between government entities, educational institutions, and private sectors to combat cyber threats effectively.

This comprehensive overview at national levels provides an analysis of the cybersecurity strategies highlighting the ways in which these countries safeguard their digital environments, engage educational sectors, and collaborate across public and private sectors.

In brief, prevailing Cyber Threats at national levels:

- [Greece](#): Cyberbullying, malicious use of social media, illegal access to personal data, fake and deep fake news, and financial cybercrime are prominent threats.
- [Italy](#): Cyberbullying emerges as the most prevalent issue, followed by sexting and trolling. Emotional responses to cyber threats are widespread, with feelings of anger, hopelessness, loneliness, and worry reported among youth.
- [Portugal](#): Cyberbullying is prevalent, followed by fake identities on social media and sexting. Instances of online fraud and extortion targeting youth are also reported, often leading to psychological distress and the need for support systems.
- [Romania](#): Cyberbullying, online pranks, fake identities, and over-gaming are identified as common threats among youth.
- [Slovakia](#): False identities, online hoaxes, cyberbullying, sexting, trolling, and excessive gaming are significant concerns.

GREECE

[Author: [SIGMA Tournis Symvouleftiki](#)]

SECTION 1: NATIONAL CYBERSECURITY POLICIES

Greece, through Law 4577/2018 and Ministerial Decision 1027/2019, integrated EU Directive 2016/1148/EU (NIS Directive) and Regulation (EU) 2019/881 into its national legislation. These laws establish cybersecurity standards across critical sectors like energy, transport, finance, and healthcare. They define criteria for basic security requirements, incident reporting procedures, and certification systems. The General Directorate of Cyber Security within the Ministry of Digital Governance oversees national cyber security planning and serves as the National Cyber Security Authority (NCSA). It ensures compliance with Law 4577/2018 and facilitates cross-border cooperation within the EU.

The country's Cybersecurity principles are:

- 1 Modern digital environment: Facilitating innovation and technology development.
- 2 High cybersecurity standards: Protecting information infrastructures, applications, and services.
- 3 Fundamental rights protection: Ensuring data privacy, personal development, and digital equality.
- 4 Safe use culture: Promoting digital literacy and awareness of technology risks.
- 5 Trust in digital governance: Utilising technology for societal and economic advancement.

The major policy of the state for young people aged 14-17 in relation to cyber security is to protect them from malicious acts, such as cyber bullying, cyber grooming, violation of personal data and privacy, violent behaviours etc. The policy is implemented through a combination of government and private initiatives.

The HQ of the Hellenic Police through the Directorate of Cybercrime, implementing the mission of the Hellenic Police which is the prevention and then the suppression of crimes, have developed a set of innovative actions to inform citizens. These include:

- Workshops and lectures held both in-person and remotely, focusing on safe internet browsing, especially targeting students, parents, and teachers.
- Information days covering topics such as the risks of new technologies, social networking dangers, cyberbullying, online scams, and more.
- Adaptation to the COVID-19 pandemic by conducting remote briefings to educate people about safe internet use during the heightened online activity.
- Participation in events like World Safer Internet Day, organising awareness activities for educators and mental health professionals.
- Support for children in institutions during Christmas holidays through informative workshops and briefings.
- Publication of information leaflets on safer internet browsing, updated regularly to address evolving cyber threats.
- Collaboration with NGOs, such as Axion Hellas, for information actions in remote areas.
- Production of educational material like the fairy tale "Sifis the Mouse & the Internet" and audiovisual content.

- Participation in various events, conferences, and exhibitions to raise awareness about cybercrime.
- Operation of websites like cyberkid.gr, cyberalert.gr, and the Cyberkid app, providing information and e-learning resources on internet safety.
- Active presence on social media platforms to disseminate information about cyber threats and law enforcement efforts.
- Broadcasting television and radio "spots" to inform the public, with campaigns addressing different target groups.
- Collaboration with PLAYMOBIL HELLAS to develop educational materials for children on safe internet navigation.
- Establishment of the "Digital Academy" in partnership with academic institutions, offering interactive games to educate minors about internet dangers.

SECTION 2: LOCAL CYBER SECURITY INITIATIVES

The information workshops for 14–17-year-olds are held in person, online or through a visit to the General Police Directorate of Attica auditorium and their content is tailored to the target audience. The activities in schools are carried out following a memorandum of cooperation between the Ministry of Civil Protection and the Ministry of Education, Religious Affairs and Sport and the material presented has been approved. The information workshops are held at the request of the school and the particular challenge faced is the high volume of requests submitted, which is why some of them are serviced by videoconference.

The sample of information obtained from the interview with a local school shows that the school does not have a permanent and regular cooperation with the local police authority. It has cooperated on two occasions, one involved the management of a morphing incident in the school environment and the other was of an informative nature, where the cybercrime department mainly informed pupils about cybercrime and cyber risks.

SECTION 3: EDUCATIONAL INTEGRATION OF NATIONAL CYBERSECURITY POLICIES

In cyberspace, students in the local community face a variety of threats. Prevalent threats include cyberbullying, malicious use of social media, and illegal access to personal data. There are also trends such as the spread of fake and deep fake news and financial cybercrime that threaten the safety of students.

The local police department understands the importance of addressing cyber threats in the local community, especially in regard to student safety online. Collaboration with the Cybercrime Unit is promoted to identify, proactively monitor and respond to cyber threats. Preventive measures such as educational programmes for pupils, monitoring of online activities and information campaigns for parents are implemented. In addition, mechanisms are put in place to deal with incidents and provide psychosocial support to victims.

According to the school interview, no structured education is provided by the school system, there are only references in the textbook of the first grade of high school to cyberbullying (on the internet and specifically on social media). School/personal initiative ensures basic knowledge and awareness on these issues, but not in a separate structured lesson, but with local references in the IT lesson (what is the current situation, proper use of the internet, what students should be aware of, etc.). In some cases, interaction between the IT teacher and the students is sought and feedback is collected.

There is also no specific policy for the prevention and response to incidents of cyberbullying, neither by the school itself nor by the national school system. The school educates students about the consequences of

cyberbullying with simple reports rather than a structured and methodical lesson. No clear support mechanism is provided for victims, except at the discretion of school staff.

SECTION 4: EDUCATIONAL APPROACHES FOR CYBER RESILIENCY

From the research conducted, no specific mechanisms were found to support teachers in teaching cyber security and critical thinking. There are also no specific training programs, workshops and certifications that enhance teachers' skills. Some training programs are implemented by state and private initiatives, without, however, being mandatory for teachers. The only educational material available for teachers is the same as for students.

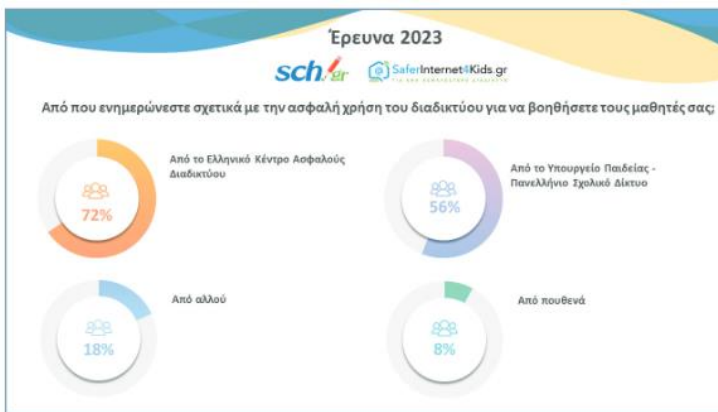


Figure 2: SaferInternet4Kids 2023 survey on the resources teachers use to educate students: 72% from the Hellenic Safer Internet Centre, 56% from the Ministry of Education, 18% from other sources, while 8% do not receive any information from any source.

Therefore, educators' confidence in integrating cyber resiliency lessons and the effectiveness of ongoing training initiatives cannot be evaluated.

A recent 2023 survey shows that 67% of teachers can inform their students about the basics of digital security (Figure 3).



Figure 4: A SaferInternet4Kids 2023 survey shows that 67% of teachers can inform their students about the basics of digital security.

The information gathered from an interview with a local school indicates a lack of clear guidelines on appropriate online behaviour for both students and staff. While some guidance is provided for students

through school initiatives and references in IT lessons, staff responses vary based on individual knowledge and considerations. Additionally, there are no continuous professional development opportunities such as training programs or seminars on digital security, data protection, and online safety for teachers.

Based on the online youth survey results, 53,3% of students don't feel confident about school support in addressing cyber threats. At the same time 70% of students do not participate in school workshops or discussions on cybersecurity or proper internet use while 36.7% of students consider that education methods on cybersecurity, proper use of the internet and online behaviour are not engaging, while 26.7% are neutral (Figures 4,5 & 6).

Figure 5: 53,3% of student don't feel confident about school support in addressing cyber threats

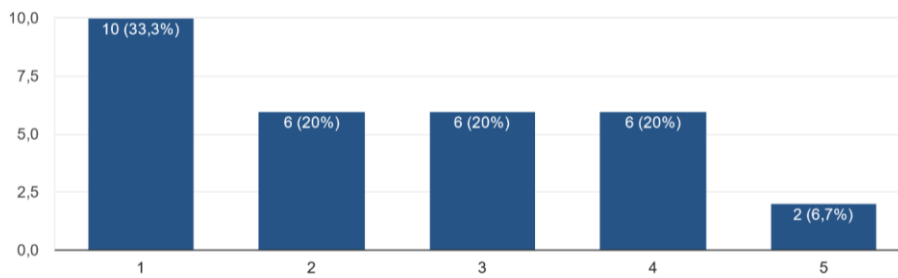


Figure 6: 70% of students do not participate in school workshops or discussions on cybersecurity or proper internet use.

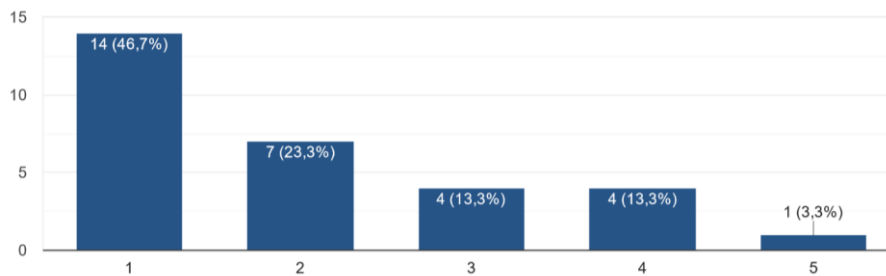
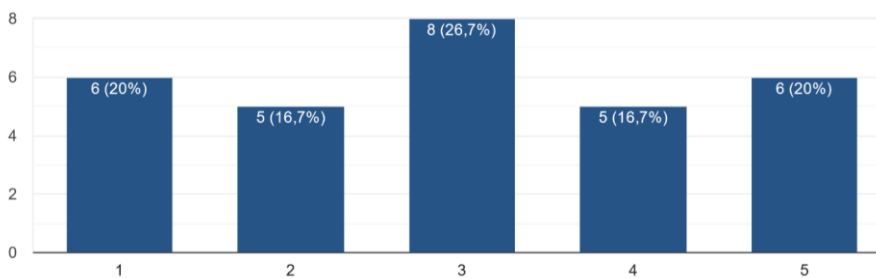


Figure 7: 36.7% of students consider that education methods on cybersecurity, proper use of the internet and online behaviour are not engaging, while 26.7% are neutral.



SECTION 5: DIGITAL LEARNING PLATFORMS

Digital learning platforms are now integrated into the educational process in all schools, public and private. The integration of cyber security in digital learning platforms (e-classes) is done by the acceptance by the users of the rules of good use and the privacy policy. More specifically, each student must accept the following terms of use when creating the educational account:

- I have informed my parents/guardian or a school teacher about the account I am creating.
- The title and description of my account do not contain inappropriate, inappropriate or abusive words.
- I will not send invitations to join my account to people I do not know personally.
- If I want to send invitations to students I don't know personally, I will first think about whether they will be bothered by the invitation. If in doubt, I will get the consent of my parent/guardian or a school teacher.
- If I want to accept requests to join my cell from students I do not know personally, I will first ask the other members so that there is no objection.
- I will respect the other members! I will not share photos or videos with inappropriate or offensive content on the wall or in the account files.
- I am in charge of the account I create! Consequently:

a) I will regularly check account files, wall posts and comments for offensive, inappropriate content.

b) if I find posts or comments with offensive content I will delete them immediately or politely ask the member who made the post or comment to delete it.

- if a member systematically insults other members I will delete him/her, delete the material he/she uploaded in the account archives and delete the comments from the account wall.
- I will convey these rules of good behaviour to the members of the account so that we respect each other.
- I know that if I do not respect one or more of the above rules or if I offend other members with my behaviour, the platform administrators, after notifying me first, may close my cell so that I am not allowed to enter. My parents/guardian and school will also be notified.

Also, each student must accept the following privacy policy terms.

- The website of the digital platform collects personal information such as the name, e-mail, school unit, class, department and status of the users (student, teacher).
- This data is used exclusively for statistical reasons and for reasons of improving the services provided and is not disclosed to any third party (natural or legal person) for any reason, with the exception of relevant provisions of the law and only to the competent authorities.
- This website may also collect non-personal identification information of users using corresponding technologies, such as cookies and/or Internet Protocol (IP) address tracking. Cookies are small text files that are stored on the hard drive of each visitor / user and do not take notice of any document or file from their computer. They are used to facilitate the access of the visitor / user regarding the use of specific services and/or pages of the Platform, for statistical reasons and in order to determine the areas which are useful or popular. These

data may also include the type of browser (browser) used by the visitor / user, the type of computer, its operating system, network service providers and other such information.

SECTION 6: LOCAL CYBER THREAT TRENDS

In cyberspace, students in the local community face a variety of threats. Prevalent threats include cyberbullying, malicious use of social media, and illegal access to personal data. There are also trends such as the spread of fake and deep fake news and financial cybercrime that threaten the safety of students.

The local police department understands the importance of addressing cyber threats in the local community, especially in regards to student safety online. Collaboration with the Cybercrime Unit is promoted to identify, proactively monitor and respond to cyber threats. Preventive measures such as educational programmes for pupils, monitoring of online activities and information campaigns for parents are implemented. In addition, mechanisms are put in place to deal with incidents and provide psychosocial support to victims.

The most common platforms used by the Greek youth are Tik-Tok, Facebook and Instagram. As shown in the figure below, the most common - local cyber threats, as reported by students (30 in total) who participated in the analysis are Morphing, Banning, Trolling, Over Gaming and Pranks & Scams.

Figure 8 Most common - local cyber threats among Greek Students

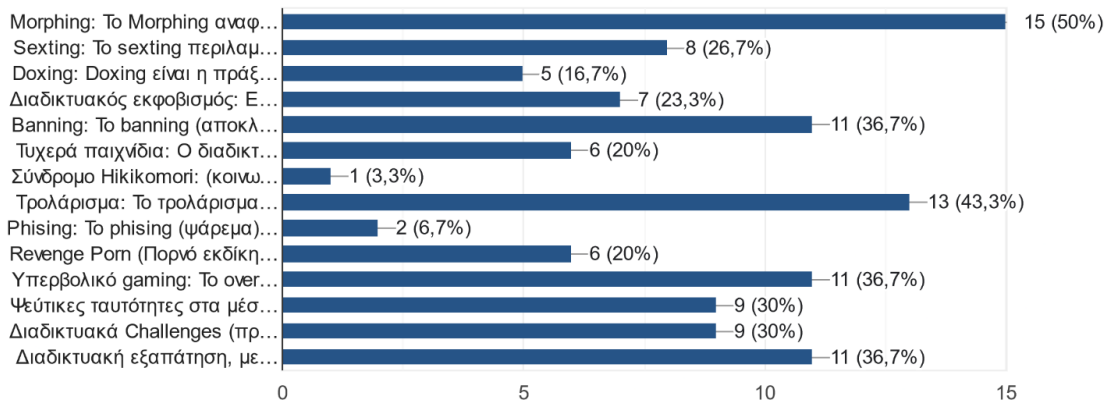
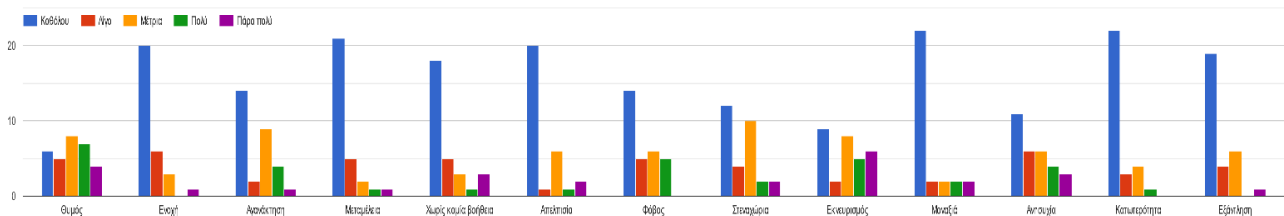


Figure 9: The negative emotions as a result of cyberbullying/cybercrime vary

Ποια ήταν τα αρνητικά συναισθήματα που ένιωσες ως αποτέλεσμα του διαδικτυακού εκφοβισμού/εγκλήματος στον κυβερνοχώρο;



There are many examples where cyber threats have a direct impact on the psychological well-being of young people. Cyberbullying, for example, can lead to increased anxiety, depression and self-isolation. Young people may face challenges in the area of social relationships and their overall psychological well-being.

The negative emotions as a result of cyberbullying/cybercrime vary (Figure 8). Guilt, exhaustion, loneliness, hopelessness and remorse were the most common emotional states experienced by the students participating in the survey.

