


Author: Ioanna Athinodorou



**Youth online behavior,
risks and avenues for
mitigating them**

National report: Cyprus



Co-funded by
the European Union



Project Title: **Action-Based Approach in Addressing and Mitigating Risks of Young People in Online Social Networks**

Agreement Number: **2021-1-R001-KA220-YOU-000028688**

EU Programme: **KA2 – Cooperation partnerships in youth**



This document has been produced with the financial support of the 'ERASMUS+ KA220-YOU - Cooperation partnerships in youth' programme of the European Union. The content represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Table of contents

I.	INTRODUCTION	2
II.	METHODOLOGY	3
III.	LITERATURE REVIEW	4
	NATIONAL CONTEXT: CYPRUS.....	10
	PUBLIC INSTITUTIONS RESPONSIBLE FOR ADDRESSING THE MANIFESTATION OF THE RISKS.....	11
	EU AND INTERNATIONAL CONTEXT	14
IV.	MAIN FINDINGS OF THE RESEARCH	15
	MAIN PATTERNS OF MANIFESTATION OF THE RISKS IN CYPRUS (RISK INDICATORS).....	15
V.	CONCLUSIONS AND RECOMMENDATIONS	26
	CONCLUSIONS.....	26
	TRAINING NEEDS IN RESPONSE TO FAKE NEWS AND DISINFORMATION.....	27
	RECOMMENDATIONS FOR DESIGN, CONTENT AND PROMOTION OF THE GAME	29
	BIBLIOGRAPHY	31

I. INTRODUCTION

The aim of this report is to provide for data and information on the youth online risks in Cyprus. Specifically, the report examines the risks that young people face in online environments, particularly on social media.

The target groups are young people between the ages of 18-30, who have an online presence on social networks; and Youth Workers and Youth Trainers.

The research questions examined in the course of the RISE report, are the following:

- Which are the main factors making young people vulnerable to risk factors?
- How can a safe online environment for young people be achieved?
- What should be the design and content of an online game combating online fake news and other types of disinformation among youth?

The Cyprus country report consists of five parts. The first part is the introduction, while the second presents the methodology followed throughout the research and reporting. The third part presents the literature review; the fourth part contains the main findings of the research; and the fifth and final part, comprises the conclusion and recommendations.

The report offers an innovative multi-layered methodology that will support youth and youth workers, not only to identify the risks of social media, but also to minimise those risks. At the same time, it proposes a design of a content strategy to collect and develop the digital content of the RISE Game, while ensuring that it is in accordance with the capacity building programme that will be designed in the framework of the RISE project.

The report looks into socio-demographic factors, social media use, risk perceptions, preventive behaviors, attitudes and other relevant factors in the context of the COVID-19 pandemic; and reveals the link between youth's offline-online vulnerability, risky behaviors online and consequences and impact of social media.

The analysis introduces data on social media use, cybercrimes targeting youth, and measures the critical thinking skills of young people. Regarding the professionals and experts, the analysis covers their profile and their areas of expertise while examining youth online behavior, and making recommendations.

The use of both the target groups in the report, focuses on producing a comprehensive, multi-perspective and robust framework of needs and support structures for the future for youth, that will also serve as a compass for professionals and policy makers.

The interviews of professionals and experts aimed at eliciting expert opinions about how the situation in Cyprus is on the online behavior of young people, the level of media use and critical thinking, and the challenges and needs, while proposing training needs to avoid or deter these risks.

The RISE report is the first project result of the RISE project “Action-Based Approach in Addressing and Mitigating Risks of Young People in Online Social Networks” funded by the Erasmus+ programme of the European Union, and project number 2021-1-RO01-KA220-YOU-000028688.

II. METHODOLOGY

SECONDARY RESEARCH

The aim of this report is to provide for data and information on the online behavior of young people in Cyprus. The research under this theme focused on documenting the subject, examining the term “social media” and the risks associated with youth and social media, while it studies the Cyprus context and EU and international framework.

The desk research ran from May to October 2022, and reviewed existing research on youth risks associated with social media, and its objective is to identify the state of play and legal framework in Cyprus. The objective of the desk research is to assess the contents of qualitative research results for future publication, and to provide data to other Project Results (PRs) of the project RISE.

The desk research is done in a keyword led search via online resources, online libraries, government websites, professional networks, and internet keywords, in Greek and English, such as:

- Social Media and youth
- Data on youth and social media
- EU policies on social media and internet
- International documents on youth
- Youth risks in Cyprus
- Social Networks
- Youth social media risks

PRIMARY RESEARCH

Regarding the collection of data for the primary research, and specifically for the questionnaire for young people, the partners’ consortium initiated the creation of a sample draft. The leading partner, CLNR, provided the consortium partners with a sampling technique, which would be used in order to make the sample more representative in each partner country, and a coding scheme.

Accordingly, SYNTHESIS invited young people aged 16 - 30, and living in Cyprus, to participate in the questionnaire, in an open call. SYNTHESIS also used personal contacts and contacts collected from youth organizations, to reach the specific number of replies on time. The questionnaire was open for responses from September to October 2022, when all 40 responses were collected. It

was an online questionnaire developed by the consortium, and transferred into an online form by SYNTHESIS, for Cyprus.

The experts and professionals for the interviews were selected upon their knowledge and experience on youth in general, youth risks, digital environments, etc., in the Cyprus context. Four experts were invited and took part in the interview.

The analysis of the data obtained from these sources will be performed through a process of triangulation. The desk research, along with the data collected through the survey and one-to-one interviews, contribute to the documentation of the problem and to the collection of the necessary data for creating the content of the Game and the Capacity Building Programme foreseen in the project.

The analysis of the collected data establishes a set of risk factors in young people, as well as strategies and good practices in addressing the threat of Cyberbullying, Online harassment, Exposure to sexually explicit material / sexting, Alienation from the real world, Grooming, Misinformation / Fake news, Breach of privacy, Identity theft, Revenge porn, Addiction, Mental health issues among youth. It also results in methods of identifying fake news and disinformation and building resilience strategies, through increased media literacy, critical thinking, civic consciousness, fake news resilience and responsible behavior. Also, the goal is to formulate recommendations for combating these risks, through trainings and an online game.

III. LITERATURE REVIEW

The internet has become a huge part of our lives, especially after the COVID-19 pandemic breakout; and has significantly transformed many different fields. It has become a global means of communication in our everyday lives and at the same time, a primary source of information. With the help of the internet, people can make calls and video calls, send messages and work anytime from and to any place in the world.

The term “Social Media” is hard to define. Some early researchers referred social media as social networks or social networking services in the mid-2000s. According to research, “social media” is a media which is initially used to transmit or share information with a broad audience, while social networking is an act of engagement as people with common interests associate together and build relationships through community. Social networking is a two-way communication, where conversations are at the core, and through which relationships are developed¹. Social

¹ Edosomwan, Simeon & Prakasan, S.K. & Kouame, D. & Watson, J. & Seymour, T.. (2011). The history of social media and its impact on business. *Journal of Applied Management and Entrepreneurship*. 16. 79-91.

media means any website that allows for social interaction and the exchange of ideas². A few networking sites which were invented in the 1990s included Six 6 Degrees, Black Planet, Asian Avenue, and Move On, while blogging services included Blogger and Epinions. In 2001, fotolog, sky blog and Friendster, were created, and in 2003, MySpace and LinkedIn were created and launched. In 2004, popular sites such as Facebook, Dogster and Mixi appeared; and in 2005, Yahoo!360 and YouTube³.

