Author: Dimitris Georgoulis
Contributor: Stella Ioannou

Youth online behavior, risks and avenues for mitigating them

National report: Greece

Co-funded by the European Union

RISE

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

Agreement Number: **2021-1-RO01-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.

Contents

Introduction

This report examines socio-demographic factors, social media use, risk perception, preventive behaviors, attitudes and other relevant factors in the context of the post-COVID-19 pandemic. The end-purpose of this report is to evaluate the current state of affairs and the learning needs of young people, in order to provide relevant information for the development of an online game aimed as equipping young people with the necessary tools for avoiding the risks identified.

The report provides an overview of youth online behavior, the main online risks associated with youth, patterns of manifestation of these risks and their regulation in the Greek law.

This report examines the socio-demographic characteristics of Greek youth aged 16-30 (age, gender, socio-economic status, rural/ urban residence, level of education, ethnicity), the main characteristics of their social media use and online behavior, their risk perception, existing preventive behaviors and attitudes, as well as the manifestation of the risks, in the post COVID-19 pandemic. The study also explores the attitudes and behaviors of youth towards global threats, such as pandemics, international politics, armed conflicts and refugee and to identify the risk factors in youth regarding to online activity (cyberbullying, revenge porn and other image-based sexual abuse, the spread of fake news and misinformation, online gaming/ gambling addiction and identity theft), as well as other relevant risks.

The analysis of the collected data will establish a set of risk factors in young people, as well as specific and general recommendations and strategies for preventing and combating the identified risks. This research is based on both quantitative data, collected through an online survey addressed to young people, and on qualitative data, obtained through a series of 4 interviews conducted with youth trainers, young workers and other professionals working with young people.

This report has been elaborated with the scope of the RISE project: Action-Based Approach in Addressing and Mitigating Risks of Young People in Online Social Networks, financed by European Union’s Erasmus+ Programme, Strategic Partnerships - Key Action 2, project number 2021-1-RO01-KA220-YOU-000028688.

Methodology

The quantitative data for this study was collected through on online survey addressed to young people (16-30) conducted by the Institute of Entrepreneurship Development (iED) in Greece in the period of October-December 2022. The survey was based on a questionnaire including 29 multiple-choice questions designed to assess demographic characteristics of the sample, media use and online habits, risky behavior and manifestation of associated risks, feelings and attitudes towards current events as well as critical reading skills. The questionnaire was circulated through google forms and was filled in by 42 participants, on a volunteer basis.

The small size of the sample, as well as its homogeneity, are likely to influence the quality of the results and to make it impossible to extract relevant data for some of the items which were tested in the survey. Since the study was conducted online and could be answered by any young person willing to do so, a self-selection effect occurred and respondents were mainly the kind of people who are inclined to respond to online survey, which means they share a significant number of characteristics and do not accurately reflect the structure and diversity of the wider population. Given the fact that certain socio-demographic categories are disproportionately represented among the respondents, it was decided in most situations to present percentages instead of absolute numbers when it came to frequencies. However, all percentages presented should be considered in relation to the absolute numbers they represent, given the small number of respondents. It should be kept in mind that all the findings in the present report are only applicable to the present sample and cannot be extrapolated to the general population, for methodological reasons.

The qualitative data was obtained through semi-structured interviews conducted with youth workers and youth trainers in Greece, in November - December 2022. The professionals consulted for this research had between 2 and 7 years of working experience with young people. The age of young people within whom the interviewed professionals work ranged from 8-30 years old. The experience of the professionals interviewed includes formal education (one high school teacher), non-formal education (one youth workers), and one physical education teacher.

In the survey with young people, IED invited Greek youth aged 16-30 to participate in an online questionnaire. The questionnaire, which was developed by the consortium and adapted for Greece by IED, consisted of three sections. The first section collected demographic information such as age, gender, ethnicity, income, place of residence and education level. The second section examined the participants' knowledge of various online risks, including fake news, cyberbullying, exposure to adult content, and identity theft, as well as the existence of risky behavior, manifestation of risks, level of critical thinking and attitude towards global events, such as the Covid-19 pandemic, the war in Ukraine and migration. The final stage of the research involved interpreting the collected data to identify overarching themes and formulating recommendations.