SECTION 7: COMMUNITY ENGAGEMENT

There's a lack of specific protocols for reporting cyber threats within schools, and no established feedback process on digital security measures. Given children's early exposure to the digital world, regular education sessions by cyber experts and psychologists are crucial. These sessions cover safe internet use, risk identification, incident management, and real-life examples.

Students should also know official channels for reporting incidents, like the internet illegal content reporting line and the Hellenic Police Cyber Crime Division. These efforts include briefings for students, parents, and teachers.

The themes are developed based on actual cases handled by our Service regarding the following: the phenomenon of online coercion and bullying; the phenomenon of online deception through social media accounts and online games; fake online accounts; internet challenge phenomenon; the phenomenon of revenge pornography and victim-blaming in the real world; cyberbullying; online games and time spent in them; online scams.

On the other hand, the students themselves should, through their student councils, their student newspapers, their social network groups, inform their classmates about the dangers they recognize or fall victim to, whether they involve strangers or acquaintances within the community.

SECTION 8: MAYOR CYBER RESILIENCY CHALLENGES

The unforeseen challenges in the field of prevention for young people due to evolving cyber threats include:

- **Cyberbullying:** new forms of cyberbullying can cause psychological effects on young people, such as anxiety and depressive symptoms.
- **Grooming:** grooming is a cyber activity in which a person, usually an adult, tries to contact and deceive a child for the purpose of exploitation, usually for sexual purposes. This activity may occur through online platforms, social networks or other online means of communication. Grooming can seriously affect the psychological and emotional well-being of young people, putting them in dangerous situations. Exploiters may use techniques such as false representation, false identity, and manipulation to gain the trust of young people.
- **Evolving fraud techniques:** Cyber criminals are constantly using new techniques to defraud and hide behind advanced tools to mislead young people.

To address these challenges, prevention strategies can include:

- **Education and awareness raising:** Educational programmes focusing on threat identification, critical thinking and safe online behaviour.
- **Working with parents and teachers:** Parents and teachers need to be aware of the evolving threats and play an active role in educating young people.

A key challenge facing schools and reported in school consultation is the lack of awareness among students about cyber challenges and the inability to understand the risks they face. They are often attracted to hacking

issues, while they do not understand the dangers that the internet can pose to them and that they may be victims themselves in the future. Incidents of morphing (one recorded incident), cyberbullying, banning have been identified and reported by students themselves. For the rest there are no detection methods.

SECTION 9: FUTURE EXPECTATIONS

According to the youth survey of the results were alarming:

- 56.6% of the students surveyed said that they had either not been taught any or little digital literacy-related modules while 36.6% had a neutral attitude (Figure 9).
- 60% of the students surveyed said that they had not been informed at all or had been informed a little about protocols for reporting cyber threats in the school environment (Figure 10).
- More than 50% of students consider school support on cyber security and incidents of cyber bullying and threats to be inadequate (Figure 11).
- More than 50% of students have limited or no participation in school workshops or discussions on safety and responsible online behaviour (Figure 12)

Figure 10: 56.6% of the students surveyed said that they had either not been taught any or little digital literacy-related modules while 36.6% had a neutral attitude.

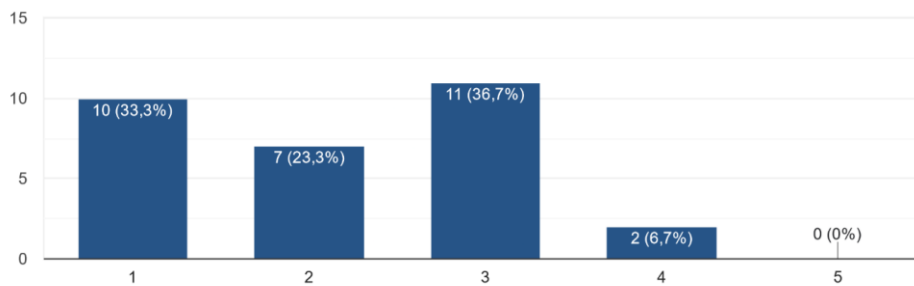


Figure 11: 60% of the students surveyed said that they had not been informed at all or had been informed a little about protocols for reporting cyber threats in the school environment.

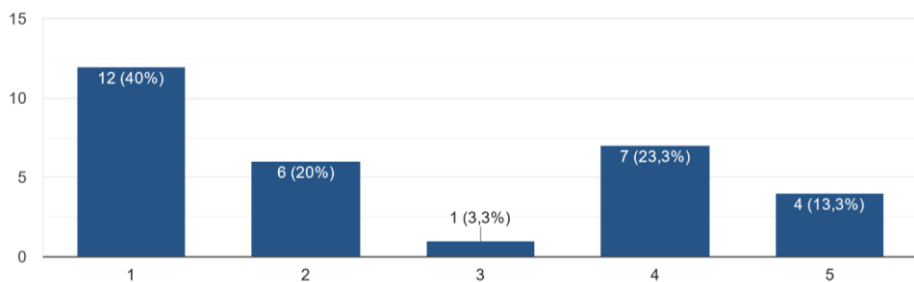


Figure 12: More than 50% of students consider school support on cyber security and incidents of cyber bullying and threats to be inadequate.

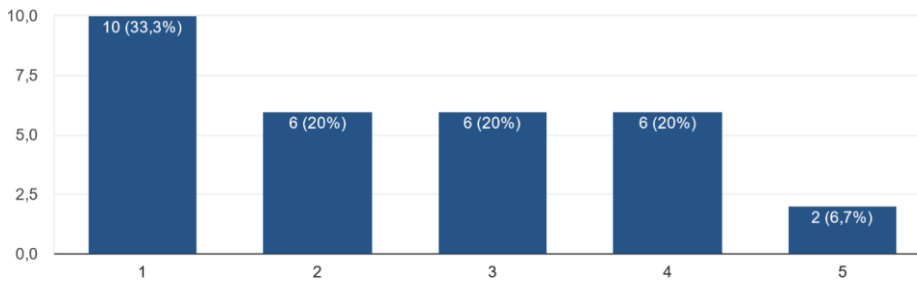
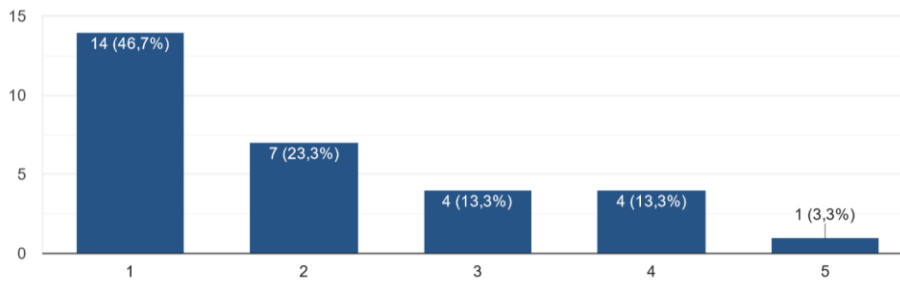


Figure 13: More than 50% of students have limited or no participation in school workshops or discussions on safety and responsible online behaviour



Successful initiatives include integrating cybersecurity into the curriculum and fostering communication between schools and parents. Key metrics for success include student and parent participation, reduction of cyberbullying, and increased reporting of potential risks.

A Greek school representative stresses the importance of educating students about cyber threats through workshops focusing on hacking, online fraud, and fake news.

SECTION 10: CONCLUSIONS

The online survey among 14-17 year olds in Greece highlights prevalent cyber threats like cyberbullying, social media misuse, and financial crime. These threats impact students' well-being, causing anxiety and isolation. The Police Department's Cybersecurity Unit emphasises the importance of collaboration to address these issues, underscoring the need for preventive measures and ongoing education.

However, the survey reveals gaps in students' education on digital literacy and reporting protocols for cyber threats at school. Many students feel school support on cybersecurity and cyberbullying is insufficient. Comprehensive educational programs and policies are needed at school and national levels to address these issues, along with training for teachers.

Empowering students with knowledge and skills to recognize cyber threats is crucial. Structured education and workshops focusing on identifying cyber threats are needed to help students navigate the digital world safely.

Greece: Bibliography

Hellenic Republic Ministry of Digital Governance. (2022). National cybersecurity strategy 2020-2025. Retrieved from https://mindigital.gr/wp-content/uploads/2022/11/E%CE%9D-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf

Hellenic Republic Ministry of Education. Retrieved from <https://auth.e-me.edu.gr/>

Hellenic Police. Advice for safe access to the Internet. Retrieved from <https://www.astynomia.gr/citizens-guide/useful-information/advice-for-safe-access-to-the-internet/?lang=en>

Hellenic Police. Innovative actions. Retrieved from <https://www.astynomia.gr/elliniki-astynomia/eidikes-ypiresies/diefthynsi-dioxis-ilektronikou-egklimatos/kainotomes-drasesis-prolipsi-kai-enimerosi/>

Hellenic Police – Cyber Security Site for Kids. Retrieved from <https://www.cyberkid.gov.gr/>

Greek Safer Internet Center. Retrieved from <https://saferinternet4kids.gr/>

Greek Safer Internet Center (2023). Research on online sexual abuse/seduction, cyberbullying and addiction (period 12/2022-01/2023). Retrieved from https://saferinternet4kids.gr/ereyna/survey_4400_educ/

National Printing Office (2018). Law 4577/2018. Retrieved from www.et.gr

ITALY

[Author: [PRISM Impresa Sociale s.r.l.](#)]

SECTION 1: NATIONAL CYBERSECURITY POLICIES

The National Cybersecurity Agency (Agenzia per la cybersicurezza nazionale - ACN) serves as the national authority for cybersecurity, safeguarding national interests in cyberspace. Established by Decree Law No. 82 of June 14, 2021, the agency is tasked with ensuring security and resilience in cyberspace, as well as preventing and mitigating cyberattacks. Its responsibilities include implementing the National Cybersecurity Strategy, adopted by the Prime Minister, which outlines objectives to be achieved by 2026.

General national cybersecurity policies, as outlined in the National Cybersecurity Strategy 2022-2026, emphasise the importance of developing adequate cybersecurity strategies to secure and bolster the nation's digital infrastructure and develop a security-oriented approach at all societal levels.

The main challenges identified by the strategy are:

- Ensure a cyber-resilient digital transition of the Public Administration (PA) and the productive fabric.
- National and European strategic autonomy in the digital sector.
- Anticipate the evolution of cyber threats.
- Cyber crisis management.
- Counteracting online disinformation within the broader context of the so-called hybrid threat.

The Implementation Plan emphasises education in cybersecurity through various measures:

- Training programs aim to familiarise students with new technologies and bridge gender gaps in technical careers.
- Continuous updating of teaching methods and teacher preparation ensures educators stay abreast of cybersecurity advancements.
- Specific training paths for non-specialists in cybersecurity target employees of both public and private organisations.
- Comprehensive digital education programs include skills acquisition for verifying online content and information.

These educational efforts aim to promote a cybersecurity culture and ensure a well-prepared workforce to address evolving cyber threats.

For the 2022 edition of the Digitisation of Economy and Society Index (DESI), Italy ranks 18th among the 27 EU Member States. Italy's recovery and resilience plan, which is the largest in the entire EU, amounts to EUR 191.5 billion. 25.1 % of this amount (i.e. EUR 48 billion) is earmarked for digital transition, providing large resources to all schools in Italy.

SECTION 2: LOCAL CYBER SECURITY INITIATIVES

The Cybersecurity National Lab, established by the CINI (Consorzio Interuniversitario Nazionale per l'Informatica), spearheads several local cybersecurity initiatives under "The Big Game" programme, epitomising community-driven efforts in Italy. These initiatives, deeply entrenched within educational institutions, not only fortify the national cybersecurity ecosystem but also wield a profound impact on local communities, particularly in nurturing youth education.

Among these endeavours, CyberChallenge.IT stands out as the premier national cybersecurity training program tailored for students aged 16-24. Conducted by the Cybersecurity National Lab, it serves as a beacon for identifying and nurturing the next generation of cybersecurity professionals. Over twelve weeks,

participants engage in comprehensive training sessions, delving into fundamental scientific, technical, and ethical principles of cybersecurity under the tutelage of academic experts and industry leaders. The program, hosted across more than 40 participating institutions, including universities, the Tuscan Cybersecurity Competence Centre, the Training Command and Application School of the Army in Turin and the Air Force Academy in Pozzuoli. It amalgamates theoretical learning with gamification and practical exercises, culminating in a final competition. This initiative not only fosters cybersecurity skills but also bolsters participants' prospects in the industry, aligning with the national cybersecurity strategy.

Additionally, OliCyber, constituting the Italian Cybersecurity Olympics, serves as a conduit for student engagement with cybersecurity challenges. Open to all Italian high schools federated under the CyberHighSchools program, OliCyber provides a platform for students to confront cybersecurity issues, enhancing their visibility to national organisations and industry players. Its inclusion as a recognized project by the Ministry of Education underscores its significance in fostering excellence among students and promoting cybersecurity awareness at the grassroots level.

Furthermore, CyberTrials, a complimentary program geared towards Italian high school girls, seeks to promote cybersecurity themes and online civility. Through a 22-hour curriculum, students delve into various facets of cybersecurity, including network security, web security, and cryptography, augmented by soft skills development such as teamwork and pressure management. By addressing gender disparities in the field, CyberTrials not only enriches participants' skill sets but also contributes to a more inclusive and diverse cybersecurity workforce

These initiatives, coupled with the CyberHighSchools program, exemplify a concerted effort to integrate cybersecurity education into the fabric of Italian secondary education. By offering federated schools access to specialised training, resources, and networking opportunities, the Cybersecurity National Lab fosters a community of educators and students committed to advancing cybersecurity awareness and expertise. Moreover, the tangible benefits afforded to participating schools, teachers, and students and the private-public network built underscore the transformative impact of these initiatives on the local community, laying the foundation for a cyber-resilient future driven by empowered youth.

SECTION 3: EDUCATIONAL INTEGRATION OF NATIONAL CYBERSECURITY POLICIES

Since September 2020, Civic Education has been integrated as a cross-curricular discipline across all school levels, ranging from kindergarten to upper secondary school. Civic Education includes as main thematic “Digital citizenship” referring to an individual's ability to consciously and responsibly utilise virtual communication tools.

The Ministero dell'Istruzione e del Merito (MIM) has established the first Curriculum for Digital Citizenship Education, that aims to frame the array of themes and contents fundamental for the development of students' full digital citizenship through education. The initiative enters in the “SIC- Generazioni Connesse” project that has been co-funded by the European Commission under the Connecting Europe Facility (CEF) programme, through which the Commission promotes strategies aimed at making the Internet a safer place for younger users. The consortium of the project includes some of the main Italian organisations dealing with online safety: The Childhood and Adolescence Authority, the State Police, the Ministry of Cultural Heritage and Activities, the Universities of Florence and 'La Sapienza' in Rome, Save the Children Italia, Telefono Azzurro, the EDI onlus cooperative, Skuola net and the Giffoni Experience.

In the Generazioni Connesse websites are available open resources targeted for youth, school and educators and parents. First of all, students can access to two Hotline services, enabling users to report the presence of



child sexual abuse material found online, and one Helpline service (1.96.96) that can provide support on problematic experiences related to the use of the Internet and digital technologies.

For school communities, support is offered in the development of an internal policy aimed at promoting digital skills and the use of technology in teaching; preventing problematic situations; and recognising, managing, reporting and monitoring incidents of misuse of tools. Thanks to the new platform, a further 15,000 schools of all levels are participating in the course offered. The platform ELISA provides e-learning training for professors and a monitoring system.

Furthermore, though the educational Kit (Kit Didattico) schools are guided by the inclusion of the key concepts and themes to be covered in their Three-Year Educational Offer Plan (PTOF), they will have to take into account all the areas of the framework, but will have full freedom in the construction of the vertical curricula associated with it. The Kit includes five main areas: the internet and ongoing change, media education, information literacy, quantification and computation: data and artificial intelligence, digital culture and creativity.

SECTION 4: EDUCATIONAL APPROACHES FOR CYBER RESILIENCY

In Italy, the enactment of Law 107 in 2015 designated the training of school personnel as "mandatory, permanent, and strategic," acknowledging it as an opportunity for professional development and contribution to educational innovation. The official recognition of participation in research and training, as mandated by law, incentivizes teachers' professional development, potentially bolstering educators' confidence in incorporating cybersecurity concepts and methodologies into their teachings.

The initiative known as "Future Labs" is dedicated to in-service training for school personnel on the digital transition of schools. These Future Labs serve as innovative spaces within respective institutions, designed to train and empower teachers in utilising digital technologies in teaching, with a particular focus on cybersecurity.

The initiatives described above, CyberHighSchool.IT, "The Big Game" and ELISA platform, leverage schools to benefit both teachers and students. These courses, aimed primarily at secondary school teachers, raise awareness of cybersecurity issues related to the use of IT tools and technologies. Additionally, platforms like Scuola Futura, integrated into the National Recovery and Resilience Plan (PNRR), offer comprehensive training for school personnel, including a 12-hour Cyber Security course focusing on digital transition.

In terms of student-focused initiatives, Cisco's cybersecurity scholarships and training courses play a pivotal role in nurturing a cyber-resilient generation. These programs, offering 1000 scholarships for individuals aged 16 to 45, provide free access to a cybersecurity career path, including webinars with Cisco professionals and hands-on labs with partner academies nationwide. By equipping students with essential cybersecurity skills and fostering a supportive community for knowledge exchange, Cisco's initiatives empower the next generation to navigate the digital landscape safely and responsibly.