Nowadays, the most popular social networking websites for young people include Facebook, Twitter, Instagram, LinkedIn, and TikTok. There are many reasons why young people love to use social media. Some of the reasons, include the following:

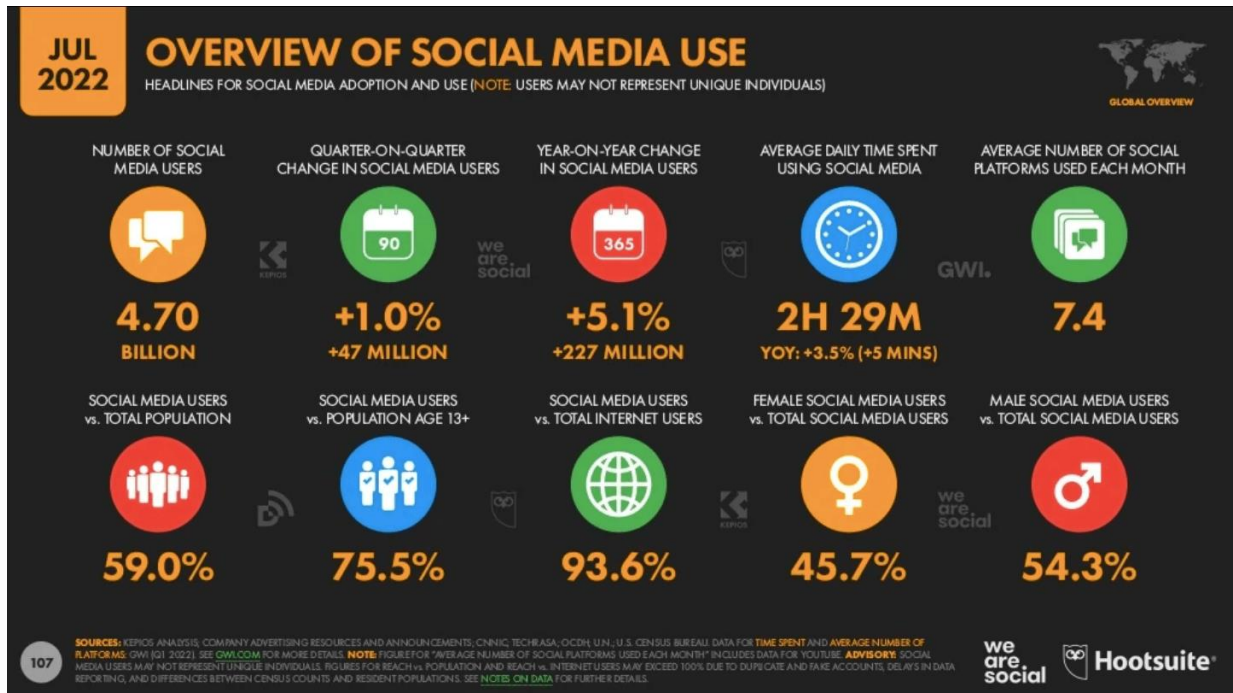
- Easy and free access to information and education
- Build their identities
- Have a sense of belonging and building their self esteem
- Develop and maintain supportive relationships

Simultaneously, the use of social media and networking websites such as Facebook, Twitter, Instagram, and TikTok has become a daily habit, illustrated by people checking their accounts on social media very often during the day. More specifically, according to recent research by Global WebIndex, 59 percent of the world uses social media, while the average daily time spent using social media is 2 hours and 29 minutes⁴.

² Clinical Report--The Impact of Social Media on Children, Adolescents, and Families Gwenn Schurgin O'Keeffe, Kathleen Clarke-Pearson and COUNCIL ON COMMUNICATIONS AND MEDIA Pediatrics; originally published online March 28, 2011; DOI: 10.1542/peds.2011-0054 <https://research.fit.edu/media/site-specific/researchfitedu/coast-climate-adaptation-library/climate-communications/youth-climate-amp-social-media/O'Keeffe--Pearson.-2011.-Impact-of-Social-Media-on-Children,-Adolescents,-and-Families..pdf>

³ Edosomwan, Simeon & Prakasan, S.K. & Kouame, D. & Watson, J. & Seymour, T.. (2011). The history of social media and its impact on business. Journal of Applied Management and Entrepreneurship. 16. 79-91.

⁴ DataPortal: Digital 2022: July Global statshot report : <https://datareportal.com/reports/digital-2022-july-global-statshot>



These digital environments also offer space for communication. 88 percent of Internet users (aged 18-24) in Europe are active/present in social media⁵.

In Cyprus, young people appear to be addicted to their smartphones and to social media⁶. It was found that, 88 percent of online users are Facebook members, which puts Cyprus at the top of the list in all of Europe⁷. Cyprus ranked third highest among EU member states in terms of percentage of people aged 16 to 74 with an active social media account, in 2020. Around 78 percent of people interviewed in Cyprus confirmed they use social media regularly, whereas the average figure in the EU stands at 57 percent⁸.

More recent research has shown that the prevalence of social media and internet use among youth in Cyprus are a cause for concern and that this fact poses a real problem for public health⁹. At the same time, social media use has also been linked with depression, suicide and self-harm, particularly in girls and marginalised groups¹⁰. These types of concerns can take the form of social

⁵ Eurostat 2016.

https://ec.europa.eu/eurostat/statisticsexplained/index.php?title=Archive:Internet_access_and_use_statistics_-_households_and_individuals

⁶ <https://www.goldnews.com.cy/en/economy/teenagers-in-cyprus-addicted-to-multimedia-devices>

⁷ <https://knews.kathimerini.com.cy/en/news/cypriots-beat-europeans-on-facebook>

⁸ <https://cyprus-mail.com/2021/07/01/cyprus-in-eu-top-three-for-social-media-use/>

⁹ Christodoulides, C., Intziegianni, K., Mappourides, A., Antoniou, P. and Hadjifoti, P. (2021). Exploring the relationship of young people in Cyprus with the Social Media and the Internet. Alexander College-Alexander Research Centre

¹⁰ Kelly Y, Zilanawala A, Booker A et al. *EClinicalMedicine* 2019;6:59-68

isolation, disturbed sleep, cyberbullying, pressures to conform to lifestyles and body images, and more.

Overall, accessibility to social media may cause serious problems. Youth can engage in problematic use, which may include talking to strangers online, sharing personal information, etc.

More specifically, the risks associated with youth and social media are the following:

- Cyberbullying
- Online harassment
- Exposure to sexually explicit material / sexting
- Alienation from the real world
- Grooming
- Misinformation / Fake news
- Breach of privacy
- Identity theft
- Revenge porn
- Addiction
- Mental health issues

Cyberbullying occurs when people use technology to embarrass, harass or bully someone. According to UNICEF, cyberbullying is bullying with the use of digital technologies¹¹. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behavior, aimed at scaring, angering or shaming those who are targeted. Examples include:

- Spreading lies about or posting embarrassing photos or videos of someone on social media.
- Sending hurtful, abusive or threatening messages, images or videos via messaging platforms.
- Impersonating someone and sending mean messages to others on their behalf or through fake accounts.

Face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying leaves a digital footprint – a record that can prove useful and provide evidence to help stop the abuse¹². Cyberbullying is very pervasive since malicious messages or rumors can rapidly spread to many people from various locations.

¹¹ UNICEF: Cyberbullying: What it is and how to stop it <https://www.unicef.org/end-violence/how-to-stop-cyberbullying> [Accessed September 2022]

¹² UNICEF: Cyberbullying: What it is and how to stop it <https://www.unicef.org/end-violence/how-to-stop-cyberbullying> [Accessed September 2022]

Cyberbullying is a form of *online harassment*. According to researchers, online harassment can be defined as “threats or other offensive behavior (not sexual solicitation) sent online to the youth or posted online about the youth for others to see”¹³. The most common online environments that online harassment can take place, include social media (66 percent), comments section of a website (22 percent), online gaming (16 percent), personal emails (16 percent), discussion sites (e.g., reddit) (10 percent), dating sites or apps (6 percent)¹⁴.

Exposure to sexually explicit material is another risk that youth face, that causes important concern, especially, since there is evidence that such exposure is related to greater sexual uncertainty and more positive attitudes towards uncommitted sexual exploration among young people¹⁵.

“Sexting”, which includes sending or receiving sexually explicit images or video via a cell phone, is also an associated risk of social media. It relates to risks, as images or videos sent can easily become public or sent to large groups of people online.

Spending too much time on the internet can also create a *sense of isolation and/or alienation from the real world*.

Research shows a lack of understanding of the term *grooming* in online communications and social media. The Cambridge dictionary defines grooming as “the criminal activity of becoming friends with a child, especially over the internet, to try to persuade the child to have a sexual relationship. Online grooming is when someone builds an online relationship with a young person and tricks them or pressures them into doing something sexual¹⁶. Online grooming enables relationships to be built more quickly through regular contact via instant communication techniques, unless the parties know each other.

According to the European Commission, *disinformation* is false or misleading content that is spread with an intention to deceive or secure economic or political gain, and which may cause public harm. *Misinformation* is false or misleading content shared without harmful intent though the effects can be still harmful¹⁷. Therefore, the main difference between the two is the intent. The spread of both disinformation and misinformation can have a range of harmful

¹³ Child Abuse & Neglect 32 (2008) 277–294 Are blogs putting youth at risk for online sexual solicitation or harassment? Kimberly J. Mitchell *, Janis Wolak, David Finkelhor Crimes against Children Research Center, Family Research Lab, University of New Hampshire, Durham, NH, USA Received 6 June 2006; received in revised form 13 April 2007; accepted 13 April 2007

¹⁴ Beyond technology—dealing with people

John Sammons, Michael Cross, in The Basics of Cyber Safety, 2017

¹⁵ Lin WH, Liu CH, Yi CC. Exposure to sexually explicit media in early adolescence is related to risky sexual behavior in emerging adulthood. PLoS One. 2020 Apr 10;15(4):e0230242. doi: 10.1371/journal.pone.0230242. PMID: 32275669; PMCID: PMC7147756.