The authors of this study interviewed four experts who were selected based on their knowledge and experience working with youth and online risks in Greece. The professionals interviewed included a music historian, a gender studies expert, a Greek teacher, and a researcher, all of whom have experience in youth work and organizing workshops, seminars, and activities related to active citizenship, social inclusion, sustainability, and other thematic areas.

Literature review

Youth are the heart of our society. As Internet natives [Gui & Argentin, 2011], they are born and raised inside an environment where Internet and digital technologies are omnipresent. The universal broadband penetration in most countries, in concert with the advent of smart, mobile devices with touch-screen and networking capabilities, have also changed the cyber society that our young children live in. A characteristic example is the exponential growth rate of online social networking (OSN) penetration among youth, starting from early adolescence [Quinn & Oldmeadow, 2013]) (Magkos et al. n.d.).

The potential beneficial impact of (balanced) use of the Internet and digital technologies into the psychosocial well-being, creativity, cognitive skills and academic performance of youth has already been noted in the literature [Jackson et al, 2006, Fiorini et al, 2010]. This is reflected on the fact that most OECD countries support, starting from primary education, the development of digital skills in early childhood, while less developed countries engage initiatives such as the “one laptop per child” project. Not surprisingly, the majority of parents support their young children’s acquaintance with the computers and the Internet [Holloway et al, 2013].

As most things in life have dual aspects, children’s exposure to the Internet can also be seen from a different, more negative theories. Specifically, children may be exposed to a number of threats such as, among others, inadequate content and/or contacts [Marinos et al, 2011], Internet addiction [Andreou et al, 2013], other psychosocial deviation [Fiorini et al, 2010, Wang et al, 2013], loss of personal/sensitive data, etc.

During the nineties, shopping malls were a popular place for teenagers to hang out in public, but they were gradually pushed out along with other public spaces such as streets, parks, and libraries, due to the perception of a threatening street culture. Nowadays, teens and children have migrated to online public spaces, such as social networking sites (SNSs), instant messaging (IM), and mobile phones to socialize, negotiate identity, gossip, support one another, collaborate, share information, flirt, joke, and goof around. By using social media, young people can expand their social interactions beyond physical boundaries, with SNSs being a popular tool for communication, maintaining relationships, finding friends, jobs, and dates, extending their networks, updating others on their activities and whereabouts, sharing information, photos, videos, and music, receiving event updates, inviting others to events, presenting an idealized version of oneself, sending private messages, and posting public testimonials.

The emergence of information and communication technologies (ICT) has increasingly mediated all aspects of young people’s lives as they engage daily in multiple online practices in various spaces such as their homes, schools, and communities, but also ‘on the move’, through the use of portable devices and wireless connection (Livingstone Helsper, 2007; Lauricella et al., 2014; Michikyan and Suarez andOrozco, 2016). As the integration of these technologies in young people’s lives has changed the context in which they are growing up, there has been increasing interest in exploring, conceptualizing, and understanding the opportunities and the risks being created in the digital era. Furthermore, contemporary studies on youth, digital media and education aim to investigate how these changes influence various aspects of young people’s development (Erstad, 2013; al., 2016 ; Livingstone and Seft onGreen, 2016).

It is crucial to identify the main patterns of risk manifestation related to the social media and online presence of youth in Greece as they could lead to future adverse effects. Understanding the generation and accumulation of vulnerability is essential to managing risks effectively. The identified patterns can be divided into two categories: exposure and vulnerability.

Exposure refers to the elements in online environments, including social media, where risks can occur, such as the amount of time spent online, frequency of visits, type of environments visited, and interests.

Vulnerability pertains to contextual conditions, including cultural, social, environmental, political, and economic factors, that can result in risks due to exposure to hazards that are more likely to cause harm to certain groups of people. Elements of vulnerability may include gender (such as peer pressure), age (such as the use of non-filtered vocabulary by teenagers), level of critical thinking, lack of education on the subject, lack of curiosity to explore, absence of theoretical understanding of hidden ideologies behind news, uncontrolled online content, lack of multiple sources of information, and no cross-checking of sources.

In Greece, risks related to youth online behavior are regulated by a number of laws and regulations aimed at protecting children and teenagers from harmful content and online activities.

One of the primary pieces of legislation governing this area is Law 4070/2012, which focuses on the protection of personal data in the context of electronic communications. This law requires service providers to take appropriate measures to protect personal data and ensure the privacy of users, including minors.