The impact of these initiatives has been very significant considering, for example, that: through the ELISA platform more than 5,000 teachers started training in the 2018/2019 school year, involving almost 50% of Italian state schools and that "Future Labs" has led to the establishment of 28 hubs in all Italian regions and envisaged the setup, following the future classroom model, of innovative training environments used for education.

SECTION 5: DIGITAL LEARNING PLATFORMS

Italy adheres to the EU's General Data Protection Regulation (GDPR), which establishes guidelines for data protection and security measures applicable to digital platforms. Educational institutions must comply with GDPR requirements when collecting, processing, and storing personal data within digital learning platforms. Although Italy does not have specific regulations for learning platforms to integrate cybersecurity policies and guidelines, the country recently approved its National Cybersecurity Strategy (2022-2026) and its accompanying Implementation Plan developed by the National Cybersecurity Agency (ACN). This comprehensive framework aims to address cyber threats across various sectors, including digital learning. The strategy emphasises proactive risk assessment, incident response protocols, data protection measures, and compliance with regulatory requirements to effectively mitigate cyber threats. It also stresses the importance of fostering a cybersecurity-aware culture among users and stakeholders.

In response to the challenges posed by the COVID-19 pandemic, educational institutions in Italy have prioritised the implementation of digital learning platforms to ensure continuity of education while safeguarding the health of students and faculty. The Ministry of Education (MIUR) has published guidelines and initiated funding programs aimed at equipping schools with smart classrooms and digital learning tools. Schools and universities must move towards tools that have data protection measures by design (in the GDPR, this is the so-called Privacy by Design principle) and by default (Privacy by Default principle). There is no need for an impact assessment (Impact Assessment), provided for in the European Regulation in cases of high risks if the data processing carried out by schools and universities, insofar as it relates to minors and workers, does not have any additional features that are likely to increase the risks.

When a platform processes personal data on behalf of an educational institute, the relationship must be governed by contract or legal act (Art. 28 of the Regulation). This includes cases like the electronic register, where the provider acts as a data controller. The platform's data processing for schools or universities should be limited to what's strictly needed for online education, avoiding any additional purposes specific to the provider. Minors' personal data requires special protection due to their potential lack of awareness of risks and rights. This protection should specifically prevent the use of their data for marketing or profiling. Educational institutions must inform all parties involved, including minors, about the essential aspects of data processing in a language accessible to them.

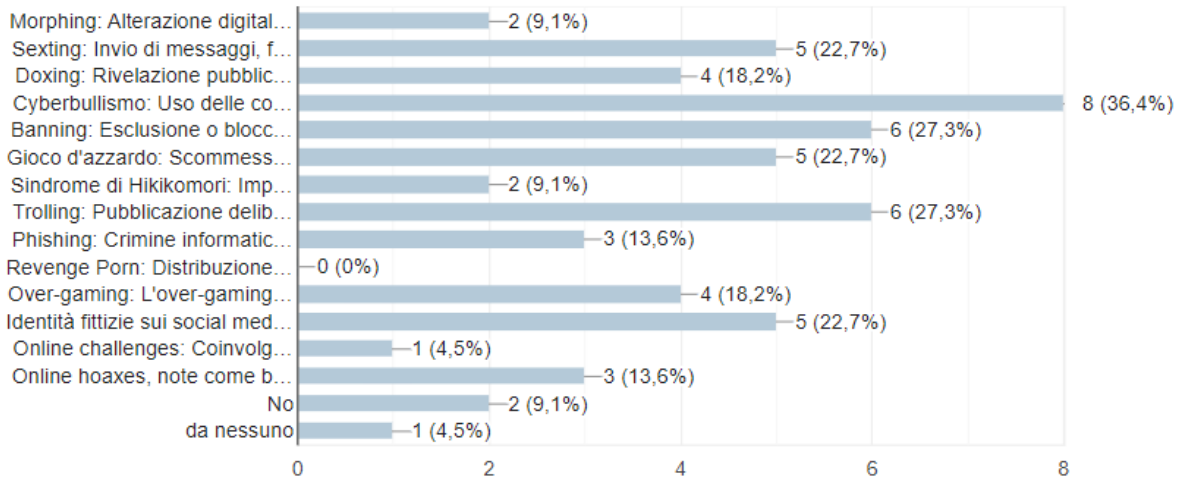
SECTION 6: LOCAL CYBER THREAT TRENDS

The data collected from youth respondents sheds light on the prevailing trends in local cyber threats. Approximately 45% of respondents reported initiating their usage of social media platforms between the ages of 10 to 12, and around 40% between the ages 13-15. Despite spending varying amounts of time online, with 35% spending more than three hours daily, there seems to be a disparity in their confidence levels in recognizing and avoiding potential cyber threats. Additionally, over 60% reported experiencing relevant negative emotions due to online bullying or cybercrimes.

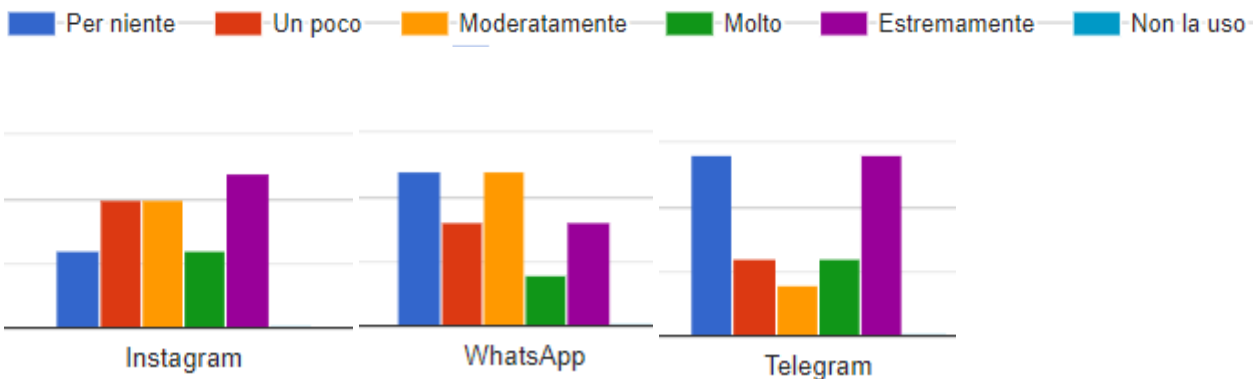
Based on direct experiences reported by the youth, several concerning trends in local cyber threats have been identified. Cyberbullying emerges as the most prevalent issue, with six respondents acknowledging personal encounters. This is closely followed by sexting and trolling, each reported by four respondents. Additionally, four respondents highlighted experiences related to gambling, while three reported encounters with fake identities on social media platforms. Doxing, over-gaming, morphing, and the Hikikomori syndrome were also cited as significant concerns, each mentioned by two respondents.

Tu o qualcuno che conosci è stato influenzato da una delle seguenti sfide online o minacce cibernetiche?

22 risposte



The social networks/platforms in which youth witness upper levels of cybercrimes are: Instagram, WhatsApp and Telegram.



Exploring the data reveals a myriad of emotional responses among the youth when encountering cyber threats, shedding light on the often overlooked psychological impacts lurking beneath the surface of online interactions.

The findings paint a nuanced portrait of emotional turbulence. Reported experiences from moderate to extreme levels:

- Close to 70% of individuals experienced feelings of anger, showcasing the pervasive nature of emotional reactions provoked by cyber threats
- Over 50% of respondents expressed feelings of hopelessness, underscoring the profound impact of cyber threats on mental well-being.
- Approximately 40% of loneliness, highlighting the complex interplay between digital connectivity and social isolation, and raising important questions about the long-term effects of cyber threats on mental health.
- 55% of respondents reported feeling at least moderately worried about their online safety, reflecting the pervasive nature of cyber threats and their potential to instil deep-seated anxiety in those who encounter them.

Insights from schools provide valuable perspectives on local cyber threat trends. Specifically: Sexting was noted as a significant concern due to past events. Additionally, the occurrence of online hoaxes, including the alarming possibility of causes related to the "Blue Whale Challenge," raised alarms, reflecting the prevalence of misinformation and deceptive content on digital platforms. Cyberbullying, another, was also flagged by the schools as one of the main detected cyber threats.

SECTION 7: COMMUNITY ENGAGEMENT

In Italy, addressing cyberbullying and fostering a safe online environment for minors involves both centralised reporting systems and decentralised initiatives led by various stakeholders. At the national level, legislative measures such as the "Legge sul cyberbullismo" (Cyberbullying Law) of 2017, provide a framework for combating online harassment. Under this law, minors or their parents can request the removal or blocking of offensive online content through website or social media platform administrators. Should the platform fail to respond promptly, the Italian Data Protection Authority can intervene to ensure the timely removal of harmful material, thereby safeguarding minors from cyberbullying incidents.

Additionally, decentralised strategies spearheaded by schools and NGOs further enhance the reporting and support mechanisms available to minors. Schools, as crucial stakeholders in the fight against cyberbullying, often implement dedicated reporting systems and peer support networks tailored to their educational environments. For instance, schools across Italy have implemented innovative approaches to address cyberbullying, including the establishment of online reporting platforms and confidential channels for reporting incidents. One notable example is a system developed by a school in Milan, allowing students and their families to report instances of bullying or cyberbullying through an online form. Similarly, another school provides a first-reporting module accessible to the entire school community, allowing anyone - students, teachers, parents, or administrative staff - to report incidents of bullying or cyberbullying. Reports can be submitted in various formats, either digitally or in print, and are directed to designated school personnel for further action.

Furthermore, NGOs like Telefono Azzurro play a vital role in providing support services and reporting avenues for cyberbullying victims. Through their toll-free helpline, available 24/7, and online reporting system that can be used also anonymously, Telefono Azzurro offers immediate assistance and guidance to those affected. Furthermore, Telefono Azzurro collaborates with the National Center for the Contrast of Child Pornography on the Internet (CNCPO) to investigate reported incidents and address illegal activities. This collaborative effort underscores the importance of community engagement in combating cyberbullying and promoting online safety.

SECTION 8: MAYOR CYBER RESILIENCY CHALLENGES

In exploring the primary challenges faced by students, particularly those aged 14-17, our survey uncovered a diverse landscape. While 13 out of 22 students demonstrated commendable awareness of cyber threats and the importance of critical internet usage, their familiarity with reporting protocols varied widely. Additionally, our findings revealed that 6 out of 22 students reported minimal parental control measures, and 4 indicating sparse ones.

Given the significant percentage of students experiencing varying levels of negative emotions in response to cyber threats, and the fact that 20 out of 22 students have either experienced or know someone who has experienced cyber threats, it's evident that structured and clear measures are imperative. Additionally, there is a pressing need for increased parental engagement to bolster cyber resilience efforts effectively.

In navigating the realm of digital safety within educational contexts, schools face a multitude of challenges, often stemming from difficulties in fostering open dialogues with students. Several factors contribute to this hurdle, including the age of students, which may deter them from openly discussing sensitive topics. Another significant barrier arises from societal pressures, as young individuals may hesitate to report or denounce acts of cyberbullying to authorities or designated representatives due to fear of social stigma or retaliation. This reluctance further exacerbates the challenges faced by schools in addressing digital safety concerns comprehensively.

In Disadvantaged neighbourhoods and among disadvantaged youth, establishing trust-based relationships becomes more intricate, compounded by parental unfamiliarity with digital safety and emotional intelligence.

Outlined within these challenges lie significant risks, including increased vulnerability to cyber threats, heightened emotional distress among students, and the perpetuation of harmful behaviours due to underreporting and lack of intervention.

Moreover, societal pressures and cultural norms play a pivotal role in shaping students' perceptions and behaviours, further complicating efforts to foster open dialogues and promote digital safety.

SECTION 9: FUTURE EXPECTATIONS

Future initiatives are needed to address the evolving challenges faced by schools and students. These initiatives may include:

1. Comprehensive Digital Safety Education Programs: Implementing comprehensive digital safety education programs is essential to empower students with the skills and knowledge to navigate online risks. These programs should encompass a variety of approaches:
 - **Formal Education**: Integrated into the curriculum, digital safety should be a mandatory part of Civic Education across all school levels.
 - **Non-formal Education**: Workshops and interactive activities can help reinforce learning and engage students in practical scenarios.
 - **Informal Education**: Peer discussions and online forums provide platforms for students to share experiences and strategies.
2. Peer Support Networks and Mentoring Programs: Establishing peer support networks and mentoring programs can provide students with avenues for seeking help and guidance. Peer support networks offer a valuable source of support and understanding for students facing online challenges, fostering a sense of community and belonging within the school environment.
3. Enhancing Parental Involvement: Enhancing parental involvement through workshops, seminars, and outreach programs is crucial for promoting digital literacy and fostering open communication between schools and families. By engaging parents as partners in digital safety education, schools can strengthen the home-school connection and empower families to support their children in navigating the digital world safely.
4. Strengthening Partnerships: Strengthening partnerships with community organizations, law enforcement agencies, and mental health professionals can provide holistic support for students' well-being. Collaborative efforts between schools and external stakeholders can enhance the



effectiveness of digital safety initiatives and ensure that students receive comprehensive support for their social, emotional, and mental health needs.

SECTION 10: CONCLUSIONS

Our consultations and survey findings have identified significant challenges and opportunities in enhancing cyber resiliency among Italian youth. Italy faces critical obstacles in safeguarding its youth from cyber threats, with cyberbullying emerging as a pervasive issue affecting many young individuals. The emotional toll of cyberbullying—feelings of anger, hopelessness, loneliness, and worry about online safety—underscores the profound impact these threats have on mental well-being.

Our research highlights the urgent need for proactive and comprehensive digital safety education programs. While many students aged 14-17 show commendable awareness of cyber threats and critical internet usage, their familiarity with reporting protocols varies widely. Notably, a significant number of students reported minimal parental control measures, highlighting the need for increased parental engagement in cyber resilience efforts.

Navigating digital safety within educational contexts presents a multitude of challenges. Schools face difficulties in fostering open dialogues with students, influenced by factors such as student age and societal pressures. Young individuals often hesitate to report acts of cyberbullying due to fear of social stigma or retaliation, complicating schools' efforts to address digital safety comprehensively.

Insights from schools provide valuable perspectives on local cyber threat trends. Cyberbullying remains a prevalent issue, with notable concerns about sexting and online hoaxes. The data highlights the significant emotional responses among youth encountering cyber threats, emphasizing the need for prioritizing mental health support in digital safety initiatives.

Moving forward, collaborative efforts among policymakers, educators, parents, and community stakeholders are crucial for developing tailored interventions and support networks. These efforts are essential to address the unique needs and challenges faced by Italian youth in the digital age and to promote a cybersecurity culture at all societal levels.

Italy: Bibliography

Ministero dell'Istruzione, dell'Università e della Ricerca (2020). *Linee Guida Didattica Digitale*. Retrieved from https://www.miur.gov.it/documents/20182/0/ALL.+A+ +Linee_Guida_DDI_.pdf/f0eeb0b4-bb7e-1d8e-4809-a359a8a7512f

Cybersecurity 360 (2021). *Strategia Nazionale di Cybersicurezza: ecco gli obiettivi da raggiungere entro il 2026 per la resilienza del paese*. Retrieved from <https://www.cybersecurity360.it/cybersecurity-nazionale/strategia-nazionale-di-cybersicurezza-ecco-gli-obiettivi-da-raggiungere-entro-il-2026-per-la-resilienza-del-paese/>

Ministero dell'Istruzione, dell'Università e della Ricerca (2017). *Piano nazionale scuola digitale*. Retrieved from <https://www.miur.gov.it/documents/20182/50615/Piano+nazionale+scuola+digitale.pdf/5b1a7e34-b678-40c5-8d26-e7b646708d70?version=1.1&t=1496170125686>

Ministero dell'Istruzione, dell'Università e della Ricerca (n.d.). *Piano Nazionale Scuola Digitale*. Retrieved from <https://scuoladigitale.istruzione.it/pnsd/>

Ministero dell'Istruzione, dell'Università e della Ricerca (n.d.). *Educazione Civica*. Retrieved from https://www.istruzione.it/educazione_civica/

Generazioni Connesse (n.d.). *Educazione Civica Digitale*. Retrieved from <https://www.generazioniconnesse.it/site/it/educazione-civica-digitale/>

Wired Italia (n.d.). *Cybersecurity: formazione nelle scuole con CyberChallenge*. Retrieved from <https://www.wired.it/article/cybersecurity-formazione-scuole-cyberchallenge/>

CybersecNatLab (n.d.). *Corsi CyberSec National Lab*. Retrieved from <https://cybersecnatlab.it/corsi-cybersec-national-lab/>

Ministero dell'Istruzione, dell'Università e della Ricerca (n.d.). *Scuola Futura - Cyber Security*. Retrieved from <https://scuolafutura.pubblica.istruzione.it/cyber-security>

TIM Enterprise (n.d.). *PIANO SCUOLA: I PROGETTI DI TIM SU PIATTAFORMA FUTURA*. Retrieved from <https://www.timenterprise.it/approfondimenti/pnrr-piano-scuola-piattaforma-futura>

Pianeta Giovani (n.d.). *Peer Education nelle scuole*. Retrieved from <https://www.pianetagiovani.org/peer-education-nelle-scuole/>

European Commission (n.d.). *Digital Economy and Society Index (DESI) - Italy*. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/desi-italy>

PowerDMARC (n.d.). *Cybersecurity in Digital Learning Environment*. Retrieved from <https://powerdmarc.com/it/cybersecurity-in-digital-learning-environment/>

Telefono Azzurro per ragazzi 13-18. Retrieved from <https://azzurro.it/ragazzi-13-18/#:~:text=Puoi%20contattarci%20telefonticamente%20sul%20numero,da%20telefonia%20fissa%20e%20mobile.>

Cyber High Schools (n.d.). Retrieved from <https://cyberhighschools.it/>

Agenzia per l'Italia Digitale (n.d.). *Misure Minime di Sicurezza ICT*. Retrieved from <https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict>

PORTUGAL

[Author: [Casa Do Professor](#)]

SECTION 1: NATIONAL CYBERSECURITY POLICIES

Published in 2021, The Portuguese Charter of Human Rights in the Digital Age, which represents a significant step forward in ensuring the protection of human rights in the digital age in Portugal, aims to ensure the fulfilment of the European Action Plan, safeguarding the rights, freedoms, and guarantees of citizens in the online world. Its 23 articles provide various rights, freedoms, and guarantees for citizens in cyberspace, being some of them extremely relevant in the realm of cybersecurity, for example, the right to be forgotten (the right to erase personal data, with support from the Portuguese State), and the right to privacy in digital environment and the right to cybersecurity.