¹⁶ Wood, A. C., & Wheatcroft, J. M. (2020). Young Adult Perceptions of Internet Communications and the Grooming Concept. SAGE Open, 10(1). <https://doi.org/10.1177/2158244020914573>

¹⁷ European Commission: Tackling online disinformation <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation> [Accessed September 2022]

consequences, such as threatening our democracies, polarising debates, and putting the health, security and environment of EU citizens at risk. Disinformation is directly linked to *fake news*.

At the same time, teens are increasingly sharing personal information on social media, especially while those sites are designed to encourage the sharing of information and the expansion of networks. Incidents of *data breaches* have alarmed many users in the past. Some typical social media threats include: data mining, phishing attempts, malware sharing, and botnet attacks.

Young people can also become risks for themselves by *sharing too much information* or posting false information about themselves or others. Oversharing personal data and information and vice versa, may also lead to *identity theft*. By posing as someone else on social media, scammers can easily target their victims' personal information. Accordingly, they can learn their victims' area of residence, work, bank accounts, social security numbers, etc. This can be in the form of creating fake accounts of a person i.e. on a dating site, using their pictures.

Revenge porn is explained by the European Institute for Gender Equality as the following: Non-consensual pornography (the most common form of which is known as 'revenge porn') involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images. The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship, and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship. However, perpetrators are not necessarily partners or ex-partners and the motive is not always revenge. Images can also be obtained by hacking into the victim's computer, social media accounts or phone, and can aim to inflict real damage on the target's 'real-world' life (for example, intending to cause a person to be fired from their job, or in some cases causing suicide)¹⁸.

Social media and the internet are potential risks for youth *mental health and well-being*. According to some studies, cyberbullying can cause serious mental health problems. Adolescents who experience cyberbullying both as victims and as offenders have higher rates of depression, lower self-esteem, school and academic problems, more delinquent behaviors and higher rates of suicide¹⁹. At the same time, the COVID-19 pandemic and the lockdown were linked to mental health problems and more online activity in young people. Youth are turning to social media for health-related information. They can connect with mentors, therapists, and peers reducing the mental health treatment gap. However, there is little real guidance on how to deal with these issues online.

Therefore, it is imperative that the risks are identified, understood and addressed, and that there are frameworks at national and international levels focusing on those risks.

¹⁸ EIGE (2017) Cyber violence against women and girls

<https://eige.europa.eu/publications/cyber-violence-against-women-and-girls>

¹⁹ Hinduja, Sameer & Patchin, Justin. (2010). Bullying, Cyberbullying, and Suicide. Archives of suicide research : official journal of the International Academy for Suicide Research. 14. 206-21. 10.1080/13811118.2010.494133.

A few simple practices that help to minimise the risks of social media include:

- Being careful and not upload provocative photos or snapshots and elements of their private life.
- Not oversharing personal data.
- Avoiding “checking in” to places before leaving.
- Not trusting strangers online. In case of feeling uncomfortable with the content of the discussion, report it to an adult and/or block the user.
- Not inviting people you do not know to your place.

NATIONAL CONTEXT: CYPRUS

Currently, there are no laws in Cyprus focusing on social media. However, there are laws covering cybercrime or other:

1. The Law ratifying the Convention on Cybercrime (Budapest Convention), L.22(III)/2004. This legislation covers hacking, child pornography and fraud committed via electronic communication and the Internet²⁰.
2. The Law that revises the legal framework on the prevention and combating the sexual abuse and sexual exploitation of children and child pornography, L 91(I)/2014²¹. This legislation ratifies the EU Directive 2011/93/EE and covers child pornography, grooming and notice and takedown.
3. The Law ratifying the Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Racist and Xenophobic acts, L.26(III)/2004²². This legislation covers racism and xenophobia via computer systems and the Internet.
4. The Law on the Processing of Personal Data, L.138(I)/2001²³.
5. The Law on the Retention of Telecommunication data for the investigation of serious offences, L. 183(I)/2007²⁴. This legislation transposed Directive 2006/24/JHA. Although the Directive was invalidated by the Court of Justice of the EU, the national law is still valid. The national law is founded on a constitutional provision and it includes specific safeguards for the protection of privacy; for example, communication data are released only following a court order. A case was recently filed with the Supreme Court on the impact of the annulment of the EU Directive on Law

²⁰ The Law ratifying the Convention on Cybercrime (Budapest Convention), L.22(III)/2004:
http://www.cylaw.org/nomoi/indexes/2004_3_22.html

²¹ The Law that revises the legal framework on the prevention and combating the sexual abuse and sexual exploitation of children and child pornography, L 91(I)/2014
http://www.cylaw.org/nomoi/indexes/2014_1_91.html

²² The Law ratifying the Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Racist and Xenophobic acts, L.26(III)/2004
http://www.cylaw.org/nomoi/indexes/2004_3_26.html

²³ The Law on the Processing of Personal Data, L.138(I)/2001
http://www.cylaw.org/nomoi/indexes/2001_1_138.html

²⁴ The Law on the Retention of Telecommunication data for the investigation of serious offences, L. 183(I)/2007 http://www.cylaw.org/nomoi/indexes/2007_1_183.html

183(I)/2007 and the Supreme Court found that it complied with the European Convention of Human Rights.

6. The Law 112(I)/2004 Regulating Electronic Communication and Postal Services²⁵.

7. The Law implementing Directive 2013/40/EU on attacks against information systems, 147(i)/2015²⁶.

8. The Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018)²⁷. On July 31, 2018 the national law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data (Law 125(I)/2018), was published in the official gazette of the Cyprus Republic. The law was adopted for the effective implementation of certain provisions of the Regulation (EE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), which applies as of 25 May 2018.

The GDPR aims, inter alia, to control personal data management by citizens, and to create a high pan-European level of personal data protection. The Article 8 of the GDPR provides specific conditions regarding consent to the processing of children's personal data. In particular, parental consent is required for offering services on information society directly to children 16 years old or younger. However, Member States may choose to deviate and set the age limit between 13 - 16 years. Cyprus, defined the age of digital consent to 14 years old. That is, the processing of children's personal data under the age of 14 is lawful only when there is consent of a parent or guardian. Social media platforms are responsible to verify that consent is given or approved by the person who has parental responsibility for the child.

PUBLIC INSTITUTIONS RESPONSIBLE FOR ADDRESSING THE MANIFESTATION OF THE RISKS

Cybercrime is a growing challenge in Cyprus. The National Cyber Security Strategy has considered the main framework of the EU Strategy, which focuses on intergovernmental and private sector cooperation. Accordingly, the Ministry of Justice and Public Order and the Cyprus Police identified areas of action such as strengthening crime reporting and information collection which takes place through an online complaints platform, the improvement of technical means and equipment for the effective investigation of such cases, the legislation review, the strengthening

²⁵ The Law 112(I)/2004 Regulating Electronic Communication and Postal Services

http://www.cylaw.org/nomoi/indexes/2004_1_112.html

²⁶ The Law implementing Directive 2013/40/EU on attacks against information systems,

147(i)/2015 http://www.cylaw.org/nomoi/indexes/2015_1_147.html

²⁷ The Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018)

http://www.cylaw.org/nomoi/indexes/2018_1_125.html

of cooperation with the internet service providers, as well as the training of both law enforcement authorities and judges who are called upon handling these cases.

The Ministry also focuses on prevention and public awareness, where individuals and businesses are informed on the dangers of the internet.

Furthermore, the use of the Safe Internet Centre and Digital Technologies, promoted by the Ministry of Education and Culture, has been suggested within the framework of the National Strategy for research and training purposes in the field of criminal justice²⁸.

CYPRUS POLICE: The Office for Combating Cybercrime (O.C.C.)²⁹

The specialised body for cybercrime investigation is the Office for Combating Cybercrime of Cyprus Police. The Office was established in September 2007 based on Police Order No. 3/45 in order to implement the Law on the Convention on Cybercrime (Ratifying Law) L.22(III)/2004. This legislation covers hacking, child pornography, racism and fraud committed via electronic communication and the Internet. According to Police Order No. 3/45, the Office is responsible for the investigation of crimes committed via the Internet or via computers and at the same time it is responsible for the investigation of all offences that violate the rules laid down in Law 22(III)/2004.

The main duty of the O.C.C. is the investigation of child pornography and hacking cases.

According to the statistics maintained by the O.C.C., the main trends related to cybercrime in Cyprus are the following:

- Child Pornography- possession and invitation of children to take part in child pornography.
- Police Ransomware (cryptolocker).
- DDos attacks.
- Man in the Middle- emails scams.
- Phishing sites.
- Sexting/sexortion.