Additionally, Law 4624/2019 establishes the National Safe Internet Center in Greece, which is responsible for promoting safe and responsible use of the internet by children and young people. The center provides educational resources, information, and advice to children, parents, and educators, as well as coordinating with law enforcement agencies to investigate and combat online crimes.

Moreover, Law 4521/2018 concerns the protection of minors from material harmful to their health or development, which includes online content. The law prohibits the dissemination of content that could be harmful to minors, such as pornography, violence, and hate speech, and provides for the imposition of fines and other penalties for violations.

In Greece, the legal framework for regulating risks deriving from youth online behavior is primarily governed by the Greek Data Protection Authority (HDPA), which is responsible for enforcing the General Data Protection Regulation (GDPR) within the country. The GDPR is a comprehensive EU data protection law that sets out rules for the collection, use, and storage of personal data, including data related to minors.

Under the GDPR, organizations that process personal data, such as social media companies and online gaming platforms, must take appropriate measures to ensure the security of that data and protect individuals from risks associated with their online behavior. This includes taking steps to prevent cyberbullying, grooming, and other forms of online harassment or exploitation.

In addition to the GDPR, Greece has also enacted several laws and regulations related to child protection and online safety. For example, Law 4070/2012 sets out measures for the protection of minors from harmful online content, including provisions for the establishment of a national hotline for reporting online child abuse.

Furthermore, the Greek government has established several initiatives aimed at promoting online safety and digital literacy among young people. For instance, the "SaferInternet4Kids" program is a national initiative that provides resources and educational materials to parents, teachers, and young people to help them navigate online risks and promote responsible online behavior.

Overall, the legal framework in Greece is designed to protect young people from the risks associated with their online behavior by ensuring that organizations that process personal data take appropriate measures to protect that data and prevent online harm. Additionally, the Greek government has established various initiatives aimed at promoting digital literacy and empowering young people to stay safe online.

According to a report by the Hellenic Data Protection Authority (HDPA) published in 2020, there were a total of 2,828 data breaches reported in Greece between May 2018 and December 2019. Of these, 703 were related to unauthorized access to personal data, and 115 were related to identity theft. It's worth noting that these numbers only reflect the reported cases of data breaches and identity theft, and it's likely that many incidents go unreported. Additionally, this data only covers a relatively short time period, so it may not provide a complete picture of the prevalence of identity theft in Greece. According to a report by the Cyberlaw Clinic of the University of Athens published in 2018, revenge porn was a relatively new phenomenon in Greece, and there were only a few reported cases at that time. However, the report noted that the number of cases was expected to increase in the coming years, as awareness of the issue grew and more victims came forward.

In 2019, the Hellenic Data Protection Authority (HDPA) reported that revenge porn was one of the most common types of privacy violation reported in Greece, along with unauthorized access to personal data and hacking. However, the report did not provide specific numbers or statistics on the prevalence of revenge porn in Greece. It's important to note that due to the sensitive and personal nature of revenge porn, many cases go unreported, and statistics may not fully capture the extent of the problem. Additionally, laws and policies related to revenge porn can vary widely between countries, which can make it difficult to compare statistics across different regions.

According to a study published by the National School of Public Health in Greece in 2016, the prevalence of problem gambling in Greece was estimated to be around 3.5% of the adult population. This study also found that 1.2% of the adult population in Greece met the diagnostic criteria for pathological gambling, which is the most severe form of gambling addiction.

Another study published in 2018 by the Hellenic Gaming Commission found that the percentage of Greeks with gambling problems had risen from 0.6% in 2011 to 1.5% in 2017. This study also found that men were more likely to experience gambling problems than women, and that online gambling was becoming increasingly popular among Greek gamblers (Economou et al., 2019).

A study published by the European Commission in 2018 found that Greece had one of the highest rates of people who said they had been exposed to fake news in the EU, with 62% of Greeks reporting that they had encountered fake news online. Additionally, a study published by the Reuters Institute for the Study of Journalism in 2019 found that Greece had a relatively high level of trust in news overall, with 54% of Greeks saying they trusted the news in general. However, the study also found that trust in social media as a news source was very low, with only 16% of Greeks saying they trusted news on social media.