The Portuguese police department, , together with the CNCS - National Cybersecurity Center, particularly through its cybercrime units and initiatives, actively advocates cyber resilience and promotes online safety awareness. There are specialised units, which are equipped with trained officers who investigate various forms of cyber threats, including online fraud, identity theft, hacking, and cyberbullying. By actively pursuing cybercriminals and providing support to victims, these units play a crucial role in enhancing cyber resilience. Furthermore, the police department regularly conducts public awareness campaigns to educate citizens about cyber threats and best practices for staying safe online. These campaigns often include workshops, seminars, and informational materials distributed through schools, community centres, and online platforms. By raising awareness about common cyber risks and preventive measures, the police help empower individuals to protect themselves online.

The cyber security initiatives in collaboration with schools, specifically focusing on students aged 14-17, are undertaken by the public security police department within the scope of the Integrated Proximity Policing Programme, in which the “Escola Segura” (Safe School) and “Internet Segura” (Safe Internet) teams develops awareness raising actions with the school community, addressing, among other topics, Internet security.

Within the above-mentioned Integrated Program, the Safe School Team is actively involved in promoting cyber resiliency and online safety awareness within the local community through a protocol established with schools, particularly with the school health team. The “Internet Segura” project aims to combat illegal content, minimize the effects of illegal and harmful content on citizens, promote safe use of the Internet, among others. The overall coordination of “Internet Segura” is the responsibility of the CNCS - National Cybersecurity Center and its members are the IPDJ - Portuguese Institute for Sport and Youth, the FCT - Foundation for Science and Technology, the DGE - Directorate-General for Education, APAV - Portuguese Association for Victim Support, the Altice Portugal Foundation and Microsoft. The Safe Internet project is supported by the European Commission, and has an international mission by cooperating with two international organizations: Insafe (BIK - Better Internet for Kids) and Inhope.

Every year, in the scope of the International Internet Day, these team carry out awareness raising actions in schools during two weeks and similar prevention activities are undertaken during the Teen Dating Violence Awareness Month. Besides these annual awareness raising actions, they are always available to cooperate with schools, sometimes working directly with the classes, when a specific issue arises.

SECTION 2: LOCAL CYBER SECURITY INITIATIVES

The cyber security initiatives in collaboration with schools are undertaken by the public security police department within the scope of the Integrated Proximity Policing Programme, in which the Safe School Team develops awareness raising actions with the school community, addressing, among other topics, Internet security.

Within the above mentioned Integrated Program, the Safe School Team is actively involved in promoting cyber resiliency and online safety awareness within the local community through a protocol established with schools, particularly with the school health team.

Every year, in the scope of the International Internet Day, this team carries out awareness raising actions in schools during two weeks and similar prevention activities are undertaken during the Teen Dating Violence Awareness Month. Besides these annual awareness raising actions, they are always available to cooperate with schools, sometimes working directly with the classes, when a specific issue arises.

Through the above mentioned programme, actions about online safety and responsible internet usage are carried out not only to educate students, but also parents and guardians. However, what is observed is that the number of parents and guardians who participate in these actions is very low, with the aggravating factor that those who need it most do not attend.

The police department states that to make educational efforts undertaken remain engaging and relevant to the local community's needs, it is necessary to involve other institutions, such as parish councils, companies and schools, which must be committed to continue promoting the issues covered. Although there is openness on the part of some institutions for this to be done, mainly in schools, they consider that it is not enough to carry out the actions if the promotion of prevention is not continued, since there is a risk that the shared knowledge falls into oblivion. Another way of ensuring that these educational efforts involve the community is by promoting prevention through their communication channels.

The police department refers that they know they have effectively enhanced cyber resiliency among the local community through the feedback they receive from the audience when carrying out awareness-raising actions. One example of this is when students report that they had no knowledge about those subjects and say that from that moment on they will change certain behaviours because they are informed, or through their guardians who, when meeting the police, report having been aware that they went to their children's school to carry out awareness-raising activities.

SECTION 3: EDUCATIONAL INTEGRATION OF NATIONAL CYBERSECURITY POLICIES

The main policy to prevent and address cyberbullying incidents in school is the training of young people and teaching and non-teaching staff, in order to detect evidence, signs or clues that show that a child may be a victim of any of these phenomena.

Students are educated about the consequences of cyberbullying, by internal actors, mainly by class teachers, but, there are also a vast number of actions are carried out in partnership with the Public Security Police Safe School Team as well as with the psychologists who belong to the school grouping.

In terms of subsequent monitoring, there is a large team of psychologists and internal technicians available to deal with the situations and provide support for victims. In addition to the disciplinary dimension for offenders, which must always be present students need to understand that there are borders that should not be crossed and that when they are there are always consequences both for the victims and even for potential aggressors.

As a sign of modern times, digital literacy education, covering social engineering, online privacy, cyberbullying, and responsible social media use, is provided by schools and this issue is integrated into the curriculum to ensure comprehensive education on these topics. Indeed, cybersecurity policies are part of the curriculum of some subjects, such as English and ICT, but these matters are addressed particularly in Citizenship classes, a transversal subject, throughout all school years. Furthermore, when what is part of the curricula is insufficient, the school carries out a range of activities with partner entities to achieve these ends, for example, with the Public Security Police Safe School Team, in the case of cyberbullying and online privacy, through awareness raising actions.

School consultation allowed us to understand that there are no written and structured cybersecurity guidelines for schools, but instead, a set of messages that are shared recurrently, in the form of internal training, provided through emails and alerts to do, for example, simple things, such as not having all the recipients' addresses in "CC" or "to", but use, for example, "BCC" with hidden knowledge. There are also several activities in this regard and peer-to-peer training in the sense of non-exposure on social media that mainly covers teaching staff and students.

SECTION 4: EDUCATIONAL APPROACHES FOR CYBER RESILIENCY

Enhancing cyber resilience among students implies addressing these challenges from a prevention perspective, through campaigns and awareness-raising actions within the school community. These can involve all the students or can be directly targeted at a specific group, which is signalled by the school. This work is usually done in collaboration with the police department, through the Safe School Team, but also with the school's psychologists, who undertake workshops to deal with this issue, who believe that sharing negative experiences due to the use of the Internet can be very useful to avoid similar situations or even to prevent others.

At the start of digital transformation, teachers were mostly focused on learning about digital security, data protection, and online safety. As a result, more training courses on these topics became available. Nowadays, there is something that can be called internal training, messages that are shared recurrently, through emails and alerts, and that emphasise best practices such as email etiquette to minimise cyber risks. The information about these issues is mainly shared to parents through social networks, which is a concern that schools have, they feel that carrying out parental education initiatives in this area is urgent. Even though there have been some workshops for parents/guardians, the number of participants is usually non-satisfactory.

Overall, cyber threats seem to have been addressed through a comprehensive approach in schools, encompassing various elements such as education, support, collaboration with external entities, internal policy reinforcement and communication, and digital literacy integration into the curriculum. This multifaceted procedure demonstrates a commitment to tackling cyber threats within the school environment by addressing it from various angles. However, not all these efforts are enough if the community is not involved, particularly regarding parent supervision. Schools, parents/guardians, students and other entities must work together and as a whole, in order to enhance cyber resilience at educational level.

SECTION 5: DIGITAL LEARNING PLATFORMS

In Portugal, the protocols to manage cybersecurity incidents impacting digital platforms involve coordination between various stakeholders, including government agencies, regulatory bodies, law enforcement agencies, cybersecurity experts, and the affected organisations. Although they may vary depending on the severity and nature of the incident, these are the general steps followed: incident detection and initial response, notification of authorities, coordination and information sharing, investigation and forensic analysis, mitigation and remediation, communication and public disclosure, post-incident analysis and lessons learned.

Integrating cybersecurity policies within digital learning platforms is essential to ensure the security and privacy of users, particularly students and teachers. Digital platforms are required to comply with data protection regulations and privacy policies, implement secure authentication mechanisms and strong password policies, enforce access control measures and implement encryption protocols to safeguard transmission of data and protect sensitive communications. These digital platforms also undergo regular security audits and assessments to identify vulnerabilities, assess compliance with security standards and mitigate potential risks, they have established incident response procedures to promptly detect, assess, and

respond to cybersecurity incidents and inform users about the reporting channels and steps to follow in the event of a security incident, they obey to regulatory requirements and industry standards related to cybersecurity, privacy, and data protection and comply with assessments and certifications, which demonstrate the platform's commitment to maintaining robust cybersecurity practices and protecting user data.

The use of digital platforms is governed by various cybersecurity guidelines and regulations aimed at ensuring the security, privacy, and integrity of digital systems and data, which encompass legal frameworks, industry standards, and best practices established by regulatory bodies, government agencies, and international organisations. The primary cybersecurity guidelines regulating the use of digital platforms in Portugal include the General Data Protection Regulation, Portuguese Data Protection Law, National Cybersecurity Strategy, National Cybersecurity Centre, Regulatory Authority for the Media, as well as industry standards and best practices, among others.

Moreover, relevant communication strategies are employed both in response to cybersecurity incidents and as part of ongoing cybersecurity efforts, in order to ensure effective communication, transparency, and collaboration among stakeholders, including government agencies, businesses, the public sector, and the general public. The key communication strategies are public awareness campaigns, incident response notifications, coordination with government agencies, collaboration with industry partners, public-private partnerships and cybersecurity training and education.

SECTION 6: LOCAL CYBER THREAT TRENDS

Cyberbullying is the most common cyber threat among young people, in line with the police and school consultation, even though a few cases of exposure were reported. The online survey also shows that it is the most prevalent threat, followed by fake identities on social media and sexting.

The police reports that other problems have been identified in the local area, affecting not only teenagers, but the community in general. In fact, they have recently received numerous complaints from citizens reporting encounters with individuals posing as someone else. These impostors coax victims into sharing intimate photos, only to demand ransom money thereafter. Within the school community, this scenario is also common, often stemming from students' naivety. They may not realize the consequences of their actions as they share everything and exercise little caution when selecting photographs.

The victim subsequently needs psychological support in several situations. The police disclosed an incident at a school in which classmates fabricated a false profile posing as a girl. They engaged in messaging with a boy who subsequently sent photos. Initially, the boy struggled to accept that his classmates were behind this, genuinely believing the messages originated from the girl and reflected her genuine interest. The victims are typically more vulnerable children, and to make matters worse, they may refuse to attend school, as they experience shame, which might require psychological and medical assistance. The police described another incident that had happened three weeks ago: a 16-year-old computer science student attending Year 11, received a message from an Instagram profile of a girl who asked him to send intimate photos which he did. The next day he received a message from an individual threatening to publish what he had sent if the student didn't deposit a certain amount of money. The victim panicked and went to the police station to file a complaint. Digital permanence indeed aggravates this whole situation because "once on the Internet, always on the Internet", which causes deep psychological scars.

SECTION 7: COMMUNITY ENGAGEMENT

The protocols for reporting cyber threats or incidents within the school community are those derived from the usual relationship with the security forces. As soon as the school becomes aware of a situation that could prove to be an infringement of the legal framework or a security risk, it promptly contacts the authorities. The entities immediately respect the school's diligence, go to the school and start the procedural consequences straight away.

During the welcoming meeting with the management in the beginning of the school year, the staff is informed about reporting procedures; the class teacher informs both parents and students during the first meeting and the first classes, respectively. The reporting instruments, depend on the channel, they can be an email to the data protection officer, an email to the management or contact with the class teacher. In case it is a situation diagnosed by a teacher or a peer, it is usually communicated to the class teacher or to the management, but sometimes the victims report these situations during psychologists' individual support sessions.

As for support during and after incidents, the school tries to make the entry and detection routes as numerous and informal as possible, so that students feel comfortable reporting situations, because sometimes they do not even realise that they are being victims of abuse. Aftercare support is readily available, with a team comprising of four psychologists, a social worker, a speech therapist, and other members of the Inclusion Supporting Multidisciplinary Team equipped to handle such situations within the school.

The school ensures the community is aware of digital safety policies and their importance through publishing general data protection regulations on the school's website, where the Data Protection Delegate is also identified, as well as the regular initiatives, the different warnings, the different awareness raising actions undertaken throughout each school year. The local police department, through the Safe School Team, engages the community in cyber resiliency strategies by promoting raising awareness actions and through their communication channels.

SECTION 8: MAYOR CYBER RESILIENCY CHALLENGES

The primary cybersecurity challenge faced by law enforcement revolves around cyberbullying, predominantly within school environments. While it can occur among the broader population, it is less prevalent. Crimes typically affecting individuals outside the school community often involve computer fraud, improper internet data usage, or sharing leading to identity theft. Conversely, within schools, the primary concern is cyberbullying.

According to school consultations, which highlight cyberbullying as a prominent issue, the primary obstacle in implementing digital safety measures is the extensive number of stakeholders: nearly 4 thousand students, 300 teachers, and 100 employees. This challenge is worsened by the changing of personnel each year, requiring ongoing training, preparation, and vigilance. Regrettably, occasional instances arise where unprepared individuals enter the picture, perpetuating vulnerabilities and posing ongoing risks.

The youth survey also points cyberbullying as the most prevalent cyber threats, followed by fake identities on social media and sexting.

Cyberbullying can trigger a range of emotional issues, including depression and anxiety, with severe cases leading to suicide. It can also induce social isolation due to fear or shame. Additionally, poor academic performance is another notable consequence of cyberbullying.

The main risks associated with sexting are embarrassment, humiliation, and damage to reputation if private images or messages are shared; it can also make teenagers vulnerable to exploitation by online predators.

Fake identities can lead to identity theft, fraud, loss of trust in interactions in online communities and platforms, among others.

These three challenges pointed by the teenagers who filled in the survey are deeply interconnected as fake identities can be used to harass, bully, or intimidate and sexts shared without consent can become tools for cyberbullying. All of them may cause significant emotional harm to the victims.

SECTION 9: FUTURE EXPECTATIONS

According to the responses of the youth survey findings, the majority of youngest people deny having participated in workshops or sessions at school focusing on online safety and responsible digital behaviour. Additionally, the document reveals that most parents do not implement parental control measures to ensure their children's digital safety and are not actively involved in discussions or workshops related to online safety and responsible internet usage.

Likewise, the police indicate lack of parental supervision as a serious problem, as many parents lack necessary computer skills to protect themselves, let alone their children, while, others spend minimal time with them. It's crucial to involve parents/guardians in supervising Internet usage and greater support from schools is also essential, since young people spend a lot of their time there. They also suggested extending the training provided to teachers within this project to include the security police as well, as well as sharing the ways of preventing risky behaviour adopted by the countries involved.

In accordance with school consultation, the possible improvement to enhance the school's digital security initiatives is to strengthen existing practices: maintaining heightened vigilance for peer pressure among students, and fostering continuous awareness among all stakeholders. Informed individuals can influence others positively pairs generate informed pairs, creating a ripple effect where teachers or students who are knowledgeable about good practices implicitly pass on these good habits to their peers leading to more meaningful learning experience.

Several forthcoming initiatives related to cyber threats may include an increased collaboration between schools, the police department and parents/guardians, from information sharing to the exchange of good practices and cybersecurity insights, increased cybersecurity education and even international cooperation.

Actually, a comprehensive approach to cybersecurity and enhanced cooperation can help identify and respond to cyber threats more effectively and facilitate coordinated efforts to combat evolving cyber risks.

SECTION 10: CONCLUSIONS

Schools' approach to preventing and addressing virtual challenges, such as cyberbullying incidents, and promoting digital literacy and cybersecurity is thorough and proactive.

Some notable highlights include the incorporation of online safety education into certain subjects' curricula and the reinforcement of key messages and skills related to cybersecurity, digital citizenship, and ethical online behaviour in crosscutting subjects like Citizenship classes. Additionally, peer-to-peer communication is encouraged, facilitating the sharing of experiences and best practices related to cybersecurity and digital safety, among both students and teachers. However, to ensure effectiveness and sustainability, it seems to be essential to enhance training for all staff members. While there were numerous training opportunities on cyber threats available for teachers in the past, such opportunities are now less common. Providing teachers

with more knowledge would facilitate discussions about cyber resiliency and online safety in the classroom, better preparing students to navigate these issues.