Its work is supported by the Digital Evidence Forensic Laboratory (DEFL), Cyprus Police, which is responsible for the effective examination of electronic evidence. DEFL is staffed with specialised officers for the collection and forensic analysis of electronic devices.

²⁸ Ministry of Justice and Public Order:

<http://www.mjpo.gov.cy/mjpo/MJPO.nsf/All/F4D7B01F53011671C225863100352B74?OpenDocument>

²⁹ Cyprus Police

<https://www.police.gov.cy/police/police.nsf/All/671EB91BDCAA303EC22584000041D696?OpenDocument>

The Commissioner for Personal Data Protection³⁰

The Commissioner for personal data protection is an independent public authority responsible for monitoring the implementation of Regulation (EU) 2016/679 (GDPR) and other laws aiming at the protection of individuals with regards to the processing of their personal data.

The Commissioner performs the duties and exercises the powers assigned by the GDPR or any other relevant law in complete independence.

The Commissioner for Children's Rights³¹

The Commissioner for Children's Rights is an independent institution which deals exclusively with the rights of the child and whose competences and obligations are prescribed by law.

Youth Board of Cyprus³²

The Youth Board's main role is advisory but it also undertakes youth related projects, following the approval of the Council of Ministers, either during the approval on the organisation's annual budget or under another special decision. It carries out symposiums, training, workshops on bullying, fake news and misinformation.

The Cyprus Safer Internet Centre (SIC) ³³

The project Cyprus Safer Internet Centre (CYberSafety) aims to strengthen the efforts for the creative and safe use of the internet in Cyprus. The centre promotes cooperation between national stakeholders aiming to create a Cyber Security culture. It has also developed and promoted the National Strategy for Better Internet for Kids in Cyprus. The project involves eight partners:

- Cyprus Pedagogical Institute, Ministry of Education, Culture, Sports and Youth
- Digital Security Authority (DSA)
- University of Cyprus (UCY)
- Cyprus University of Technology (CUT)

³⁰ Data Protection

https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_el/home_el?opendocument

³¹ http://www.childcom.org.cy/ccr/ccr.nsf/index_en/index_en?opendocument

³² <https://onek.org.cy/en/who-we-are/our-role/>

³³ <https://www.betterinternetforkids.eu/sic/cyprus>

- Pancyprrian School for Parents (PSP)
- Cyprus Neuroscience and Technology Institute (CNTI)
- Cyprus Telecommunications Authority (CYTA)
- Epic Ltd

EU AND INTERNATIONAL CONTEXT

Regarding the European Union (EU), currently there is no regulation that is applicable specifically to social media platforms. The regulatory framework is divided into multiple regulations. However, the EU has adopted a series of strategies and legislations to improve digital services. In May 2022, the Commission adopted a new European strategy for a Better Internet for Kids (BIK+), to improve age-appropriate digital services and to ensure that every child is protected, empowered and respected online³⁴. The strategy follows a provisional political agreement which contains new safeguards for the protection of minors and prohibits online platforms from displaying targeted advertising based on profiling to minors. The Audiovisual Media Services Directive (EU) 2018/1808 and the European Electronic Communications Code lay down provisions that:

- Protect children and consumers by establishing rules for the protection of minors against harmful content in the online world, including protections on video-on-demand services; and
- Combat racial, religious and other types of hatred by having reinforced rules to combat the incitement to violence or hatred, and the public provocation to commit terrorist offences.
- Provide for consumer protection: the Code benefits and protects consumers, irrespective of whether end-users communicate through traditional (calls, text message) or app-based services;

Also, the 2008 Framework Decision on combating certain forms of expressions of racism and xenophobia requires the criminalisation of public incitement to violence or hatred based on race, colour, religion, descent or national or ethnic origin.

³⁴ A European strategy for a better internet for kids (BIK+) <https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids>

IV. MAIN FINDINGS OF THE RESEARCH

3.1 Description and analysis of the data obtained from primary sources online (groups, forums etc.)

MAIN PATTERNS OF MANIFESTATION OF THE RISKS IN CYPRUS (RISK INDICATORS)

Finding the main patterns of manifestation of the risks appearing in the social media and online presence of youth in Cyprus is crucial, as it allows for the possibility to prevent and combat adverse effects in the future. More importantly, in order to effectively manage risk, it is essential to understand how vulnerability is generated, and how it builds up. Accordingly, these patterns can be classified into two categories: exposure and vulnerability.

Exposure refers to the elements in an area of online environments including social media in which risks may occur. It relates to the frequency of the presence there, and the quality of information that the person will come across. Based on the above, *elements of exposure* may be:

- The amount of time that the person spends on social media
- The frequency of visits
- The type of online environments visited
- The interests of the person involved

Vulnerability refers to conditions of people that relate to cultural, social, environmental, political, and economic contexts. Accordingly, vulnerability causes risks as it relates to exposure to hazards that are more likely to cause harm to this specific group of people who are described as vulnerable. In this sense, *elements of vulnerability* may be:

- The gender of the person involved (i.e., peer pressure)
- The age (i.e., teenagers are more likely to use more non-filtered vocabulary,)
- The level of critical thinking
- Possible lack of education on the subject
- The lack of curiosity to explore more (“Read then forget attitude”)
- The lack of a theoretical understanding of ideologies that are hidden behind certain news items;
The uncontrolled content of online resources;
- Lack of multiple sources of information;
- No cross-checking the sources.

3.2 Description and analysis of the data obtained from the survey with young people

3.2. In the framework of the survey with young people, in an open call, SYNTHESIS invited youth aged 16 - 30 living in Cyprus to fill in the questionnaire. It was an online questionnaire developed by the consortium, translated, adapted and transferred into an online form by SYNTHESIS, for Cyprus. The questionnaire included a brief presentation of the project, and then continued to the questions. The questionnaire was divided into three sections. The first section included the demographics such as age, gender, educational status, ethnicity, etc. The second part of the questionnaire seeks to examine the topic knowledge, including questions that would be used as a compass examining which type of activities young people carry out online, the frequency of their activities, identifying the risk factors in youth regarding to Cyberbullying, Online harassment, Exposure to sexually explicit material / sexting, Alienation from the real world, Grooming, Misinformation / Fake news, Breach of privacy, Identity theft, Revenge porn, Addiction, Mental health issues, documenting the main sources and methods of spreading fake news and other types of disinformation related to the global threats; identifying the key narratives employed by various actors in spreading fake news and disinformation online, as well as the main audiences targeted by these narratives.

The last stage of the research was the interpretation of the data. Interpretation consisted of studying the questions, categories and the coding to determine whether there were any overarching themes that provided insight on the subject.

Regarding demographics, out of the 40 replies, 17 individuals mentioned that they were 23 - 26 years old; 17 were in the age group 27 - 30; 4 were 19 - 22, and only 2 individuals belonged in the age group 16 - 18.

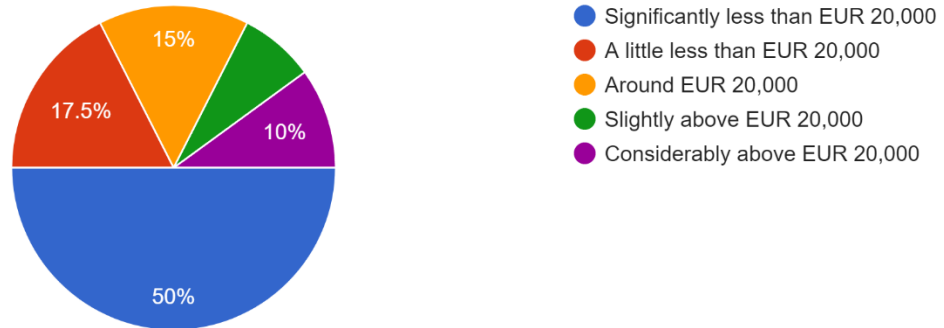
Regarding gender, 24 individuals (60 percent) were female, while 15 (37.5 percent) were noted as male. One participant mentioned gender as “not specified”.

Considering the total household income for the first semester of 2022 the replies varied³⁵. Accordingly, half of the respondents (20) mentioned that their total household income per semester was “significantly less than EUR 20,000”; 7 individuals noted that they earn “a little less than EUR 20,000”; 6 noted “around EUR 20,000”. Only 7 respondents mentioned that they were earning more than EUR 20,000 (3 replies for “slightly above EUR 20,000”; and 4 replies for “considerably above EUR 20,000”).