In terms of specific examples of fake news in Greece, a report by the Hellenic Foundation for European and Foreign Policy (ELIAMEP) published in 2018 identified several instances of fake news circulating in Greece, including false claims about government policies, fabricated stories about crime and public health, and misinformation about the refugee crisis. It's worth noting that fake news can be difficult to define and measure, and statistics on the issue can vary depending on the source and methodology used. Additionally, the spread of fake news can be influenced by a range of factors, including social and political context, media literacy, and the prevalence of social media and online platforms.

Studies conducted in Greece have revealed that the majority of young people spend an average of 90 minutes per day online, while at least 10% of adolescents spend more than three hours online daily (Haddon et al. 2012; Makri-Botsari and Karagianni 2014). This excessive and potentially risky behavior online among Greek youth appears to be worsened by the limited discussions of online safety with parents and teachers compared to data from other countries (Athanasiades et al. 2015). In the Greek context, there is a lack of recent research data about young people’s social media practices. The vast majority of Greek youth are using social media platforms, in accordance to similar findings from the European context (EU Kids Online, 2012). The communicational and informational uses of social media platforms are among the most popular types of social media practices.

According to official statistics, in Greece, 67% of 10-11 year-olds (4th, 5th and 6th grade in primary education) and 78% of 12-15 year-olds (1st, 2nd, 3rd grade of gymnasio) were internet users in 2008. Almost half of the young people go online on a weekly basis, with younger children using the internet slightly more (47%) than older ones (43%). However, daily internet use reverses this trend, with only 16% of 10-11 year-olds online compared to 41% of 12-15 year-olds. Gender differences in internet use are decreasing, with girls using the internet slightly more than boys (76%:70%).

Boys tend to use the internet more than girls on a daily basis (39%:33%), but girls use it more on a weekly basis (43% of boys vs. 46% of girls) (Greek Observatory for the Information Society, 2008). Home is the main location for internet access for two-thirds of children, followed by school (27%). However, interestingly, 21% of children access the internet from an internet café, and 20% from a friend's or relative's house, which raises concerns about supervision and potential risks (Greek Observatory for the Information Society, 2008). There is a lack of Greek academic research on social networking practices of young children and teenagers. However, it appears that children and teenagers in Greece are not particularly fond of social networking sites. The uptake of social networking is significantly lower in the younger age group, but increases with older teens. Gender differences in online activity are decreasing, with girls showing a relatively stronger preference for social networking compared to boys, a trend that increases with age. Almost 35% of girls aged between 15-18 have created an SNS profile compared to 30% of their male peers.

Until the 2010s, ICT penetration in Greece was low, but this trend rapidly changed with potentially problematic behaviors such as cyberbullying becoming more prevalent due to increased ICT use, especially among young people (Hasebrink, Livingstone, & Haddon, 2008). As cyberbullying can have damaging consequences, systematic research on this issue is necessary, particularly for youth who are heavy ICT users (Hinduja & Patchin, 2009). Greece is a country with great geographical diversification, including densely populated urban areas, remote rural areas, and small islands across the Aegean and the Ionian seas. Despite similarities with other Mediterranean countries in terms of ICT advances, such as Italy, Spain, and Cyprus, there is a lack of systematic research evidence regarding cyberbullying in Greece, which makes mutual comparisons challenging (Mora-Merchán & Jäger, 2011). The rapid advances in technology have also left a gap in regulations that should respond to the nation's needs in terms of ICT threats. A study and codification of empirical and sociological assets is needed to address these issues (Nouskalis, 2012). Additionally, Greece's recent economic development, ongoing economic crisis, and high risk of economic recession have impacted the national, social, and cultural context, including an increase in violence among youth (e.g., Kalliotis, 2000).

According to the uses and gratifications theory, people with high economic capital (i.e. higher socio-economic status) may use the Internet more “effectively” (e.g. for educational purposes), in a way, which reinforces their economic, social and cultural capital and resources (Van Deursen & Van Dijk, 2014). On the contrary, people with a weak economic capital status (i.e., low-income and low educational level), usually do not use the Internet “effectively” (e.g. they use it only for entertainment purposes).