There's evident cooperation between the public security police department and schools in promoting educational initiatives centred on preventing cyberbullying, safeguarding online privacy, and promoting responsible social media use. This is facilitated through awareness-raising actions carried out by the Public Security Police Safe School Team. However, engaging parents/guardians, essential for the success of these measures, poses challenges. To address these challenges and ensure the sustainability of law enforcement and educational efforts it is crucial to continue promoting awareness messages on cybersecurity through both communication channels', to reach not only students but also parents/guardians.

In summary, it's clear that the greater the number of lessons and activities provided, the more empowered students become to make informed decisions and develop critical thinking skills in Internet usage. Similarly, for teachers, the more training and skills acquired, better equipped they are to assist students in adopting responsible behaviours.



Portugal: Bibliography

European Commission. *Online privacy and safety*.

<https://digital-strategy.ec.europa.eu/en/policies/online-privacy>

European Commission. (2020). *Communication strategies for cybersecurity incidents*.

Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=ES>

European Union Agency for Cybersecurity. (2018). *General Data Protection Regulation (GDPR)*.

Retrieved from <https://www.enisa.europa.eu/about-enisa/data-protection>

European Union Agency for Cybersecurity. (2020). *National Cybersecurity Strategies*.

Retrieved from <https://www.enisa.europa.eu/topics/national-cyber-security-strategies>

National Institute of Standards and Technology. (2020). *Cybersecurity Framework*.

Retrieved from <https://www.nist.gov/cyberframework>

National Institute of Standards and Technology. (2020). *Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations*.

Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

Portugal Digital. (2022). *National Strategy for Cyberspace Security*.

Retrieved from <https://portugaldigital.gov.pt/en/accelerating-digital-transition-in-portugal/get-to-know-the-digital-transition-strategies/national-strategy-for-cyberspace-security/>

Portugal.gov.pt (2022). *Novo Regulamento dos Serviços Digitais em vigor*.

<https://eportugal.gov.pt/noticias/novo-regulamento-dos-servicos-digitais-em-vigor>

Portuguese Republic. (2018). *Lei de Proteção de Dados Pessoais*. [Portuguese Data Protection Law]. Retrieved from

https://www.cnpd.pt/bin/rqpd/Lei_67_98.pdf

Portuguese Republic. (2019). *Estratégia Nacional de Cibersegurança*. [National Cybersecurity Strategy]. Retrieved from

<https://www.cncs.gov.pt/pt/estrategia-nacional/>

Portuguese Republic. (2020). *Centro Nacional de Cibersegurança*. [National Cybersecurity Centre]. Retrieved from

<https://www.cncs.gov.pt/>

Portuguese Republic. (2021). *Carta Portuguesa dos Direitos Humanos na Era Digital*. [Portuguese Charter of Human Rights in the Digital Age]. <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-164870244>

Programa Escola Segura da PSP. (n.d.)

Retrieved from <https://www.psp.pt/Pages/atividades/programa-escola-segura.aspx>

Regulatory Authority for the Media. (n.d.). Retrieved from <https://www.erc.pt/pt/>

ROMANIA

[Author: [Centrul Judetean de Resurse si de Asistenta Educationala Botosani](#)]

SECTION 1: NATIONAL CYBERSECURITY POLICIES

In Romania, the National Cyber Security Directorate (DNSC) spearheads cyber security coordination nationally. While collaborating with various public institutions, many of these have a military focus, prioritising national defence. These entities constitute the National Cyber Security System, overseeing strategic cyber security efforts. For civilian concerns, DNSC has issued extensive cyber security regulations, alongside GDPR policies for personal data protection. In 2022, the Romanian Government endorsed a Cyber Security Strategy for 2022-2027 (Government Decision no. 1321, 2021). Despite these actions, Romania's cyber security development remains uncertain, as legislative regulations insufficient address the rising tide of cybercrime.

In Romania, existing laws address violence situations, drawing from international conventions like the UN Convention on the Rights of the Child. Laws such as Law no.18/1990, Law no.272/2004, and Law no.217/2003 focus on protecting children's rights and combating domestic violence. However, there's a lack of specific national cybersecurity policies for young people aged 14-17. Instead, current policies cover all citizens and prioritise safeguarding critical infrastructure, personal data, and national security.

ORDER No 4.343/2020, issued on May 27, 2020, targets psychological violence, particularly bullying, aiming to foster a safe environment in educational settings. It provides guidelines for preventing, identifying, and intervening in instances of bullying and cyberbullying in the pre-university education system. Despite institutional efforts, public awareness and education on online safety remain inadequate. Limited media coverage and sporadic awareness campaigns fail to sufficiently inform or shield the population from cyber threats.

Some objectives outlined in the order are carried out by school counsellors from the County Centre for Educational Resources and Assistance. These specialists aid in identifying potential violence victims, providing counselling to victims and their families, implementing violence prevention activities, and more. In Romania, in the context of European Union (EU) policy, several directives and regulations on cyber security have been adopted and implemented. Among the most important are:

1. NIS (Network and Information Security) Directive - This is one of the most significant EU initiatives in the field of cyber security. The NIS Directive was adopted in 2016 and imposes standards and requirements for cyber security across the EU.
2. GDPR (General Data Protection Regulation) - Although not specific to cyber security, GDPR is closely related to this area through its regulations on personal data protection.
3. European Cyber Security Strategy - The EU has adopted a series of cyber security strategies and action plans to improve resilience and responsiveness to cyber threats at European level.

To increase citizens' awareness of the danger of cyber-attacks, the Romanian Police carried out more than 1.620 prevention activities at the national level in 2022 alone. Beneficiaries received advice on how to spot online fraud attempts and what to do to avoid becoming a victim (Press release M.A.I, 2022).

SECTION 2: LOCAL CYBER SECURITY INITIATIVES

Local cyber security initiatives, primarily led by the County Police Inspectorate, participate in national-level online safety programs run by the Romanian Police. These initiatives encompass both county-wide projects

and smaller campaigns, although they may not always prioritise student engagement. Instead, they often target teachers and parents, with significant participation from schools, especially following high-risk cyber events or prevention activities.

Local cyber security initiatives involve collaborations between companies, institutions, and the Police Inspectorate to conduct education activities based on a county-level safety plan. These efforts extend to schools, supported by partnerships with external organisations offering digital education solutions. Additionally, annual partnerships address cyber safety concerns, including the prevalent issue of minors coerced into providing compromising photos.

A study carried out by the NGO World Vision Romania (2023) found that over a third of teenagers experienced sexual messages from adults online, and 40% faced online bullying. Additionally, 10% encountered fake content using their image or voice. Many bullied students felt powerless, angry, or sad, with some unsure how to recognize victimisation. Nearly a quarter reported incidents of peer threats like revenge porn. Most students preferred confiding in teachers or principals when facing abuse. Surprisingly, only one in five considered contacting the police for help. To address these issues, World Vision Romania released educational videos on International Safer Internet Day 2023, using AI technology and TikTok to equip teenagers with strategies to combat online abuse. These resources are available on the organisation's website

In the past year, there has been considerable media attention on cases of violence, including cyber-violence. Authorities have conducted information campaigns highlighting the legal repercussions of such crimes in Romania, which range from fines to suspended imprisonment and even imprisonment with execution, depending on the severity of the offence. Additionally, in 2023, a significant milestone was reached with the first conviction in a cyberbullying case. The incident involved the cloning of a teacher's social media account, where offensive content was distributed by two students. As a result, the students were ordered to pay moral damages to the teacher. These developments underscore both the growing awareness of cyber-violence and the legal consequences associated with such behaviour (Ziarul de Cluj, 2023).

SECTION 3: EDUCATIONAL INTEGRATION OF NATIONAL CYBERSECURITY POLICIES

At the national level, legislative concern has arisen to regulate and introduce anti-disinformation education in schools. There is in the Romanian Parliament the Draft Law for the introduction of the subject "Media Education and Culture" in pre-university education - PL-x no. 326/2019 which specifies that "the subject proposed by this law will include mandatory teaching of communication theories, training of a critical and analytical mechanism for the reception of news, identification of manipulation of information for the benefit of extremist or anti-democratic interests, filtering of information whose ultimate purpose is to restrict and threaten fundamental rights, identification of fake news" (Joamisoa, 2020, p.223).

There is currently no code of conduct governing online safety. Apart from the GDPR policies and security protocols provided by the platforms used to carry out school activities, there are no other legal regulations. According to the new education law no. 198/2003 in Romania, mobile phones are forbidden in schools, and students can only access the internet through computer booths or library computers. Each school has internal rules of operation that also include rules on the conduct of staff and students.

The national SMART-EDU project (Modern, Accessible, Resource-based School and Digital Technologies 2021-2027) is currently being implemented and has set out several priorities including the creation of a digital education ecosystem based on clear ethical principles, the development of digital competences for the digital transition towards a competitive society, focused on sustainable development, social equity and resilience, digital literacy and combating disinformation.

A test that measured and analysed the digital literacy of students from grades I-XII in Romania in 2022 indicated that only a quarter of students have a functional level of digital skills, which represents a very small percentage compared to the results obtained in other European countries. (Radu Pârcă, 2023).

One cause of these results is the fact that schools in Romania offer digital education which is rather theoretical. This boils down to classroom hours or various extracurricular activities, but insufficient for current needs.

In the gymnasium there is the discipline of Computer Science and Information and Communication Technology (I.C.T.) with one hour per week allocated and at the high school level, Information Technology and Computer Science is studied, depending on the profile, 1-2 hours per week.

The measures to prevent and control cyberbullying are framed in a broader context and are included in the "Procedure regarding the management of cases of violence against ante-preschoolers / preschoolers / pupils and school staff, as well as other correlated situations, in the school environment and suspicion of violence against children outside the school environment" approved by Minister Order nr. 6.235/2023. This procedure provides for the obligation to implement a mechanism for anonymous notification of suspicions and acts of violence, in accordance with the provisions of Article 65 of the Law on pre-university education nr. 198/2023 (Official Gazette of Romania, 2023).

SECTION 4: EDUCATIONAL APPROACHES FOR CYBER RESILIENCY

Structured educational approaches regarding the awareness of students regarding cyber security appeared in 2016, when according to ORDER no. 3590 of April 5, 2016, the framework plan for the secondary school cycle was changed (Ministry of National Education And Scientific Research, 2016).

School programs aim to cultivate skills in computing, communication, critical thinking, and creativity, emphasising the importance of securing computers, networks, and Internet use. Optional high school subjects like Introduction to IT Security and Artificial Intelligence cover cyber security, but uptake is limited due to insufficient offerings and student interest. In recent years, programs of the following type have been implemented:

- "Net Hour" - run by "Save the Children!" (O.N.G.) It included several awareness campaigns on cyber threats: "Give BLOCK to aggression! And the "jokes" miss. Stop cyberbullying!" (2018 – 2019) "A world without fear" (2019) (Net Hour, nd).
- "Heroes of the Internet" - made in collaboration by the Ministry of Education, the Romanian Police, the Ministry of Education and Research of the Republic of Moldova, Radio Itsy Bitsy, Radio Kiss. It is aimed at students between the ages of 7 and 15, but it can also be successfully accessed by young people aged 14-17. The program includes several types of activities for students: an optional, a contest, an online game (Heroes of the internet, online safety program for children, n.d.).
- "Cyber4Kids" - provided by certSIGN and comprises a series of animated films that talk in a simple way about what cyber security means. Each episode is accompanied by a guide with tips: one page for parents and one for children (Cyber4Kids, nd).
- "Online Security" - carried out by the Romanian Police, in partnership with the National Directorate of Cyber Security (DNSC) and the Romanian Association of Banks (ARB) offers good cyber security practices, to avoid internet users becoming victims of computer fraud, child pornography or malware attacks (Online Safety, n.d).

Training sessions and workshops designed for professors to stay updated on cybersecurity matters

Casele Corpului Didactic, specialised institutions for teacher training, offer training courses on cyber security. Unfortunately, the offer is limited because there are few such institutions that offer these courses.

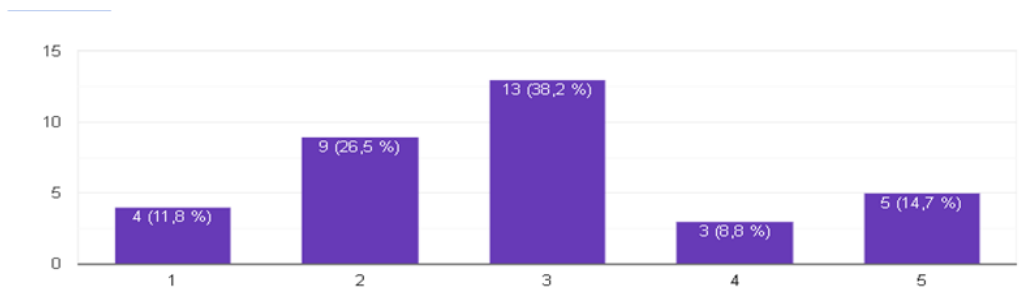
Twenty higher education institutions have introduced or are about to introduce post-graduate (short-term) and master's courses in cyber security into the university curriculum.

There are cyber security training programs offered free of charge by private companies and government organisations such as those in the projects listed above; the CYGER-AID platform; The CyberStarter project belonging to the EOS Foundation; Adservio e-learning platform.

Involvement of parents in initiatives related to cybersecurity education.

The school encourages parental involvement in cyber security through presentations, round tables, and information sessions, but participation remains low, especially among those who may benefit the most. National programs include training for parents through webinars, outreach activities, e-learning courses, and information materials on online safety. Despite educational efforts, only 23.5% of students feel adequately informed about digital literacy topics like online privacy and cyberbullying prevention.

Have you gained knowledge of digital literacy, including topics such as social engineering, online privacy and cyberbullying prevention, in the subjects you studied at school?



Statistical data to certify educators' confidence in integrating online resilience lessons does not exist.

In the survey conducted, the teaching staff as well as students and the police representative emphasise the need for a more consistent structured education.

SECTION 5: DIGITAL LEARNING PLATFORMS

Learning platforms aimed at creating a safe online environment are mainly focused on basic digital literacy, targeting mainly primary and secondary school students. The main shortcoming of these platforms is a predominantly expository character.

Digital learning platforms are the preserve of private players, who work with schools on an ad hoc basis on online safety issues. The most prominent of these are:

- Adservio: is the platform with the highest media visibility, designed as an educational process management platform, the primary function being of electronic school catalogue.
- CRED project: CRED (Relevant Curriculum, Open Education for All) contains open educational resources (R.E.D.) developed by teachers.
- Edus: an online educational management platform. It manages internal school processes or dedicated processes for online teaching.

- Intuitext School: educational portal with interactive lessons. Also contains features for class management.
- Brio: Brio tests are standardised digital tests, through which Romanian students in grades I-XII can objectively assess their knowledge in the main school.
- Digitaliada: centralised platform with materials developed in LIVRESQ-type platforms and text editors. It also contains useful features for principals, teachers and parents.
- iTeach: a dynamic platform that is becoming increasingly popular in our country.
- sigurantaonline.ro: a national project to raise awareness about online threats launched by DNSC, Romanian Police and the Romanian Association of Banks (ARB).

Cybersecurity platforms are designed to raise awareness, but they are not sustainable: the resources often become unavailable when the project ends.

The guidelines for safe internet use and privacy protection have been developed by various NGOs, which have targeted collaborations with public institutions:

- Safer Internet Guidelines - Safer Internet for all children. It was developed by the Save the Children! organisation as part of the Net Hour project.
- Internet Heroes - Family Guide. A guide developed by the NGO ADFaber in collaboration with the Romanian Police, contains some important recommendations for parents.
- Safe first steps in digital life - A guide for parents and educators. The result of a collaboration between the Ministry of Communications and Information Society and CERT-RO.

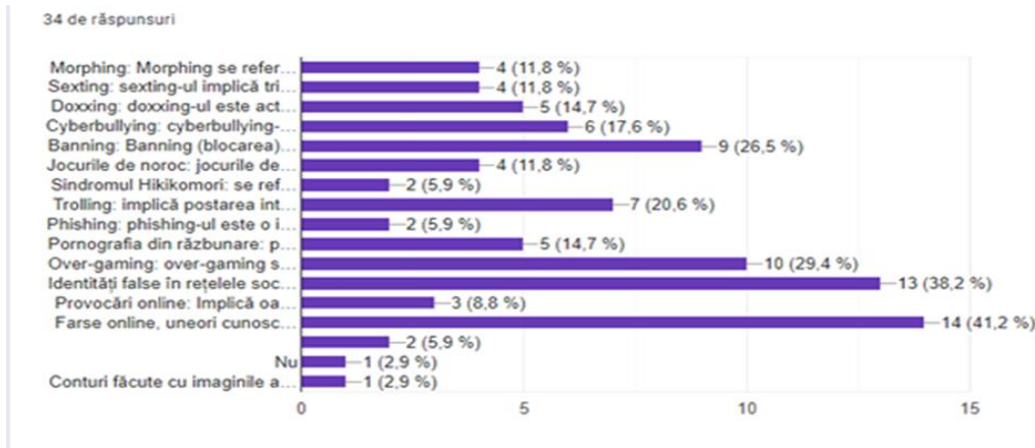
Romania's cyber security strategy, approved by GD (Governmental Decision) no. 271 / 2013, states in the introductory part the importance of communication between the relevant actors.

Regarding the steps to follow in the event of a cyber incident, there are no existing protocols in the schools. However, the National Cyber Security Directorate (DNSC) recommends the following steps, consecutive to a cybersecurity incident: Immediately notify the DNSC and users affected; work with the team dispatched by DNSC; switching the compromised platform to offline mode; using backups to restore the system; determine the attack vectors used; updating the organisation's cybersecurity policies; hold an organisation-wide meeting to draw conclusions and prevent further incidents.