³⁵ For Cyprus, the average household income per semester was set to around EUR 20,000 <https://www.cystat.gov.cy/el/StaticPage?id=1203>

During the first semester of this year, your household total income was:

40 responses

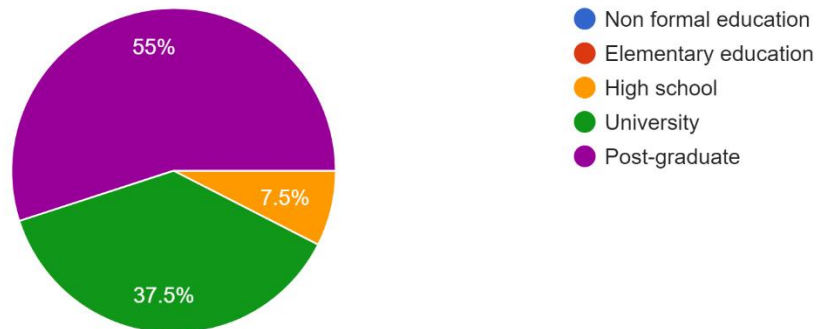


With reference to the area of residence, 21 respondents live in an urban area with 41,000 - 51,000 inhabitants; and 9 live in an urban area with 20,000 - 44,000 inhabitants. 10 of the respondents live in a rural area of 15,000 - 30,000 inhabitants; while 9 live in a rural area of 6,000 - 14,000 inhabitants.

As regards to education, 22 respondents have completed a post-graduate programme; and 15 have a university degree. Only 3 respondents are high-school graduates.

What is your highest educational program completed?

40 responses



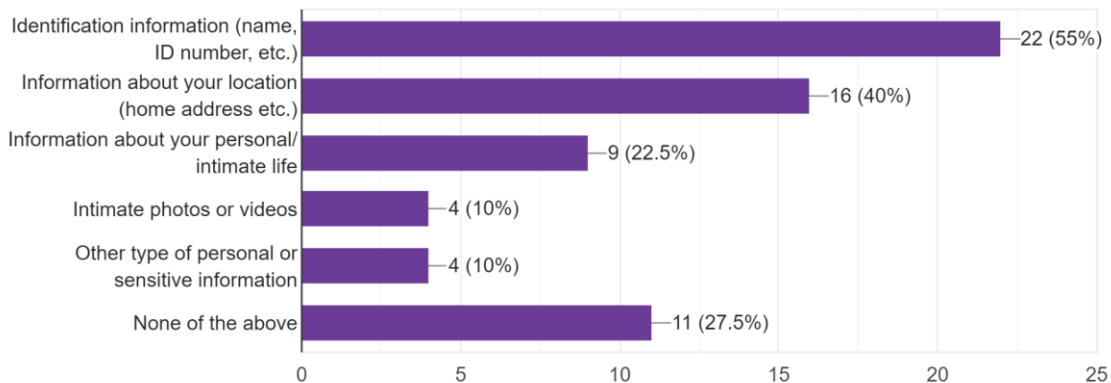
In terms of occupational status, 24 respondents are employees, while 8 are students. 6 are self-employed, and only 2 are not employed at all.

Regarding ethnicity, 34 respondents are Greek Cypriots, while only 6 mentioned "other".

As to the topic of internet use, 95 percent (38 individuals) of the respondents noted that they access the internet on a daily basis; while 1 note that they access it several times a week; and another one mentioned “never”.

On providing information to a person from the internet which they have never met in person and with whom they have no institutional affiliation, 22 respondents noted they shared identification information (name, ID number, etc.); 16 respondents shared information about their location; 9 shared information about their personal/intimate life; 4 shared intimate photos or information; 4 shared other types of information. Only 11 mentioned that they do not share anything from the above.

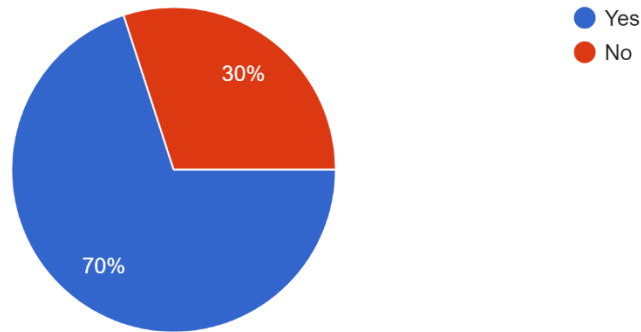
Did you ever provide the following information to a person from the internet which you have never met in person and with whom you do not have an ins...ffiliation? (mark as many options as applicable)
40 responses



Also, 70 percent (28 individuals) of the respondents provided intimate information, photos or videos to a friend or partner online.

Did you ever provide intimate information, photos or videos to a friend or partner online?

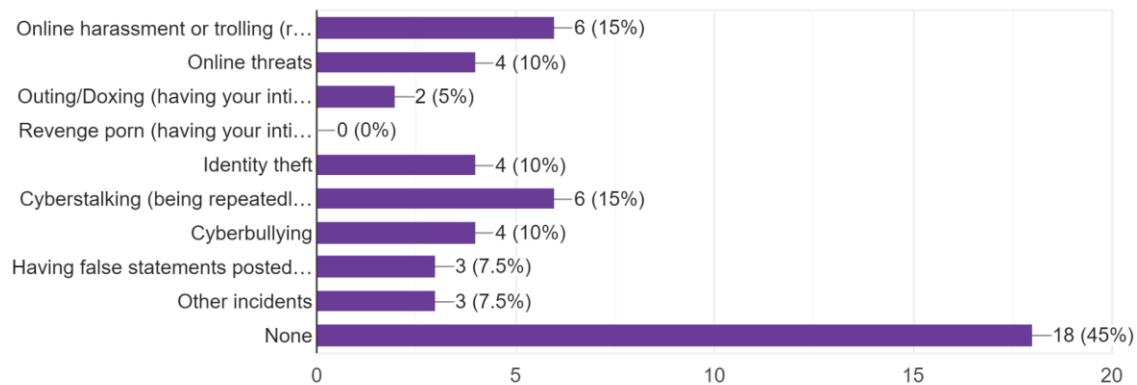
40 responses



Concerning online incidents, 45 percent (18 individuals) have never fell victims to cybercrime. 6 individuals fell victims to online harassment or trolling; another 6 individuals fell victims to cyberstalking; cyberbullying, identity theft, online threats, 4 individuals each; 3 individuals had false statements posted online in their name; while 2 individuals fell victims to outing/doxing. Interestingly, none of the respondents fell victim to revenge porn.

Have you ever been a victim of the following incidents when accessing the internet?

40 responses



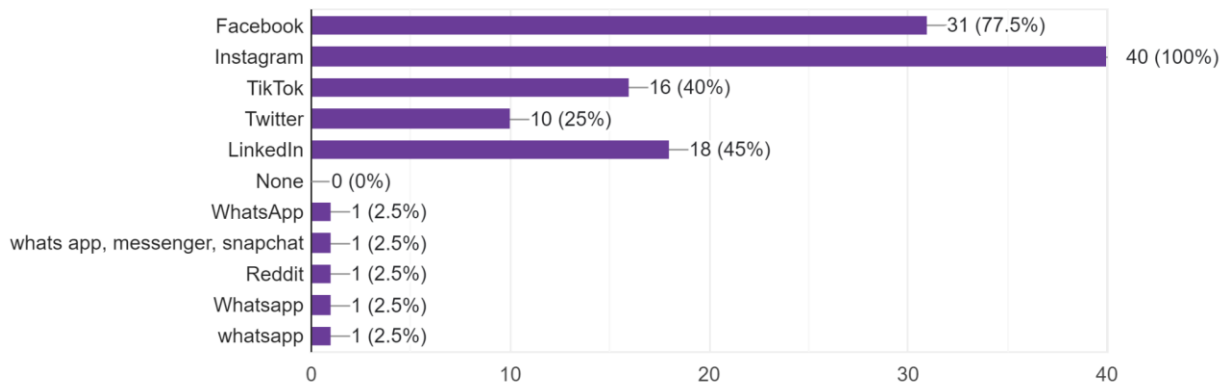
As for how young people spend their time online, 32 individuals replied that they search for information; 36 people chat with friends and family; 33 people shop; 31 watch movies or listen to music; 30 read the news about politics and current events; 24 participate in educational programmes or work from home; 16 play games; and 14 participate in online discussions. Only a few individuals search for friends or partners (9), and blog or vlog (3). Interestingly, none of the respondents mentioned that they practice online gambling.

However, in the next question regarding whether they have engaged in gambling in the past two years, 3 individuals noted that they had, while 37 individuals noted that they had not.

Regarding what social networks they use, 40 individuals mentioned that they use Instagram; 31 Facebook; 18 LinkedIn; 16 TikTok; 10 Twitter. Other social networks mentioned included WhatsApp (3), Messenger (1), Snapchat (1) and Reddit (1).