This inequality has the potential to be passed down to future generations. Sianou-Kyrgiou and Tsiplakides (2012) found in their earlier research on first-year students at the University of Ioannina and TEI Epirus that diversification in internet use is linked to the socio-economic status of parents, specifically their education level and proficiency in the English language. Huyer and Sikoska (2003) found similar results. Young people's internet use is influenced by the stimuli they receive from their family and friends, as well as their family's social status. Children from middle or upper-class families are more likely to be familiar with the internet compared to children from poor families. Knowledge of English is also a significant factor (Huyer & Sikoska, 2003). Children whose parents are proficient in foreign languages, especially English, are more likely to use the internet than those whose parents have lower levels of education.

The internet and social networks have become an essential part of daily life for a significant part of the global population due to their enormous communication capabilities. The number of internet users worldwide has grown from almost one billion in 2010 to 2.8 billion in 2019 (Clement, 2019), leading to a significant increase in the flow of information exchange. However, this information also poses a risk to personal and digital security. The Cambridge Analytica scandal in 2014 is one example of the potential dangers of internet use, highlighting the risks involved in violating the privacy of social networking sites (SNS) users, which is not necessarily guaranteed despite the terms of use privacy policies of SNSs (Todd, 2018; González-Bailón, 2018). The breach of personal data of users is a concern that accompanies the use of social networking sites by both users and researchers ("Today's social network sites," 2017).

There are four categories of risks affecting social network users, the first of which is privacy and security risks (classic threats). The second category involves new risks affecting social networking infrastructure, including threats that undermine the privacy and security of social media users. The third category combines threats from the previous two categories, resulting in greater risks. The fourth category mainly deals with risks related to children, such as cyberbullying, invasion of privacy, and offensive content through social media (Fire et al., 2014).

Classic threats involve attackers using personal information provided on social networks to attack users and their friends using malware, spam, phishing attacks, spammers, cross-site scripting, and internet scams. Such risks, although not new, continue to be a major problem, especially due to the structure and nature of social networks. Modern threats aim to expose the personal information of users and their contacts, such as fake profiles, identity clone attacks, location leakage, and socware. Combined threats involve combining old and new forms of threats, such as using internet phishing to extract passwords or security codes and then posting a message on a user's log (clickjacking), prompting them to click on the post and install a hidden virus on their computer (Fire et al., 2014).

Children and adolescents are particularly vulnerable to social networking risks, such as online predators, risky behaviors, and cyberbullying, which can have long-lasting negative effects. The risks of social networking sites are not limited to personal security, but also include privacy and ethical issues.

On the internet, as in everyday life, opportunities and risks are inextricably linked, since what constitutes an opportunity for some, may be a risk for others: for those who make friends online, there are others who risk encountering 'stranger danger', for those who seek information about sex or politics, there are those who may accidentally come across pornographic or racist content.

Studies indicate that there is a positive correlation between the benefits and risks that children experience when using the internet. This implies that as opportunities increase, so do risks, and vice versa (Livingstone, 2004; Livingstone and Helsper, 2008). The same applies to skills, where the more proficient and experienced a child is, the more likely they are to encounter opportunities and risks compared to less skilled users. Essentially, children with good internet skills are more likely to take advantage of opportunities online, which also means that they are more exposed to online risks.

Moreover, there is evidence of a significant rise in reported experiences of cyberbullying through the internet over the last few years (Floros et al. 2013). Cyberbullying refers to the use of technology to harass, intimidate, or harm others. It involves using electronic devices, such as smartphones, computers, or social media platforms, to spread rumors, make threats, send hurtful messages or images, or engage in other forms of aggressive or harassing behavior. Cyberbullying can take many forms, including sending harassing or threatening messages via text or social media, sharing embarrassing or private photos or videos without permission, spreading rumors or gossip online, or creating fake profiles or accounts to impersonate or harass others.

However, epidemiology of cyberbullying among adolescents in Greece is like that of other western countries, with percentages ranging from 3 to 20 % for the victims and from 2 to 25 % for the bullies, depending on the type and frequency of cyberbullying and cybervictimization (Athanasiades et al. 2015; Kapatzia 2008; Tsorbatzoudis and Aggelakopoulos 2012). Research suggests that young people engage in a variety of communicational, informational, and creative practices on social media platforms. Social media constitutes a space where they navigate relationships and express themselves. Thus, their social media practices relate directly to their everyday experiences which contribute to the shaping of their identities (Haddon et al., 2012).