SECTION 6: LOCAL CYBER THREAT TRENDS

Young people who participated in the online survey consider the most common cyber threat to be online pranks (41% of respondents). Fake identities are another important trend (38%), followed by over-gaming (29%) and banning (27%). Then we have, in order, trolling (21%), cyberbullying with 18% of responses, doxxing (15%). The least common threats are Hikikomori syndrome and phishing with 2 out of 34 responses.

Have you been affected (or someone you know) by one of the following online challenges or cyber threats?



In the County Police Inspectorate, most of the crimes recorded in the county are related to the transmission of pornographic material combined with threats or blackmail. Another common threat is morphing, to blackmail a person or make them look bad out of revenge.

From the point of view of schools, among the most common cyber threats are cyberbullying and online challenges. Detection of these is only done through student or parent reporting. It is addressed by counselling both the victimised pupils and the bullies.

Schools in Romania do not have the means to monitor students' online activity, even if they try to limit online access from students' mobile phones during school time.

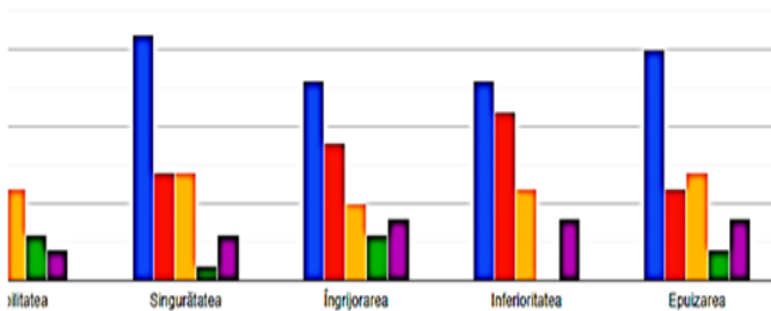
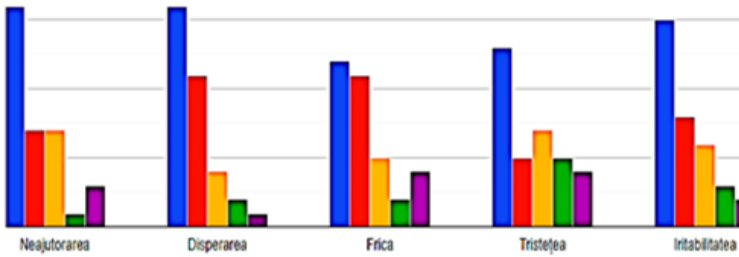
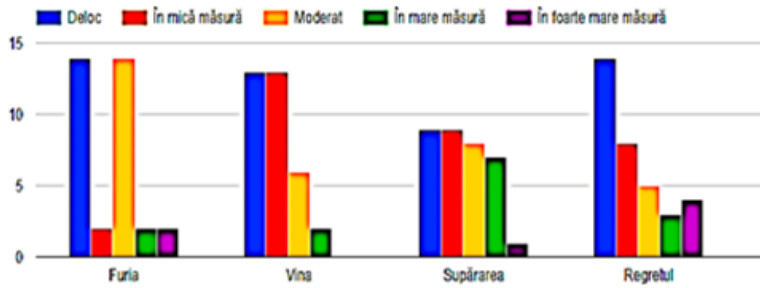
Common parts of different sources reporting cyber threats would be exposure of young people to inappropriate content, pornographic content, violence and theft of personal data.

For students, cyber threats revolve around two main themes. Firstly, they are vulnerable to fear-inducing online content designed to shock and provoke anxiety, yet they also seek out such content for the emotional intensity it provides. Secondly, they face identity-related threats such as fake identities, trolling, cyberbullying, excessive gaming, and exclusion from online interactions, which are particularly concerning due to their need for social affiliation.

From the perspective of police, law enforcement concerned with cybercrime, the main problem is students' overexposure to the online environment, their aptitude to continuously broadcast their lives to strangers on the internet. Police and departments fighting cyber threats are concerned that minors do not limit their personally identifiable information on various social networks, making them targets for predators actively seeking new victims: paedophiles, pimps, scammers.

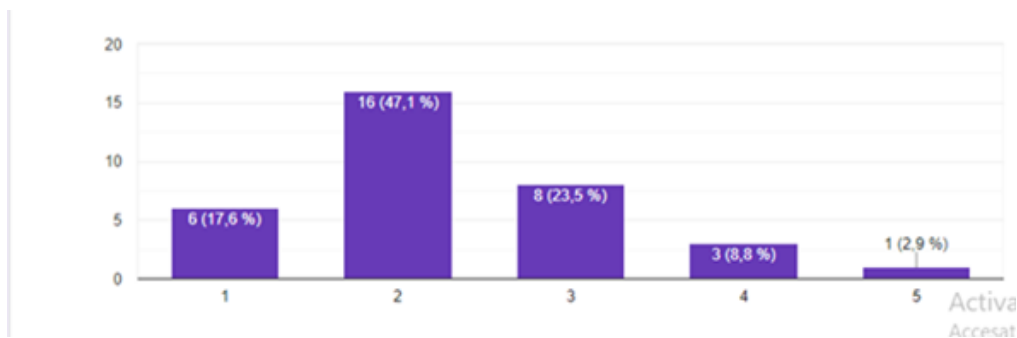
Of the 34 young people in the online survey group, only one experienced negative emotions to a very great extent as a result of bullying or cybercrime, 3 to a great extent and 8 moderately. In terms of emotions, to a very great extent they felt regret, fear, sadness, worry, inferiority and exhaustion (4 respondents each), to a great extent they felt anger (7) and sadness (5), and to a moderate extent they felt anger (11), sadness, loneliness, helplessness and exhaustion (7 respondents each), irritability and inferiority (6 respondents each).

What were the negative emotions you felt as a result of online bullying?



It is observed that young people are reluctant to acknowledge the intensity of the negative emotions they experience when they encounter or are victims of cyber threats.

To what extent has online bullying or various cybercrimes caused you negative emotions?



SECTION 7: COMMUNITY ENGAGEMENT

Until 2023, monitoring online behaviour was not a school activity and could not influence it. In 2023 a set of standard procedures were adopted to be followed in the case of violence in the school environment (OME no. 6235, 2023). Within these procedures the focus is mainly on physical violence, but teachers also use them in cases of cyberbullying. According to them, if threats are detected, the person who detects them will inform the head teacher and he/she will then inform the relevant authorities (police, DGASPC). There are no other specific procedures for cyber bullying now.

In fact, clear, official recommendations on appropriate online conduct for students and staff, including the use of social media and respectful communication, do not exist in schools. What does exist is at the level of verbal advice that some understand, others do not. However, 70.6% of pupils say they are familiar with the existence of clear rules on appropriate online behaviour, rules provided by the school, including on the use of social media and respectful communication.

The National Directorate of Cyber Security has published a "Cyber Security Planning Guide" that includes recommendations for action in the case of various cyber threats: privacy and data protection; scams and fraud; network security; website security; email, mobile devices; employees, use of bank cards, response to incidents, development and management of policies. It can help companies, institutions and individual users.

The engagement strategy is based on two pillars: 1 Operational collaboration between stakeholders to exchange information, increase visibility and fuel creative cybersecurity solutions; 2. Educating organisations, end users about cyber dangers and risks and how they can help promote security best practices in the future.

In terms of schools' relationship with the rest of the community, the main activities where cybersecurity issues are raised are the parent meetings organised by the head teachers and the parent lectures organised by the school counsellor. Elements of cyberbullying are discussed during these activities. Unfortunately, only a small number of people take part in the activities, which is why the information does not reach enough people.

SECTION 8: MAYOR CYBER RESILIENCY CHALLENGES

The study conducted in Romania by the NGO Save the Children in 2019 shows that students between 14 and 17 years old can face various challenges when it comes to cyber safety. Here are some of them: theft of personal data; inappropriate posts; approaching them by strangers; inappropriate communication on the internet; hacking or cloning accounts; use of unprotected devices (Save the Children, 2023).

According to the analysis carried out by the Ministry of Education and Research in 2021, presented in the draft Strategic Initiative for Digitization of Education in Romania (SMART-Edu, 2020) the challenges faced by most educational establishments and institutions are:

- Decentralised IT - most educational entities manage their own IT systems. They have a wide variety of IT systems based on their requirements. Due to this diversity and the spread of the network, implementing security policies becomes difficult;
- BYOD (bring your own device) culture;
- Open networks;
- Insider threats - Insider threats are the most common of all other cyber threats. An insider attack can be initiated by phishing email or by transferring sensitive information to personal or unsecured devices.

In recent years, police have faced familiar cyber threats, with grooming cases posing a continuing challenge. Collaborating with schools involves fostering proactive reporting to address cyber threats before they escalate, rather than reacting after incidents occur.

Theft of personal data and inappropriate online posts directly impacts students' self-image, often orchestrated by adults seeking to exploit minors. Schools struggle with decentralised IT practices, lacking national security standards and teacher education on cyber risks.

Underreporting of cyber incidents by both students and schools is a major hurdle, exacerbated by poor communication among students, schools, and law enforcement. Limited awareness of cybersecurity

practices and inadequate coordination hinder the effective implementation of cybersecurity policies and laws.

SECTION 9: FUTURE EXPECTATIONS

A 2020 survey by Adfaber in Romania found that 83% of students aged 13 to 17 want to learn more about using the Internet safely (Dumitru, V., 2020). In a notable initiative, four high schools in Cluj-Napoca, Timișoara, Iasi, and Bucharest piloted a project to teach cyber security and hygiene to students.

To enhance cyber safety education, the police representative suggests integrating a cyber-safety learning module into subjects like social education and counselling, partnering with the Ministries of Education and Home Affairs. This module would cover various aspects of cyber threats, crimes, prevention strategies, and victim response, ideally introduced early in the curriculum to address students' existing cyber experience.

The challenge lies in recognizing that the online world parallels the real world, necessitating similar security measures. Future efforts should focus on raising awareness among young people about the importance of following rules and maintaining safe conduct online.

Improving cyber safety requires establishing a platform for students to report online abuse promptly and confidentially. Collaboration with authorities such as the Romanian Police and the Ministry of Education is proposed to create such a platform.

The Cyber Security Strategy for 2022-2027 sets out five key objectives, including securing networks, strengthening regulatory frameworks, and promoting public-private partnerships.

The Ministry of Education has included the Cybersecurity Olympiad in the national school Olympiads calendar, starting in 2024.

The National Cyber Security Directorate (DNSC) aims to train 5,000 teachers in cybersecurity by 2026 through the "Building new cybersecurity skills for society and economy" program, funded by the NRP. Additionally, a national cybersecurity curriculum will be developed by DNSC for pre-university and university levels

SECTION 10: CONCLUSIONS

The Romanian Police prioritise cybersecurity, designating it a national priority since 2011. They conduct programs at national and local levels to promote cyber resilience and online safety awareness, targeting students, teachers, and parents. While there's no specific program for ages 14-17, all initiatives are tailored to this group. Collaboration with schools includes prevention activities against cyber threats, emphasising reporting by teachers. Local cybercrimes often involve distributing pornographic material, data theft, or hacking, with grooming as a significant concern. Police respond with preventive measures and legal adaptations. Success is measured quantitatively by participation, lacking studies linking activities to decreased cyber incidents. Psychological support for cyber threat victims falls outside police jurisdiction, directed to relevant institutions. A recommendation is to integrate cybersecurity into the educational curriculum consistently.

Following consultation with our associate partner, it was found that the current focus is mainly on carrying out activities and procedures to protect students from all forms of violence. The most frequent activities focused on recognising various forms of violence or aggression in the online space. Now the school does not have the necessary levers to monitor online activity, all that can be done now is to limit access to the phone. Also reporting violence can only be done by students or parents, the school can only offer counselling services



to both victims and aggressors. Counselling is carried out by the school counsellor who is part of the CJRAE network.

By the age of 15, all students surveyed use social media, with 70% starting before age 13-15, raising concerns about their well-being. Most spend over three hours daily on social networks, potentially impacting judgement and increasing the need for social validation. Student responses tend to centre around the middle option, with notable trends: feeling supported by school regarding cyberbullying, receiving information on cyber threats, adhering to school-provided social media guidelines, and learning about digital safety policies. Top online challenges include online pranks, fake identities, over-gaming, banning, and cyberbullying. Only 12% report negative emotions from online bullying, which tend to diminish over time. Respondents express confidence in recognizing and avoiding online threats (73%).



Romania: Bibliography

Cyber4Kids (n.d.), Cyber4Kids Home. Available at: <https://www.certsig.ro/en/cyber4kids/> Retrieved February 17, 2024.

<https://www.cybershield.org/proiecte> (2023). Proiecte. Available at: <https://www.cybershield.org/proiecte>. Accessed on: February 12, 2024

Codul Penal (2009) - Frauda informatică. Available at <https://lege5.ro/gratuit/gezdmnrzqi/frauda-informatica-codul-penal?dp=gqytsojvga3ds> Accessed on: February 20, 2024

Dumitru V. (2020, October 21). Online dangers: 8 in 10 students say school doesn't prepare them to use the internet safely. Available at: <https://spotmedia.ro/stiri/it/pericole-online-8-din-10-elevi-spun-ca-scoala-nu-i-pregateste-pentru-a-folosi-internetul-in-siguranta>. Accessed on: February 29, 2024.

FCC - Federal Communications Commission, SUA (2016). Îndrumar de planificare a securității cibernetice. Available at: <https://dnsc.ro/vezi/document/g-east-indrumarul-de-planificare-a-securitatii-cibernetice>. Accessed on: February 19, 2024

Government Decision no 1321 (2021). Romania's Cybersecurity Strategy for the period 2022—2027. Official Gazette of Romania no 2, January 3, 2022. Available at: <https://cdn.edupedu.ro/wp-content/uploads/2022/01/Monitorul-Oficial-Partea-I-nr.-2Bis.pdf>

Heroes of the internet, online safety program for children (n.d). Available at: <https://adfaber.org/eroii-internetului/> Retrieved February 17, 2024

Jaomiasa Handy-Francine (2023). Educația pentru o lume digitală. Studiu de caz: educația școlară pentru combaterea dezinformării online, Securitatea cibernetică: Provocări și perspective în educație, pp 221-228 Available at <https://dnsc.ro/vezi/document/cybersecurity-provocari-perspective-educatie>

Ministry Of National Education and Scientific Research (2016, 15 June). ORDER no. 3,590 from April 5, 2016 regarding the approval of the educational framework plans for secondary education. Available at: <https://legislatie.just.ro/Public/DetaliiDocument/179198> Accessed on: February 25, 2024

Ministry of Education (2020), ORDIN nr. 4.343/2020 din 27 mai 2020 privind aprobarea Normelor metodologice de aplicare a prevederilor art. 7 alin. (1[^]1), art. 56[^]1 și ale pct. 6[^]1 din anexa la Legea educației naționale nr. 1/2011, privind violența psihologică - bullying, Available at: https://www.edu.ro/sites/default/files/fi%C8%99iere/Legislatie/2020/OMEC_4343_2020_norme%20antibullying.pdf Accessed on: February 16, 2024

Ministry of Education (2023). ORDER no. 6.235 of September 6, 2023. Available at: https://edu.ro/management_cazuri_violenta . Accessed on: February 20, 2024

Ministry of Family, Youth and Equal Opportunities (2023). 19 noiembrie, Ziua Mondială de prevenire a abuzului și violenței împotriva copiilor. Available at: <https://copii.gov.ro/1/19-noiembrie-ziua-mondiala-de-prevenire-a-abuzului-si-violentei-impotriva-copiilor/>. Accessed on: February 21, 2024

Net Hour (nd). About the project. Net time. Available at: <https://oradenet.ro/despre-proiect/> Accessed on: February 24, 2024

Official Gazette of Romania (2023, July 5). Law on pre-university education. Available at: https://edu.ro/sites/default/files/fi%C8%99iere/Minister/2023/Legi_educatie_Romania_educata/legi_monitor/Legea_invatamantului_preuniversitar_nr_198.pdf

Online Safety (n.d.). Home Online safety. Safety Online - Safety Online (site). Available at: <https://sigurantaonline.ro/> Accessed on: February 21, 2024

Pârcă R. (2023, April 26), Most Romanian students do not have digital skills. "Whole generations that may be unable to handle the challenges of the future". Available at: <https://www.wall-street.ro/articol/Educatie/296659/majoritatea-elevilor-romani-nu-au-competente-digitale-generatii-intregi-care-ar-putea-to-be-unable-to-manage-the-challenges-of-the-future.html>. Accessed on February 17, 2024.

Press release MAI (2023, March 8), Press release Ministry of Internal Affairs. Available at: <https://www.mai.gov.ro/comunicat-de-presa-702/#>. Accessed on: February 15, 2024.