What type of social network platforms do you use on a regular basis? (choose all relevant options)

40 responses



On the topic of reading the news about politics and current events, 47.5 percent (19 individuals) read the news daily; and 32.5 percent (13 people) read them once every few days. 5 people read the news once a week, and 3 once a month. 55 percent (22) also mentioned that they read only the title and the first paragraph; and only 35 percent (14) read the whole article.

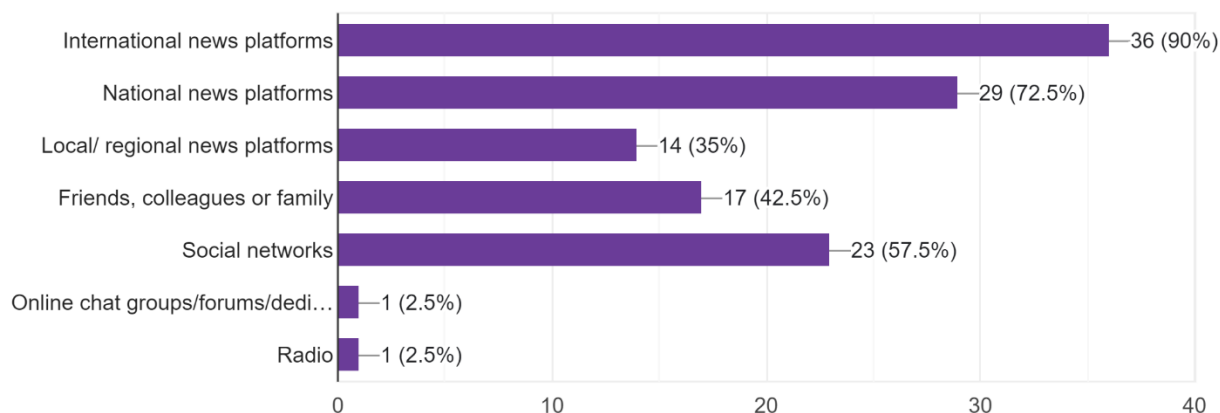
In terms of political orientation, 42.5 percent (17 people) are moderate left-wing; 27.5 percent (11) are Apolitical or not interested in politics; 12.5 percent (5) are moderate right-wing; and 10 percent (4) do not know. 7.5 pe cent (3 people) are extreme left-wing.

80 percent (32 individuals) never comment on news platforms; while 12.5 percent (5) comment once a week.

Regarding the top sources of information on politics and current events, 90 percent (36) reach international news platforms; 72.5 percent (29) read national news platforms; 57.5 percent (23) use social networks. 42.5 percent (17 people) learn information from friends and family; and 14 people from local or regional news platforms.

What are your top three sources of information on politics and current events? (choose 3 from the list)

40 responses



On interacting with others on social media, 16 individuals interact every day; 10 once or twice a week; 7 interact less than once per month; and 6 never interact with others on social media.

The situation is a bit different regarding interactions through private chats, as 92.5 percent (37) use them every day; while only 5 percent (2 people) use them less than once a week.

In order to determine the agreement of respondents with fake news, they were asked to rate their agreement with a series of four statements, all representing misinformation frequently circulated in Cyprus and internationally. We selected statements related to the COVID-19 pandemic and vaccination, the war in Ukraine, Muslim immigrants and global warming, in order to cover some of the most frequent subjects targeted by fake news.

Concerning the COVID-19 pandemic, 26 respondents mentioned that it makes them somewhat anxious; while 11 are not anxious at all. 3 individuals mentioned that the pandemic makes them very anxious.

On the war in Ukraine, 19 individuals said that they are somewhat anxious, and 14 that they are very anxious. 7 people are not anxious at all.

Regarding the accuracy of the statements that we presented the respondents, the situation was as follows:

COVID-19 vaccines can cause infertility:

19 respondents believe that it is unlikely; 11 said it is not accurate; 8 remained neutral; and only 1 noted that the statement is somewhat accurate.

The crimes in Bucha and Irpin, Ukraine were staged by the Ukrainian government in order to receive Western aid:

15 respondents stated that it is unlikely to be accurate; 12 said it was not accurate at all; 12 remained neutral; and 1 said that it was somewhat accurate.

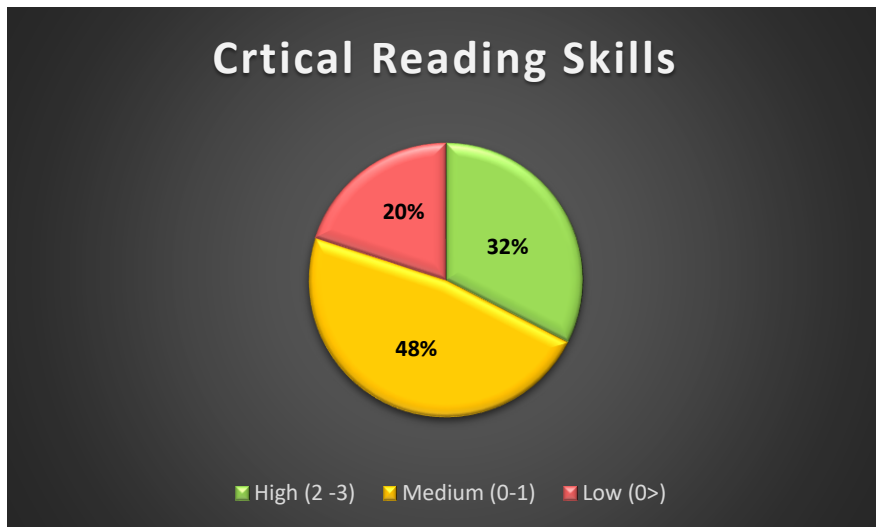
Most Muslim immigrants from the Middle East are likely to be involved in criminal/ terrorist acts:

12 respondents stated that it is unlikely to be accurate; 23 said it was not accurate at all; 4 remained neutral; and 1 said it was somewhat accurate.

Global warming is not real, but it is used as a pretext by Global elites to control global resources:

9 respondents stated that it is unlikely to be accurate; 25 said it was not accurate at all; 4 remained neutral; and 2 stated that it was somewhat accurate.

For the following question, the respondents needed to choose the correct statements. This question measured critical reading, attentive reading, and the ability to understand the meaning of the text; and focuses on the ability of people to critically evaluate online information and news. According to literature, the inability to understand the meaning of a text plays a major role in spreading fake news and misinformation³⁶. Based on the data, 32% of respondents had high critical reading skills, 48% had medium skills and 20% had low skills.



Next, the analysis suggests that many young people are skeptical about sharing their personal information online with unknown people; however, there is a high number that does share specific information. This is not the case when dealing with people known to them, such as

³⁶ Machete P, Turpin M. The Use of Critical Thinking to Identify Fake News: A Systematic Literature Review. *Responsible Design, Implementation and Use of Information and Communication Technology*. 2020 Mar 10;12067:235–46. doi: 10.1007/978-3-030-45002-1_20. PMID: PMC7134234.

friends and family, where a high percentage (70 percent) of providing intimate information, photos or videos, to friends and partners was reported. It appears that the factor of personal contacts, (knowing the person personally) makes it easier for youth to share personal information.

It appears that there is a correlation between the types of cybercrimes committed and gender. Specifically, the data suggest that females are slightly more likely than males to experience online harassment (3:2). In another manner, females are as likely as males to experience cyberstalking (3:3); while males are more likely than females to experience online threats (3:1). Regarding cyberbullying, the data suggest that males are more likely than females to be targets (3:1).

A similar number of males and females use social media such as Instagram, Facebook and LinkedIn; while TikTok is more female-oriented.

The data suggests that individuals who read the news on politics on a daily basis, usually read the whole article or the title and the first paragraph; and those who read the news every few days tend to read just the title and the first paragraph.

In terms of political orientation, 50 percent of the respondents reported being either moderate or extreme left-wing. A quarter of them consider themselves right-wing. The rest appear to be apolitical or not interested in politics.

Also, it appears that there is a potential correlation between those who read the news every day with the level of stress about COVID-19, as it was reported that the vast majority of those respondents were somewhat anxious about the pandemic. The situation is similar regarding the war in Ukraine.

Regarding critical thinking and the ability to understand the meaning of text, based on the last part of the questionnaire, the majority of the participants appear to have a good level of critical thinking, attentive reading, and the ability to understand the meaning of the text. On the other hand, there were a few cases where the participants did not appear to have good understanding of the text, and based on their answers, they had low critical thinking skills. It appears that gender is not a factor of measuring critical thinking, but age could potentially be an influencing factor, as most of the respondents with a score 3,4, and 5 on the questions measuring critical thinking were either 23 - 26 or 27 - 30 years old. However, we must keep in mind the limited number of respondents. We could not deduct any results regarding ages 16 - 18 and 19 - 22 years old.