Social media practices have been linked to various factors such as gender, school type, parental education, and ethnicity. These social locations are thought to influence the way young people use social media and how it shapes their identities and aspirations. A study on internet use in Greece found that 66% of 9-12-year-olds access the internet using mobile devices, which is the highest rate compared to other European countries where the average is 22%. Additionally, 56% of Greek children in this age group use the internet on a daily basis. Regarding social media use, 33% of 9-year-olds and 70% of teenagers (13-16 years old) use social networking platforms. The study also found that Greek children and teenagers are among the most active Facebook users in Europe, after Italians and Cypriots, with 65% of teenagers and 31% of young children in Greece reporting that they have used Facebook (Haddon et al., 2012).

Research indicates that the COVID-19 pandemic has led to a significant increase in the amount of time young people spend online.

With the shift to remote learning and social distancing measures, many young people have had to rely on digital platforms and technologies to stay connected with friends and family, as well as to continue their education. A study by Common Sense Media found that in the United States, the average amount of time children and teenagers spent on digital devices increased by almost 50% during the pandemic, with many spending more than 7 hours a day online (Rideout, V., & Fox, S., 2020).

Similarly, a survey conducted by Ofcom in the UK found that 71% of children aged 5-15 were spending more time online since the start of the pandemic, with many using the internet for socializing, entertainment, and education (Ofcom., 2020).

While increased internet use can provide many benefits, such as access to educational resources and social support, it can also pose risks such as cyberbullying, exposure to harmful content, and addiction. As such, it is important for parents and caregivers to monitor and regulate children's internet use, and for educators and policymakers to provide guidance and resources for safe and responsible online behavior.

According to a report by the European Commission in 2020, Greece has a relatively high incidence of credit card fraud, which is one of the most common forms of identity theft. In addition, the report noted that there has been an increase in phishing attacks and other forms of online fraud in Greece in recent years.

The Hellenic Data Protection Authority (HDPA) is the supervisory authority for data protection in Greece, and it provides guidance and support to individuals who have been victims of identity theft. The HDPA also works closely with law enforcement agencies to investigate and prosecute cases of identity theft and other cybercrimes.

Overall, while specific statistics on identity theft trends in Greece may be limited, it is clear that the issue is a growing concern and that measures are being taken to address it. It is important for individuals to take steps to protect their personal information and be aware of the potential risks of identity theft, both in Greece and elsewhere.

According to a survey conducted by the Hellenic Institute of Communications and Information (E.I.E.P.), 18.8% of respondents reported that they knew someone who had been a victim of revenge porn. The survey also found that social media platforms such as Facebook, Instagram, and Snapchat were among the most common ways that revenge porn was shared.

In response to the growing concern around revenge porn, Greece introduced a new law in 2019 that makes it a criminal offense to share sexually explicit images or videos without the consent of the person depicted. The law provides for fines and imprisonment for those found guilty of this offense, and it also includes provisions for the removal of such content from online platforms.

The Hellenic Data Protection Authority (HDPA) is also involved in efforts to combat revenge porn in Greece. The HDPA provides guidance and support to individuals who have been victims of this type of abuse, and it works with law enforcement agencies to investigate and prosecute cases of revenge porn and other forms of online abuse.

Overall, while data on revenge porn trends in Greece may be limited, it is clear that this is a growing problem that requires attention and action. The introduction of new laws and the involvement of organizations such as the HDPA are positive steps towards addressing this issue and protecting the rights and privacy of individuals.

Like many countries around the world, Greece has also faced the issue of fake news and misinformation in recent years. The spread of false information can have a significant impact on public opinion, political and social stability, and the overall democratic process.

In Greece, one of the most notable cases of the spread of fake news occurred during the economic crisis that began in 2009. A significant amount of false information was disseminated through social media platforms and other online sources, which contributed to widespread panic and confusion.

More recently, in the context of the COVID-19 pandemic, there have been reports of false information and conspiracy theories circulating in Greece, such as misinformation about the safety and effectiveness of vaccines.

To address the issue of fake news, Greece has introduced a number of measures. In 2018, Greece established the National Council for Radio and Television (NCRTV), which is responsible for regulating broadcasting content and ensuring the accuracy and impartiality of news reporting.

In addition, the Greek government has launched awareness campaigns to educate the public on how to identify and avoid false information, and it has also worked with social media platforms to remove fake news and misinformation from their sites.