Rebe Nathalie (2023) Cyber Law. How to Upgrade Knowledge at the University Level: Building the New Generation of Cyber Professionals, Securitatea cibernetică: Provocări și perspective în educație, pp49-57 Available at <https://dnsc.ro/vezi/document/cybersecurity-provocari-perspective-educatie>

SmartEdu (2020) - Strategic Initiative for Digitization of Education in Romania (SMART-Edu 2021-2027) Available at: <https://www.smart.edu.ro/> Accessed on: March 3, 2024

Save the Children (2023, December 6), Annual Report. Available at: https://www.salvaticopiii.ro/sites/ro/files/migrated_files/documents/f4a4c546-799e-4e9d-bea1-32d3694b5d21.pdf. Accessed on: February 23, 2024

Tofan, D. (2024). Starea pieței de securitate cibernetică în România. Available at: <https://www.contributors.ro/starea-piete-de-securitate-cibernetica-in-romania/> Accessed on: 28 February 2024

Transcena (2011). Metodologie cadru privind prevenirea și intervenția în echipă multidisciplinară și în rețea în situațiile de violență asupra copilului și violență în familie. Available at: https://transcena.ro/wp-content/uploads/181010anexa-nr_1-Metodologie.pdf. Accessed on: February 23, 2024

World Vision Romania (2023) - Ziua Siguranței pe Internet. SONDAJ: Peste o treime dintre adolescenți au fost abordați online de adulți cu mesaje de natură sexuală. Peste 60% primesc mesaje private sau comentarii de la persoane necunoscute. Available at: <https://worldvision.ro/2024/02/06/ziua-sigurantei-pe-internet-sondaj-peste-o-treime-dintre-adolescenti-au-fost-abordati-online-de-adulti-cu-mesaje-de-natura-sexuala-peste-60-primesc-mesaje-private-sau-comentarii-de-la-persoane-necu/> Accessed: February 24, 2024

Ziarul de Cluj (2023) - O profesoară din Cluj, batjocorită pe internet de doi elevi, a primit 30.000 de lei despăgubiri. Available at: <https://ziardecluj.ro/o-profesoara-din-cluj-batjocorita-pe-internet-de-doi-elevi-a-primit-30-000-de-lei-despagubiri/> Accessed on: February 27, 2024

Voluntar European (2023). Available at: <https://voluntareuropean.ro/infractiunile-cibernetice-n-romnia-tipuri-si-sanctiuni-pentru-infractiunile-comise-prin-intermediul-internetului/>. Accessed on: February 12, 2024

SLOVAKIA

[Author: [CPM Centrum Prevencie Mladeze](#)]

SECTION 1: NATIONAL CYBER SECURITY POLICIES

On January 7, 2021, it was approved by the government in the Slovak Republic National cyber security strategy for the years 2021 to 2025 (hereinafter referred to as the "National Strategy"), which anchored the direction of the Slovak Republic (hereinafter referred to as the "SR") in the field of cyber security.

The action plan of the National Cyber Security Strategy for the years 2021 to 2025 (hereinafter referred to as the "Action Plan"), which defines these tasks, determines the responsible entities and also the time horizons for individual tasks.

[STRATEGY OF THE SLOVAK REPUBLIC FOR YOUTH for the years 2021-2028](#) , the goal of which is digital transformation.

Digital Coalition - The National Coalition for Digital Skills and Professions of the Slovak Republic is an initiative with a national scope based on the initiative of the European Commission. Its mission is to improve digital skills in Slovakia.

The Ministry of Education of the Slovak Republic has in its program a section - Cyber and information security - tasks from [the Action Plan for the implementation of the National Cyber Security Strategy for the years 2021-2025](#) tasks associated with this program such as development of the starting points of education in the field of cyber security, etc.

At the moment, Cyber Security in School Curriculum: Cyber security is part of the informatics curriculum for secondary schools, covering topics like Internet security in 5 hours of study during the first year and information technology risks such as malware and cybercrime in the third year.

On April 1, 2018, Act No. 69/2018 Coll. on cyber security was enacted to comply with Directive (EU) 2016/1148, ensuring a high level of security for networks and information systems.

Slovakia established the Competence and Certification Center for Cyber Security in 2020, ranking among the top five EU countries with such a centralised cyber security coordination centre.

In our city, two police departments actively engage in crime prevention:

1. The state police conducts speeches with primary and secondary schools on safe internet practices, albeit without a specific program. These discussions cover basic Internet security.
2. The local police, supported by the city, offers targeted programs for youth aged 14-17, including: "Turn on the brain in the online world": Focuses on preventing hoaxes, fraud, and fake online identities; "That's the law, mate": Educates on criminal liability related to internet use; "Risks of the Internet": An interactive session for students aged 14 to 18 to understand online risks.

The establishment of SK-CERT in 2016 further bolsters proactive, reactive, and educational services, including personal data protection, education support, and cooperation between sectors to address cyber incidents.

SECTION 2: LOCAL CYBER SECURITY INITIATIVES

In accordance with the data protection requirements of the EU, in 2002, an entity supervising **data protection - the Office for the Protection of Personal Data - was established in Slovakia**. This office is an independent

state body that supervises compliance with all Slovak laws regarding data protection and privacy by governmental and non-governmental entities.

As part of increasing cyber and information security in the environment of local self-government in the Slovak Republic, within [the Cyber Security Section](#) of the Ministry of Investments, Regional Development and Informatization of the Slovak Republic, [methodological and working materials were created as practical aids and methodological support in the creation of security documentation.](#)

The relevant information is intended for municipalities and cities. The materials are created for the area of public administration information technology security for minimum security measures of category I, II. and III. in accordance with the provisions of Decree **no. 179/2020 Coll.** , which establishes the method of categorization and the content of security measures of public administration information technologies.

In 2022, the Ministry of Investments, Regional Development and Informatization has already announced the 7th round of the call ["Development of governance and the level of information and cyber security in the sub-sector VS"](#) , within which subjects of state and public administration, higher territorial units, cities and municipalities can apply for a non-refundable financial contribution.

[REGIONAL STRATEGY FOR EDUCATION AND EDUCATION IN SECONDARY SCHOOLS IN THE ŽILINA AUTONOMOUS REGION](#) /hereinafter referred to as ŽSK/ 2023-2027 – a basic document for secondary schools in our region. The area of digitization of education and improving the quality of IT education is one of the national priorities, including lifelong learning.

In Slovakia, there are many educational organisations and programs for informal education of students in the field of cyber security, either online or face-to-face, and even in the form of summer camps, using lectures, workshops and games. The following are very successful in our community:

- ZMUDRI organisation - [How to protect yourself from Internet threats](#)
- Civic association Preventista - [New textbook on cyber security](#) + a new non-profit project intended for primary and secondary school teachers, where from March 6, 2024, they launched an electronic library of worksheets for the topics of information security, cyber security and cybercrime prevention.

Private Banská Bystrica Grammar School has initiated a 3-year cyber security education program, thanks to the guidance and support of the Preventista Civic Association, educating nearly 40 future cyber security professionals.

Additionally, a pilot project called the **"Cybernet Security Excellence Center,"** implemented by a cluster organisation in collaboration with the Central Vocational School of Electrical Engineering, aims to educate secondary vocational school students in cyber security using modern solutions.

SECTION 3: EDUCATIONAL INTEGRATION OF NATIONAL CYBER SECURITY POLICIES

[The program of informatization of education until 2030](#) (hereinafter referred to as the "Program") represents a long-term strategy for the development of the mentioned area in the agenda of the Ministry of Education, Science, Research and Sport of the Slovak Republic (hereinafter referred to as "MŠVVaŠ SR"). The goal of this strategy is to advance the policy of the department in terms of informatization to a higher European standard.

[The Digital Coalition](#) is a successful Slovak project primarily due to the great determination and enthusiasm shown by its participants. The coalition attracted more than 65 members from various sectors and created 218 measurable commitments, including a series of scholarships for international students to study ICT in Slovakia.

[The action plan for solving bullying in schools and school facilities for the years 2022-2023](#) (hereinafter referred to as the "Action Plan") is a material developed on the basis of the Program Statement of the Government of the Slovak Republic (hereinafter referred to as the "SR") for the years 2020-2024, in the field of Human Rights and Civil company. It was developed by the Ministry of Education, Science, Research and Sports of the Slovak Republic.

[Directive no. 36/2018 on the prevention and solution of bullying of children and pupils in schools and school facilities](#) - issued by the Ministry of Education, Science, Research and Sport of the Slovak Republic defines bullying as intentional behaviour aimed at harming, threatening, or intimidating another pupil, or repeated attacks against a pupil or group unable to defend themselves effectively. It emphasises the intention to cause physical or mental harm, the aggression of the perpetrator(s), and their perceived superiority over the victim(s).

[Prevention and solution of bullying and cyberbullying of pupils in elementary school documents](#) - measures to prevent the occurrence and spread of bullying are most often school rules, elaborated into specific points in which the requirements for the behaviour of pupils during lessons and during breaks are set and the manifestations of behaviour that students are not allowed.

The implementation of measures aimed at preventing and solving cyberbullying in the educational environment in Slovakia includes a combination of legislative and educational initiatives. Here are some steps and measures that are part of the efforts to manage cyberbullying in the Slovak educational environment:

- Implementation of educational programs on cyberbullying for pupils, teachers and parents through [the Guide to the 2023/2024 school year](#)
- Development and implementation of school protocols for dealing with cases of cyberbullying, including clear procedures for teachers, school staff and students.
- Efforts to create a safe and inclusive learning environment where there is zero tolerance for cyberbullying and other forms of abuse.
- The establishment of online tools or a platform where students can anonymously report cases of cyberbullying and where support is provided for victims using, for example, the www.stalosato.sk platform, an online counselling centre for young people <https://ipcko.sk/>, or a youth prevention centre <https://cpmcdca-sk.webnode.sk/> and others.
- Ensuring access to psychological support for victims of cyberbullying and their families, including the possibility of consultations and therapy through Prevention Centers <https://www.camip.sk/>.

SECTION 4: EDUCATIONAL APPROACHES FOR CYBER RESILIENCE

According to our [online survey](#), in which 77 students from the Secondary Vocational School of Services in Čadca participated, 58.5% of students participated in workshops or meetings at your school focused on online safety and responsible digital behaviour. Up to 68.9% of pupils are aware of the support mechanisms available at school to help students who face incidents of cyberbullying or online problems.

Activities for pupils about cyber security can help raise awareness, strengthen cyber literacy and teach them important skills around the safe use of digital technology. Activities they use at this high school:

- workshops with experts on online safety and safe behaviour online ,
- presentations and games on the topic of phishing - practical activities, such as presentations and games, that help students recognize phishing attempts and fraud online.
- simulations of cyber-attacks, where students can observe and solve fictitious situations within the educational process,

- talks - organising talks with experts on ethical issues related to cyber security, including topics such as privacy rights, ethical hacking practices, responsible behaviour online, etc.
- competitions on cyber security - Involvement of pupils in competitions in the field of cyber security, where they can use their knowledge and skills to solve specific tasks or scenarios,
- information campaigns - creation of information materials and posters about cyber security, which can be placed in school premises and serve as a source of information for students.

Schools in our district use the following programs:

- [Turn on the brain in the online world](#) - focuses on improving the digital competences and skills of young people aged 13 to 18 in processing media and online content in order to eliminate the spread of hoaxes , misinformation, radicalization and violence. More information is in <https://cpmca-dca-sk.webnode.sk/> or <https://turnbrain.eu/our-learning-activities/>
- [Digital security activities contains a list of activities designed by ESET experts](#) , computer science teachers and child psychologists, which illustrate problems in the field of digital security and safe use of the Internet by children in an interesting and practical way . The Activities publication for the Digital Security Handbook is a companion material to the Digital Security Handbook, which we recommend the reader to read before applying the practical exercises and then use the two publications together. The latest versions of both materials can be found at www.bezpecnenanete.sk
- Cyber Fundamentals (ages 10-14) – a comprehensive exploration of cyber security concepts, from malware to ethics. Students will become familiar with network components and encryption techniques. Make the world of cybersecurity tangible and relatable in [Network Heroes](#) & [The Interceptors](#) , from malware secrets to layered security tests! Explore [the Cloud Champions](#) cyber careers and ethics in securing a school network as part of an incident response team.
- Cyber Expert (ages 13-18) -go deeper into advanced topics like encryption and social engineering. Witness the effects of malware and learn techniques to combat it. [Cryptic Ciphers](#) & [Daring Defense](#) covers encryption, decryption and message integrity – it's not just about warding off attacks, it's about understanding why and how. In [Malware](#) Protect yourself from the digital chaos caused by malware [with Mayhem](#) .

Teachers mainly use online trainings intended for all school teachers and youth workers, for example:

- [offers of refresher training and various workshops Regional teacher support center Kysúc](#)
- [Become Heroes of the Internet!](#) By the end of 2023, the number of teachers involved in education under this initiative exceeded 1,700.
- practical tips on digital security that are based on the experience and knowledge of our renowned experts. An important part is also [the Handbook on digital safety for teachers](#) of grades 1 and 2 and practical exercises, which can be found in the Downloadable materials section.
- [EDULAB](#) academy-training of teachers in the online environment. EDULAB is an official provider of innovative education based on authorization issued by the Ministry of Education of the Slovak Republic.

The second most common obstacle to eliminating bullying is problematic communication with parents of aggressors and the ineffectiveness of educational work with aggressors. Some parents do not believe that their child can be a bully, or refuse to cooperate in dealing with bullying, or bullies do not admit their wrongdoing.

SECTION 5: DIGITAL LEARNING PLATFORMS

In connection with the designation [of the National Security Office](#) (hereinafter referred to as the "office") as the central body of the state administration for cyber security as of January 1, 2016, the office established the National Unit SK-CERT. (Slovak Computer Emergency Response Team) and from September 1, 2019 transformed it into [the National Cyber Security Center SK-CERT](#). The department ensures national and strategic activities in the field of cyber security management, in the area of threat analysis, but also coordination of the solution of cyber security incidents at the national level, teaching , training, as well as research.

On April 1, 2018, Act No. 69/2018 Coll. on cyber security and on the amendment of some laws, which defines roles, rights and obligations in the field of cyber security. At the same time, this law determines the position of the National Security Office and the National Cyber Security Center SK-CERT.

As the National CSIRT unit SK-CERT fulfils various tasks within the framework of the law in the Slovak cyber space, as well as solves cyber security incidents, announces alerts and warnings against a serious cyber security incident, imposes the obligation to take reactive measures and approves protective measures, sends timely warnings, receives domestic reports on cyber security incidents, receives reports on cyber security incidents from abroad and ensures cooperation with international organisations and authorities of other states in dealing with cyber security incidents of a cross-border nature, etc.

The Ministry of Investments, Regional Development and Informatization of the Slovak Republic has issued [Defining technical and procedural tools and procedures for meeting the security minimum](#) . This document is a methodological material serving the needs of public authorities, which is not mandatory for use and is not binding. The document is provided freely and free of charge for use according to the needs of a specific organisation. The created document can also be used for the needs of training employees of organisations in the field of cyber and information security.

[Guidelines of the Ministry of Education, Science, Research and Sports of the Slovak Republic in connection with the employment of a teaching staff with the job title of school digital coordinator](#)

[Guidance for teachers and educators on combating misinformation and promoting digital literacy through education and training. We announced these guidelines in September 2020 as part of the Digital Education Action Plan \(2021-2027\)](#)

[Discover the digital potential of your school](#) - In this document you will find all the statements and questions of cyber communication settings that are currently in the SELFIE tool for each level of education (for example, first or second grade of elementary school).

SECTION 6: LOCAL CYBER THREAT TRENDS

According to our [online survey](#) , in which 77 students from the Secondary Vocational School of Services in Čadec participated, the students were most affected by the following cyber threats:

- **False identities - 44.2% of respondents**
- **Online hoaxes - 40.3% of respondents**
- **Cyberbullying - 40.3% of respondents**
- **Sexting - 40.3% of respondents**
- Trolling 33.8% of respondents
- Excessive gaming by 33.8% of respondents

- Morphing 31.2% of respondents
- Ban 24.7% of respondents
- Gambling 22.1% of respondents
- Doxing 19.5% of respondents

According to Maj. Mgr. František Linet , the head of the local police, and according to the statistics of the Čadca Municipal Police, online frauds against young people and physical injuries have increased. We dealt with cyberbullying 6 times in 2023, but it is always dealt with within the school, so not a single complaint about the commission of a crime was filed in our city.

According to statistical data from 2022 /since 2023 has not yet been processed/ the most frequent types of technical cyber-attacks registered at police departments in the Slovak Republic were:

- obtaining information through phishing campaigns and social engineering,
- fraudulent phone calls known as " voice phishing " or " vishing ",
- denial-of-service attacks (known as " DDoS ") aimed at making various websites and services unavailable,
- mailing
- phishing campaigns using the identity of postal and delivery services, banks or law enforcement authorities (PZ, Interpol , Europol),
- ransomware continued to dominate the spread of malicious code.

According to statistics, crime committed by youth between the ages of 14 and 18 can be divided into violent, property and moral crime. According to [statistics published by the Ministry of the Interior of the Slovak Republic, there were 21 crimes in the Žilina Region in 2022](#) for violent crime , which includes violent crimes such as intentional bodily harm, dangerous threats, kidnapping, coercion, abuse, and property crime represented 15 crimes in our region. although there were up to 120 frauds in total, violent crime represented 21 acts and moral crimes 20 acts.

In addressing socio-pathological phenomena, the associate partner identifies bullying and unwanted online content as significant challenges. Bullying persists both in physical and virtual environments, with students facing mockery, threats, and verbal abuse, often leading to school avoidance behaviours. To tackle these issues, there's a renewed focus on fostering a positive socio-cultural climate within the organisation. This includes promoting mutual respect, moral values, and active preventive programs targeting discrimination and intolerance. Police highlight increasing cyber threats such as phishing, fraud, and DDoS attacks. Schools report cyberbullying, false identities, hoaxes, and other online issues. Victims seek support from various institutions, including the police and dedicated help centres.