3.3 Description and analysis of the data obtained from interviews with youth workers/trainers

3.3. The youth workers/trainers and professionals in RISE, were selected upon their knowledge and experience on youth and youth online risks in the Cyprus context. Four experts participated in the interviews, which were held mostly by phone. After a brief introduction, in which we explained various aspects of the project RISE, and how their views would be noted, we conducted the interviews.

All the interviewees work in Nicosia and their professional occupations include music history, gender studies, Greek teacher and research. One of the professionals interviewed in the framework of the RISE project is a university lecturer. The interviewees also have experience in youth work, either by participating and/or conducting youth trainings or by carrying out research in the field; and their background includes organizing storytelling workshops, green workshops, seminars, master classes; facilitating activities relevant to active citizenship, sustainability, social inclusion, and around thematic areas such as hate speech, democracy, gender equality, peace education, environmental sustainability; working with migrant integration, STEAM, etc.

Their target groups include young people aged 16 - 30. One of the professionals also works with children from age 10 to 17, as well as young adults up to 30 years old.

Regarding the online behavior of young people, two of the youth workers mentioned that young people are rather careless, and do not have the capacity to filter the huge amount of information that they have access to, nor are they very aware of the risks involved.

However, at the same time they are very aware of many different aspects of different areas that otherwise they would not have easy access to.

It was also noted that there is a difference between young people aged 16 – 22 and 23 - 30, as the former group are more open to explore and to share different views, perspectives such as gender issues, sexuality, ethnic diversity, etc. Additionally, they have access to a certain language. Usually, teenagers use more non-filtered vocabulary, but also younger adults (25+) tend to post, but not in an unfiltered manner (they are more politically correct, but they also spread stereotypes relevant to gender).

On the topics of the COVID-19 pandemic influence upon youth online behavior, the interviewees mentioned that unavoidably, the pandemic played a huge role in the online attitudes of young people, as everything turned immediately online, including education and information, but also social life. Thus, youth were exposed more than before to either receiving or posting i.e., hate comments. The online environment also became a refuge from the lockdowns.

Also, the youth workers mentioned young people tend to share their personal information online with unknown people, because for youth there is no clear distinction between virtual and real world. Especially for teenagers, it is an extension of their reality; thus, if they have a community that they feel safe in, they will share their data easily.

One youth worker said that peer pressure also is an issue. For example, in romantic relationships, girls especially feel obliged or perceive a certain pressure to share more personal photos in order to be accepted or “cool”, usually by their boyfriends or by their male friends. On the other hand, one youth worker mentioned that young people cannot be tricked as easily as older people.

Moreover, youth tend to send intimate media content to their intimate partners online or by phone, because, according to youth workers, youth do not realise the risk associated. Unwittingly, in online communication it appears like sending intimate media content is the norm, and like young people cannot get exposed. One professional stressed that we should not demonise the action of sharing intimate moments with intimate partners, but rather set more strict sanctions for those who actually take advantage of releasing them to others or widely. It is important to deconstruct the concept of intimate moments. Young people feel pressure that someone will see them, but the truth is that this is not their problem. The issue here are the structures behind (feeling ashamed because someone saw you naked, or someone saw your breasts). As one of the persons interviewed mentioned, “It is about taking the blame out of the victim”.

The interviewees also commented that young people fall victim to online incidents quite often, saying that it happens more often than in the past, but some incidents, such as posting your personal information online, are more likely to happen than others, such as revenge porn. One youth worker mentioned that there is no effort to create a culture or to educate teenagers on how to behave in online environments, respect boundaries and protect themselves.

Related to online gambling, youth workers said that young people think of it as an easy way of gaining money. Two of the youth workers were not sure about this topic.

Regarding the level of media literacy, youth workers mentioned that young people are tech-literate but in terms of online literacy as in how to have a critical approach towards what they are reading, the level is pretty low. They cannot filter the information. They do not have a critical perspective towards news, so they take fake news as established facts and they share them with their peers.

On critical thinking, two youth workers commented that the level of youth is low, while the other two said it was high. Specifically, they mentioned that youth have critical thinking and that they should not be underestimated.

According to the interviewees, youth fall victims to online misinformation and fake news because of:

- Lack of education;
- A false believe from older generations that whatever they read on the internet is true;
- The uncontrolled content of online resources;
- Lack of critical thinking;
- Lack of multiple sources of information;
- Lack of curiosity to explore more;

- Lack of theoretical understanding of ideologies that are hidden behind certain news items;
- No cross-checking the sources.

Finally, regarding the kind of information or training that young people need in order to avoid these risks, youth workers mentioned that the training needs to start from early education and that teachers and educators should strive for a critical approach methodology that involves the student in the learning process. We could have:

- Media literacy trainings
- Specific online literacy courses at least for aspects of harassment (to identify when and how one might be harassed). For online harassment/threats we need to address the victim and the aggressor differently. Also, we need a holistic approach of training at school, specific TV approach, in society, etc.
- Human rights education and training to understand the concept and universality of human rights that everyone should be respected on sexual orientation, gender, to become more sensitized towards those issues so they become more critical.
- Hate speech and online hate speech training sessions so they know the severity of the action of posting something that can be considered hate speech and they can be prosecuted, as it is a punishable action by the ECtHR.
- For identity theft, youth need to learn not to share sensitive information, ways that someone can steal one's identity, ie. Scanning their card.
- Also, training in schools on critical thinking, hate speech, self-empowerment, sexual education, gender equality education like workshops, workshops on online behavior, what one should not or should share online, websites you should not visit.

V. CONCLUSIONS AND RECOMMENDATIONS

The RISE country report documents the status quo, as well as the risks that young people in Cyprus face on social media, and maps the current needs and recommendations for addressing these needs. The report reveals the link between youth's offline-online vulnerability, risky behaviors online and consequences and impact of social media. At the same time, it designs a content strategy to collect and develop the digital content of the Game of PR2. Accordingly, this content will be used to build a framework for the Game (PR2) and its objective is to foster support to young people in identifying the risks of social networks, and mitigating them. The Game will enhance online vigilance of young people, and offer them resources and tools to deal with underlying online social- networks (OSN) threats.

CONCLUSIONS

The main results of the primary and secondary research are as follows:

It was concluded that it is usual that young people sometimes share information about themselves to persons who they have never met in person and with whom they have no

institutional affiliation, including identification information; location; information about personal/intimate life; intimate photos; and other types of information. Only a few mentioned that they do not share anything. However, it is even more widespread to share such type of information with people they know.

Concerning online incidents, almost half of the young people who participated in the survey have never fell victims to cybercrime; but a few of them fell victims to online harassment or trolling; cyberstalking; cyberbullying, identity theft, online threats; had false statements posted online in their name; and outing/doxing. None fell victim to revenge porn.

More than half of the participants spend their time online searching for information; chatting with friends and family; shopping; watching movies or listening to music; reading the news; participating in educational programmes or working from home. A smaller number of participants spend their online time playing games; and participating in online discussions. Only a few individuals spend their time searching for friends or partners, blogging or vlogging.

Very few of the respondents engaged in gambling over the past year.

The most popular social network that young people in Cyprus use is Instagram. Facebook is second, followed by LinkedIn, TikTok, and Twitter. Other social networks used by young people were WhatsApp, Messenger, Snapchat, and Reddit.

Half of the young people consider themselves left-wing (whether moderate or extreme), while a quarter of them consider themselves apolitical or not interested in politics. The rest were right-wing, and a few people do not know their political orientation.

The majority of the participants appear to have a good level of critical thinking, attentive reading, and the ability to understand the meaning of the text. On the other hand, there were a few cases where the participants did not appear to have good understanding of the text, and based on their answers, they had low critical thinking skills.

TRAINING NEEDS IN RESPONSE TO FAKE NEWS AND DISINFORMATION

According to our research, youth fall victims to online misinformation and fake news that can attributed to the following reasons:

- Lack of education;
- A false believe from older generations that whatever they read on the internet is true;
- The uncontrolled content of online resources;
- Lack or low levels of critical thinking;
- Lack of multiple sources of information;
- Lack of curiosity to explore more;

- Lack of theoretical understanding of ideologies that are hidden behind certain news items;
- No cross-checking the sources.

To address these issues, a critical approach methodology that involves the student in the learning process is needed. Therefore, the following training needs in response to fake news and disinformation are proposed:

- Youth to have specific online and media literacy courses
- Youth to have training on:
 - Critical thinking
 - Self-empowerment
 - Online behavior (what you should not or should share online, websites you should visit or not, how to evaluate what is true or not, etc.).