However, despite these efforts, the problem of fake news and misinformation continues to be a concern in Greece and around the world. It is important for individuals to be vigilant in their consumption of news and information, and to rely on credible sources when seeking information on important issues.

Identity theft refers to the fraudulent acquisition and use of someone else's personal information, such as their name, address, date of birth, Social Security number, or bank account details, for financial gain or other illegal purposes. The perpetrator of identity theft may use this information to obtain credit, apply for loans or benefits, make unauthorized purchases, or even commit crimes using the stolen identity. Identity theft is a serious crime and can cause significant financial and emotional harm to the victim.

Identity theft can manifest in various patterns, including:

- Financial identity theft: where the perpetrator uses the victim's identity to obtain financial gain, such as opening a credit card account or taking out a loan.
- Criminal identity theft: where the perpetrator uses the victim's identity when committing a crime.
- Medical identity theft: where the perpetrator uses the victim's identity to receive medical treatment, prescription drugs or to file false insurance claims.
- Synthetic identity theft: where the perpetrator creates a new identity by combining real and fake information to open new accounts.
- Government identity theft: where the perpetrator uses the victim's identity to obtain government benefits or documents, such as passports or driver's licenses.
- Child identity theft: where the perpetrator uses a child's identity to open credit accounts or apply for government benefits.

Revenge porn, also known as non-consensual pornography or image-based abuse, refers to the sharing or distribution of sexually explicit images or videos of an individual without their consent, typically with the intention of causing harm or embarrassment. It involves the unauthorized sharing of private or intimate images, often taken within the context of a relationship, and can have serious consequences for the victim's mental health, personal relationships, and professional reputation. Revenge porn is considered a form of sexual harassment and is illegal in many jurisdictions.

Revenge porn typically involves the distribution of sexually explicit images or videos of a person without their consent. The pattern for manifestation of revenge porn can involve the following steps:

- The victim is in a consensual intimate relationship with the perpetrator and shares sexually explicit material, such as images or videos, with them.
- The perpetrator, following a breakup or in an attempt to gain revenge, distributes the material online or through other means without the victim's consent.
- The material is often posted on social media, websites, or shared through messaging apps, and may be accompanied by personal information about the victim, such as their full name, address, or workplace.

- The victim may experience significant harm to their reputation, relationships, and mental health, as well as facing the possibility of harassment, stalking, or even physical violence.
- Legal action can be taken against the perpetrator, with many countries having introduced specific laws to criminalize the act of revenge porn.

Fake news refers to deliberately misleading or fabricated information presented as if it were real news. The term is often used to describe intentionally false or misleading stories that are spread through traditional or social media, with the aim of deceiving people for political or financial gain. Fake news can be presented in various formats such as articles, videos, images or social media posts, and can be shared through various means, including email, social media platforms, messaging apps, or websites. It can be difficult to distinguish fake news from legitimate news, and its widespread dissemination can have significant negative impacts on individuals and society as a whole, including influencing public opinion, undermining trust in media, and even impacting elections or other important decisions.

Fake news can manifest in several patterns. One common pattern is the deliberate creation and dissemination of false or misleading information, often with a political or social agenda. This can be done through the use of fabricated news stories, manipulated images or videos, or misleading headlines designed to attract clicks and shares on social media. Another pattern is the dissemination of information that is technically true but taken out of context, distorted, or otherwise presented in a way that creates a false impression. This can include selectively quoting a source or presenting statistics in a misleading manner. Fake news can also be spread through the use of bots or other automated accounts on social media platforms, which can amplify false information and make it appear more widespread than it actually is. Finally, fake news can also be spread through the use of echo chambers and filter bubbles, where people are exposed only to information that confirms their existing beliefs and biases, and are less likely to be exposed to information that challenges or contradicts those beliefs.