SECTION 7: COMMUNITY ENGAGEMENT

Reporting system and network of partner support for dealing with cyber threats in Slovakia, involving multiple organisations, institutions and sectors. The main actors in such a system are:

1. Schools - in most cases, schools have specific rules for submitting pupils' suggestions on cyber threats within the school rules. The student has the opportunity to file a complaint directly at the school through the school's mailbox, and the complaint is then dealt with by authorised people. Another option if the incident is not resolved is the police.
2. Slovak Police - cyber department, where mostly victims of crimes, whether social or technical type of cyber attack, turn to.

3. CERT.SK (National Computer Security Team) - through the uniform information system of cyber security, regardless of the categorization of the cyber security incident, **voluntary incident reports are also carried out.** - [Form for reporting cyber security incidents](#)
4. The National Security Bureau (NBU) is the body responsible for providing analysis and information related to cyber security. Reporting of cyber security incidents is carried out through [a unified cyber security information system](#). The office can also conclude a written contract with the operator of the basic service or the provider of the digital service on the method and form of reporting cyber security incidents.

The Secondary Vocational School of Services in Čadec ensures community awareness with the help of various initiatives and measures. Here are some of the ways it uses:

- *Educational Programs and Workshops:* Organising informative sessions for students, parents, and teachers on digital security, covering cyber threats, safe online behaviour, and privacy.
- *Safe Internet Day at School:* Developing and distributing educational materials and brochures to students and parents, offering clear guidance on digital safety.
- *Integration into School Curriculum:* Embedding digital security topics into school curricula and educational programs to ensure students learn about safe digital practices as part of their studies.
- *Collaboration with Experts:* Partnering with cyber security specialists, including law enforcement and security companies, to provide updated information and best practices in digital security.
- *Establishing a Secure Environment:* Working with IT professionals to create and maintain a secure school environment, implementing technical measures to safeguard the school's network and equipment.

The local police organise educational talks at schools, where they focus mainly on criminal liability in digital security, show students how easily they can become a perpetrator of a crime, etc.

In the 2022/2023 school year, the local police launched the volunteer project YE - Stop Bullying for 2nd grade elementary school students. Four young and ambitious students, as well as active members of the Čadca City Police youth club, were trained for free and are actively involved in peer -to- peer prevention among young people by organizing various leisure activities focused on digital security.

SECTION 8: MAYOR'S CYBER RESILIENCE CHALLENGES

Students between the ages of 14 and 17 face multiple digital safety challenges that can impact their online safety and awareness. The main challenges include:

- Cyberbullying and online abuse
- Privacy
- Misinformation, trolling
- Sexual harassment
- Cyber security threats and fraud
- Online addiction and harmful content
- Social engineering and manipulation

Addressing these challenges requires a comprehensive approach that includes education, support from schools, parents and the public, as well as the development of cyber literacy and critical thinking.

Schools face various cyber threats that can affect not only the security of their computer systems, but also the safety and privacy of students. Some of the most common cyber threats to schools include:

- Phishing

- Malware
- Cyberbullying
- Insufficient protection of personal data
- Abuse of online education - the risk of abuse of this resource, for example unethical behaviour during online classes or copying and distribution of content.

Common cyber threats faced by the police include:

- Phishing
- Malware
- Ransomware
- Cyberbullying and online crime
- Social engineering

Identified youth cyber safety challenges pose various risks for children and young people, including:

- Cyberbullying, leading to emotional stress and mental health issues.
- Loss of privacy and identity theft due to inadequate protection of personal data.
- Low cyber literacy, making them vulnerable to security threats like phishing and malware.
- Negative impact on digital reputation and career prospects from reckless online behaviour.
- Exposure to harmful content such as violence and hate speech.
- Risk of online addiction and associated physical health problems.
- Vulnerability to social engineering and fraudulent practices.

SECTION 9: FUTURE EXPECTATIONS

According to our youth survey, young people point to the following improvements:

1. **Insufficient support from the school when dealing with digital security issues** , including incidents related to cyberbullying or online threats, where 53.3% of pupils reported little to medium support from the school + **70.2% of pupils said they did not know or knew only slightly support mechanisms** available at the school **to help students who are facing incidents of cyberbullying** or other online problems.
2. **Inadequate education** at school focused on online safety and responsible digital behaviour, where up to 74.1% of students reported no or only little educational opportunities + 49.4% of students do not have education about the consequences of cyber threats and the importance of critical use of the Internet.
3. **Uninteresting education** - 65% of students consider **cyber security education at your school to be uninteresting**, without interactive methods or real-life scenarios.
4. **Improving their emotions and tolerance** at school - up to 71.5% of pupils perceive significant negative emotions online bullying or various cybercrimes.
5. **Improving self-confidence in recognizing and avoiding potential online threats** - up to 63.1% of pupils feel little or moderately confident in recognizing and avoiding potential online threats, such as phishing attempts, fraud or fraudulent activities.

Improvements required as reported by local/national policy department.

- More preventive activities aimed at cyber threats.
- Improvement of personnel policy to significantly increase prevention actors in the economic plan of the city of Čadca for the next few years.
- More creative and volunteer activities focused on cyber threats.
- Connecting all relevant local government actors to improve the education of youth in the field of cyber security.

Improving youth cybersecurity education requires a comprehensive approach that includes not only formal education within schools, but also cooperation between schools, parents and other relevant entities. Here are recommendations from our school:

- Improve sufficient education for educators to be helpful to students in cyber security.
- Practical exercises and simulations.
- Cooperation with cyber security specialists - specialists who can provide expert advice.
- Creating information campaigns.
- Develop ethical digital behaviour at school

Other possible approaches to this issue:

- **Integrating cyber security into the school curriculum** - it is important to integrate cyber security topics directly into school curricula and learning plans. In this way, systematic preparation of students for digital security is provided.
- **Working with the technology sector and cyber security experts** to ensure that education is up-to-date and focused on real threats in the digital world.
- **More competitions for pupils in the field of cyber security** can motivate students to be interested in this field and improve their skills. Various countries organise national and international cyber security competitions for students.
- **Parent education** - involving parents in schools' educational initiatives is important for overall success. Parents are key partners in supporting children's safe digital behaviour.
- **Use of new educational technologies to increase attractiveness** - In some cases, educational programs use modern technologies, including interactive applications, simulations and online education.

SECTION 10: CONCLUSIONS

Common cyber threats faced by the police include: 1. Phishing, 2. Malware, 3. Ransomware, 4. Cyberbullying and online crime, 5. social engineering

Suggestions for improvements according to reports from the department of local/national policy in the area of prevention of pupils' cyber literacy: more preventive activities aimed at cyber threats; improvement of personnel policy to significantly increase prevention actors in the economic plan of the city of Čadca for the next few years; more creative and volunteer activities focused on cyber threats; connecting all relevant local government actors to improve the education of youth in the field of cyber security.

Some of the most common cyber threats to schools include: 1. Phishing, 2. Malware, 3. Cyberbullying, 4. Insufficient protection of personal data, 5. Abuse of online education.

According to our [online survey](#), students from the Secondary Vocational School of Services in Čadec were most affected by the following cyber threats: 1. False identities, 2. Online hoaxes, 3. Cyberbullying, 4. Sexting.

Youth highlights the following improvements in cybersecurity education:

1. Insufficient support from the school in solving digital security problems.
2. Inadequate education.
3. Uninteresting education.
4. Improving their emotions and tolerance.
5. Improving self-confidence in recognizing and avoiding potential online.

Slovakia: Bibliography

Cluster Kybernetickej Bezpečnosti. (16. 1 2024). Projekt "Cluster Kybernetickej Bezpečnosti". Dostupné na Internete: <https://clusterkb.sk/sk/aktuality#s0>

Čadca, M. p. (8. 3 2024). *Štatistiky*. Dostupné na Internete: <http://www.policia.mestocadca.sk/cinnost/statistiky.html>

Digitálna koalícia. (28. 3 2023). *Digitálna koalícia.sk*. Dostupné na Internete: <https://digitalnakoalicia.sk/good-practice/s-odbornikom-o-cybersecurity-prednasky-pre-stredne-skoly/>

GLOBSEC. (3. 2 2024). *www.globsec.org*. Dostupné na Internete: HYBRIDNÉ HROZBY NA SLOVENSKU: <https://www.globsec.org/sites/default/files/2019-06/Hybridne-hrozby-na-Slovensku-Kyberneticka-bezpecnost.pdf>

Gymnázium Ľudovíta Štúra Trenčín. (17. 1 2024). *Gymnázium Ľudovíta Štúra v Trenčíne Učebné osnovy*. Dostupné na Internete: https://www.gymnaziumtrenacin.sk/buxus/docs/dokumenty/Ucebne_osnovy/Informatika/Informatika_790_2J-inf.pdf

Minecraft education. (2 2024). *CYBER & DIGITAL CITIZENSHIP- TEACH CYBERSECURITY WITH MINECRAFT*. Dostupné na Internete: <https://education.minecraft.net/en-us/discover/cyber-and-digital-safety>

Ministerstva investícií, regionálneho rozvoja a informatizácie SR. (23. 9 2022). *MIRRI SR pomáha inštitúciám štátnej správy a samosprávy v rozvoji informačnej a kybernetickej bezpečnosti, uzatvorilo výzvu za 10 miliónov eur*. Dostupné na Internete: <https://mirri.gov.sk/aktuality/csirt/mirri-sr-pomaha-instituciam-statnej-spravy-a-samospravy-v-rozvoji-informacnej-a-kybernetecki-bezpecnosti-uzatvorilo-vyzvu-za-10-million-euro/>

Ministerstvo školstva SR. (2018). *Smernica č. 36/2018*. Dostupné na Internete: <https://www.minedu.sk/data/att/16073.pdf>

Ministerstvo školstva SR. (9 2021). *AKČNÝ PLÁN RIEŠENIA ŠIKANOVANIA V ŠKOLÁCH*. Dostupné na Internete: <https://www.minedu.sk/data/att/21853.pdf>

Ministerstvo školstva SR. (2 2024). *PROGRAM INFORMATIZÁCIE ŠKOLSTVA DO ROKU 2030*. Dostupné na Internete: <https://www.minedu.sk/data/att/23246.pdf>

Ministry of Education, Research, Development and Youth is a governmente Minister of the Education Tomáš Drucker. (25. 10 2023). Dostupné na Internete: Stratégia Slovenskej republiky pre mládež na roky 2021 – 2028: https://www.minedu.sk/data/files/11043_strategia-slovenskej-republiky-pre-mladez-na-roky-2021-2028.pdf?fbclid=IwAR2fNDFyc8qFteAHJvODJoiV3ndEPSAss0oW8-ds1dWdSz4tcA2wOKpgN6U

Regionálne centrum podpory učiteľov. (16. 1 2024). *Vzdelávanie a workshopy*. Dostupné na Internete: <https://www.rcpukysuce.sk/home/aktualiza%C4%8Dn%C3%A9-vzdel%C3%A1vanie-a-workshopy>

Slovenské národné stredisko pre ľudské práva. (02 2019). *Metodické východiská modelu prevencie násilia a šikanovania v školách*. Dostupné na Internete: <https://www.minedu.sk/data/att/13481.pdf>

SR, M. v. (2 2024). *Štatistika kriminality v Slovenskej republike za rok 2022*. Dostupné na Internete: https://www.minv.sk/?statistika_kriminality_v_SR_za_rok_2022_xml

SR, Ú. v. (2 2024). *Správa o bezpečnosti Slovenskej republiky za rok 2022*. Dostupné na Internete: https://www.vlada.gov.sk/share/uvsr/br-sr/sprava_o_bezpecnosti_sr_2022.pdf

SR, Z. m. (23. 3 2022). *KYBERNETICKÁ BEZPEČNOSŤ - Informácia pre starostov a primátorov*. Dostupné na Internete: <https://www.zmos.sk/kyberneticka-bezpecnost-informacia-pre-starostov-a-primatorov--oznam/mid/414056/.html>

úrad, N. b. (17. 2 2024). *Hlásenie kybernetických bezpečnostných incidentov*. Dostupné na Internete: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/hlasenie-kybernetickych-bezpecnostnych-incidentov/index.html>

Výskumný ústav detskej psychológie a patopsychológie (VÚDPaP) . (11. 9 2023). *vudpap.sk*. Dostupné na Internete: <https://vudpap.sk/wp-content/uploads/2023/09/manual-zacinajuceho-skolskeho-psychologa.pdf>

zmudri.sk. (27. 2 2024). *Séria: Ako sa chrániť na internete*. Dostupné na Internete: <https://zmudri.sk/seria/seria-digi-bezpecnost>

SWOT Analysis

This SWOT analysis highlights the multi-faceted approach pointing out the strengths and areas for improvement in integrating cybersecurity into broader societal frameworks. The analysis also outlines the opportunities for growth and potential threats that could impact the effectiveness of the national project efforts.

Strengths:

- **Comprehensive Legislation:** Each country has developed robust cybersecurity laws and frameworks that align with EU directives, ensuring a high standard of cybersecurity measures and compliance across the board.
- **Educational Integration:** There is a strong emphasis on integrating cybersecurity education into school curricula, helping to raise awareness and prepare the next generation to handle cyber threats effectively.
- **National Cybersecurity Authorities:** The establishment of dedicated cybersecurity agencies or directorates in countries like Italy and Greece centralizes efforts, enhances coordination, and provides clear leadership in national cybersecurity strategies.
- **Public-Private Partnerships:** Effective collaborations between government bodies, educational institutions, and private sectors enhance resource sharing, innovation, and the practical implementation of cybersecurity measures.

Weaknesses:

- **Inconsistent Parental Engagement:** Although educational programs are robust, there is a recurring challenge in actively engaging parents and guardians in cybersecurity education, which is crucial for reinforcing safe online practices at home.
- **Resource Distribution:** Some reports indicate discrepancies in the distribution of resources for cybersecurity initiatives, particularly in less developed regions or rural areas, potentially leaving parts of the population less protected.
- **Lack of standardisation in School Programs:** While cybersecurity is integrated into national education systems, the depth and breadth of these programs can vary significantly, affecting the overall effectiveness of these educational efforts.

Opportunities:

- **Expansion of Cybersecurity Education:** There is significant potential to expand cybersecurity education beyond the classroom, incorporating more community-based programs that reach a broader audience, including parents and elderly citizens.
- **Advancements in Technology:** Leveraging new technologies and innovations can enhance cybersecurity measures and educational tools, providing more interactive and engaging ways to educate and protect citizens.
- **EU Funding and Support:** Utilizing EU funds and programs can help bolster national efforts, particularly in developing comprehensive digital education programs and upgrading cybersecurity infrastructure.

Threats:

- **Evolving Cyber Threats:** Cyber threats are continuously evolving in complexity, requiring constant updates to both technological defences and educational content, which can be resource-intensive.
- **Compliance with Evolving EU Regulations:** Staying compliant with continuously updating EU cybersecurity regulations demands ongoing adjustments to national laws and practices, which can be challenging.



- **Digital Divide:** A significant digital divide between different regions and demographics can hinder the effective implementation of cybersecurity strategies and educational programs, potentially leaving vulnerable groups at greater risk.



Conclusions

The analysis conducted in the CYBER project brings to light the pressing need to address cyber threats and enhance digital safety, especially among the youth across participating EU countries. The insights reveal several pervasive challenges:

Deficiencies in Digital Literacy Education: There is a notable gap in digital literacy education across schools. This gap underscores the necessity of embedding robust digital literacy modules within school curricula to equip students with essential skills for safe online navigation.

Insufficient Support Structures: Current support structures for dealing with cyber threats, such as cyberbullying, are often inadequate. This insufficiency highlights the importance of developing comprehensive support mechanisms that can provide immediate and effective assistance to affected youths.

Prevalence of Cyber Threats: The persistent prevalence of cyber threats reinforces the need for ongoing vigilance and updated strategies to safeguard young users in the digital realm.

To comprehensively tackle these challenges, the partnership proposes several strategic actions:

- **Integrating Cyber Safety Education:** Schools must incorporate cyber safety into their educational programs systematically. This integration will enable students to develop critical digital literacy skills necessary for navigating the online world securely.
- **Parental Engagement:** Engaging parents as proactive partners in cyber safety is crucial. Parents need to be equipped with the knowledge and tools to effectively guide their children's online activities and recognize potential risks, thereby creating a more robust support network.
- **Strengthening Collaboration:** Enhancing cooperation between educational institutions, law enforcement, and other relevant stakeholders is essential. Coordinated efforts, such as joint awareness campaigns and shared information initiatives, can foster a more unified approach to cybersecurity.
- **Community Engagement Strategies:** Implementing centralised reporting systems along with community-driven initiatives can provide valuable insights and best practices. These strategies are crucial for fostering a proactive community environment where cybersecurity awareness is heightened.
- **Decentralized Efforts at the National Level:** Schools, NGOs, and community organizations should lead decentralized efforts to enhance support mechanisms. These efforts often involve dedicated platforms and confidential channels that are pivotal in supporting affected individuals.
- **Educational Workshops:** Cybersecurity experts and psychologists should conduct workshops to educate children about online risks and safe internet usage practices.
- **Promotion of Official Reporting Channels:** Awareness about official channels for incident reporting and the development of peer-to-peer support networks within schools are essential for empowering youth to manage their digital interactions safely.
- **Global Collaboration:** Strengthening ties with law enforcement, governmental bodies, and international organizations can enhance community engagement efforts significantly. This global network facilitates the exchange of resources and best practices, essential for building a safer online environment.



Conscious Youth Behaviours in Emerging Realities

Erasmus+ KA2 Cooperation Partnerships in School Education

[Reference n. 2023-1-EL01-KA220-SCH-000156982]



**Co-funded by
the European Union**

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.