They could be shaped for schools or in the form of non-formal education trainings and workshops.

RECOMMENDATIONS FOR PREVENTING AND MITIGATING OTHER RISKS

Regarding recommendations for preventing and mitigating the other risks, this report has taken a step by offering a description of the risks associated to the use of social media for young people. The next step is to develop new teaching and learning approaches that seek to develop the necessary skills for addressing these risks, and offer the tools that young people need to identify and combat them.

These training approaches need to start from early education, and teachers and educators should strive for a critical approach methodology that involves the student in the learning process. Therefore, we recommend:

- Media literacy trainings
- Specific online literacy courses at least for some aspects of harassment. The aspect about the content and information is much deeper and needs to go through a process of long education.
- For online harassment/threats we need to address the victim and the aggressor differently. We also need a holistic approach of training at school, specific TV approach, society, etc.
- Human rights education and training to understand the concept and universality of human rights that everyone should be respected on sexual orientation, gender, to become more sensitized towards those issues so they become more critical.
- Hate speech and online hate speech training sessions so they know the severity of the action of posting something that can be considered hate speech and they can be prosecuted, as it is a punishable action by the ECtHR.
- For identity theft, youth need to learn not to share sensitive information, ways that someone can steal your identity through workshops, educational videos, etc.

- Training in schools on critical thinking, hate speech, self -empowerment, sexual education, gender equality education like workshops, workshops on online behavior, what you should not or should share online, websites you should or should not visit, etc.
- The Youth Board of Cyprus can be the responsible authority to create the framework for designing these trainings
- The Ministry of Education to enter in the curriculum more workshops on safe internet practices for children and young adults
- Creation of projects targeting not only youth but also parents of young people at risk, aiming to educate them about the risks and how to combat them.

RECOMMENDATIONS FOR DESIGN, CONTENT AND PROMOTION OF THE GAME

The recommendations for the game are as follows:

Content:

- Create an educational game on social media risks (game-based learning)
- The game can include quizzes, puzzle solving based on knowledge learned (see examples here: <https://www.makeuseof.com/tag/6-internet-safety-games-kids-cyber-smart/>)
- Create different storylines based on age groups (i.e., age group 16 - 18, 19 - 22, 23 - 26, 27 - 30)

The objectives of the game can be the following:

- Target groups to learn to protect their personal information
- To learn how to identify positive and respectful communication, cyberbullying, phishing, help-seeking, and other safe behaviors while using technology to communicate.
- break bad security habits.

Design:

- Use vivid colors to attract more players
- No gender specific
- Create an interesting storyline available for both Desktop and Mobile phones (Android and iPhone)
- Use storytelling
- Actionable and practical content

Promotion:

- Share with our networks
- Share on social media
- Share with youth organizations, schools, etc.
- Create “teaser’ videos

BIBLIOGRAPHY

Edosomwan, Simeon & Prakasan, S.K. & Kouame, D. & Watson, J. & Seymour, T.. (2011). The history of social media and its impact on business. *Journal of Applied Management and Entrepreneurship*. 16. 79-91.

Clinical Report--The Impact of Social Media on Children, Adolescents, and Families Gwenn Schurgin O'Keeffe, Kathleen Clarke-Pearson and COUNCIL ON COMMUNICATIONS AND MEDIA Pediatrics; originally published online March 28, 2011; DOI: 10.1542/peds.2011-0054 <https://research.fit.edu/media/site-specific/researchfitedu/coast-climate-adaptation-library/climate-communications/youth-climate-amp-social-media/O'Keeffe--Pearson.-2011.-Impact-of-Social-Media-on-Children,-Adolescents,-and-Families..pdf>

Edosomwan, Simeon & Prakasan, S.K. & Kouame, D. & Watson, J. & Seymour, T.. (2011). The history of social media and its impact on business. *Journal of Applied Management and Entrepreneurship*. 16. 79-91.

DataPortal: Digital 2022: July Global statshot report : <https://datareportal.com/reports/digital-2022-july-global-statshot>

Eurostat 2016.

https://ec.europa.eu/eurostat/statisticsexplained/index.php?title=Archive:Internet_access_and_use_statistics_-_households_and_individuals

Christodoulides, C., Intziegianni, K., Mappourides, A., Antoniou, P. and Hadjifoti, P. (2021). Exploring the relationship of young people in Cyprus with the Social Media and the Internet. Alexander College-Alexander Research Centre

Kelly Y, Zilanawala A, Booker A et al. *EClinicalMedicine* 2019;6:59-68

Machete P, Turpin M. The Use of Critical Thinking to Identify Fake News: A Systematic Literature Review. *Responsible Design, Implementation and Use of Information and Communication Technology*. 2020 Mar 10;12067:235-46. doi: 10.1007/978-3-030-45002-1_20. PMID: PMC7134234.

UNICEF: Cyberbullying: What it is and how to stop it <https://www.unicef.org/end-violence/how-to-stop-cyberbullying> [Accessed September 2022]

Child Abuse & Neglect 32 (2008) 277-294 Are blogs putting youth at risk for online sexual solicitation or harassment? Kimberly J. Mitchell *, Janis Wolak, David Finkelhor Crimes against Children Research Center, Family Research Lab, University of New Hampshire, Durham, NH, USA Received 6 June 2006; received in revised form 13 April 2007; accepted 13 April 2007

John Sammons, Michael Cross, in *The Basics of Cyber Safety*, 2017

Lin WH, Liu CH, Yi CC. Exposure to sexually explicit media in early adolescence is related to risky sexual behavior in emerging adulthood. *PLoS One*. 2020 Apr 10;15(4):e0230242. doi: 10.1371/journal.pone.0230242. PMID: 32275669; PMCID: PMC7147756.

Wood, A. C., & Wheatcroft, J. M. (2020). Young Adult Perceptions of Internet Communications and the Grooming Concept. *SAGE Open*, 10(1). <https://doi.org/10.1177/2158244020914573>

European Commission: Tackling online disinformation <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation>

European Commission: A European strategy for a better internet for kids (BIK+) <https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids>

EIGE (2017) Cyber violence against women and girls <https://eige.europa.eu/publications/cyber-violence-against-women-and-girls>

Hinduja, Sameer & Patchin, Justin. (2010). Bullying, Cyberbullying, and Suicide. *Archives of suicide research : official journal of the International Academy for Suicide Research*. 14. 206-21. 10.1080/13811118.2010.494133.

The Law ratifying the Convention on Cybercrime (Budapest Convention), L.22(III)/2004: http://www.cylaw.org/nomoi/indexes/2004_3_22.html

The Law that revises the legal framework on the prevention and combating the sexual abuse and sexual exploitation of children and child pornography, L 91(I)/2014 http://www.cylaw.org/nomoi/indexes/2014_1_91.html

The Law ratifying the Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Racist and Xenophobic acts, L.26(III)/2004 http://www.cylaw.org/nomoi/indexes/2004_3_26.html

The Law on the Processing of Personal Data, L.138(I)/2001 http://www.cylaw.org/nomoi/indexes/2001_1_138.html

The Law on the Retention of Telecommunication data for the investigation of serious offences, L. 183(I)/2007 http://www.cylaw.org/nomoi/indexes/2007_1_183.html

The Law 112(I)/2004 Regulating Electronic Communication and Postal Services http://www.cylaw.org/nomoi/indexes/2004_1_112.html

The Law implementing Directive 2013/40/EU on attacks against information systems, 147(i)/2015 http://www.cylaw.org/nomoi/indexes/2015_1_147.html

The Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018)
http://www.cylaw.org/nomoi/indexes/2018_1_125.html

Project's Partners



Institute Of Entrepreneurship Development
<https://ied.eu/>
info@ied.eu
<https://www.facebook.com/ied.europe/>



VITALE TECNOLOGIE COMUNICAZIONE - VITECO S.r.l
<https://www.vitecolearning.eu/en/>
projects@jogroup.eu
<https://www.facebook.com/VITECO.eLearning.LMS.SeriousGames.SCORMConversion>



BK Consult GbR
<https://bk-con.eu/>
info@bk-con.eu
<https://www.facebook.com/bkcon.eu>



Learning For Integration Ry
<https://www.lfi.fi/>
marjaliisa@lfi.fi
<https://www.facebook.com/LearningForIntegration>



Asociatia Central Pentru Legislatie Nonprofit
<https://clnr.ro/>
office@clnr.ro
<https://www.facebook.com/clnr.ro>



Synthesis Center For Research And Education Ltd
<https://www.synthesis-center.org/>
info@synthesis-center.com
<https://www.facebook.com/synthesis.cyprus>



Action-based approach in addressing and mitigating risks of young people in online social networks



**Co-funded by
the European Union**

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.