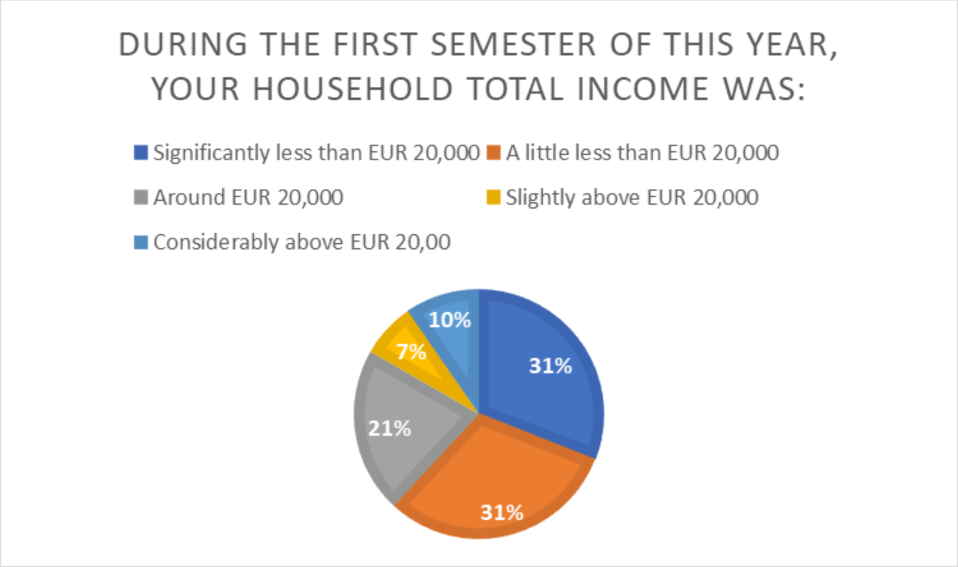
Analysis of the data

Presentation of the survey results

Demographic characteristics

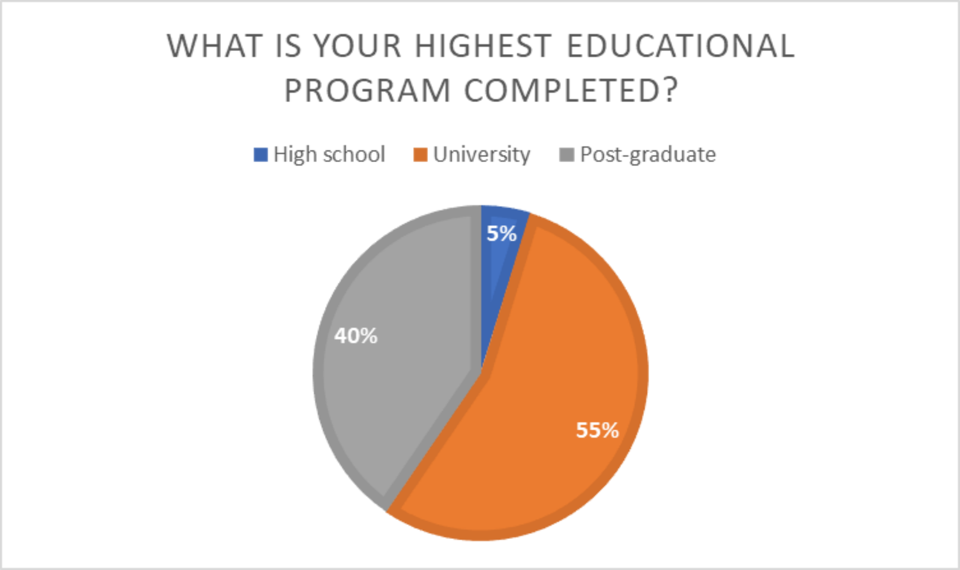
Out of the 42 survey respondents, 15 were aged 23-26, 7 were aged 27-30, 18 were aged 19-22, and 2 were aged 16-18. Regarding gender, 21 participants were female, and 21 were male.

Regarding household income, 31% of the respondents reported a total income of "significantly less than EUR 20,000" per semester, 31% reported "a little less than EUR 20,000," and 21% reported "around EUR 20,000." Only 7% of the respondents reported an income higher than EUR 20,000, with 10% reporting "slightly above EUR 20,000" and 4 reporting "considerably above EUR 20,000."



Regarding residence, 20 respondents live in an urban area with a population of 41,000-51,000 people, while 22 live in an urban area with a population of 20,000-44,000 people.

In terms of education, 40% of the respondents have completed a post-graduate program, 55% have a university degree, and 5% are high-school graduates.



Regarding occupational status, 8 respondents are employees, 24 are students, 8 are self-employed, and only 2 are unemployed.

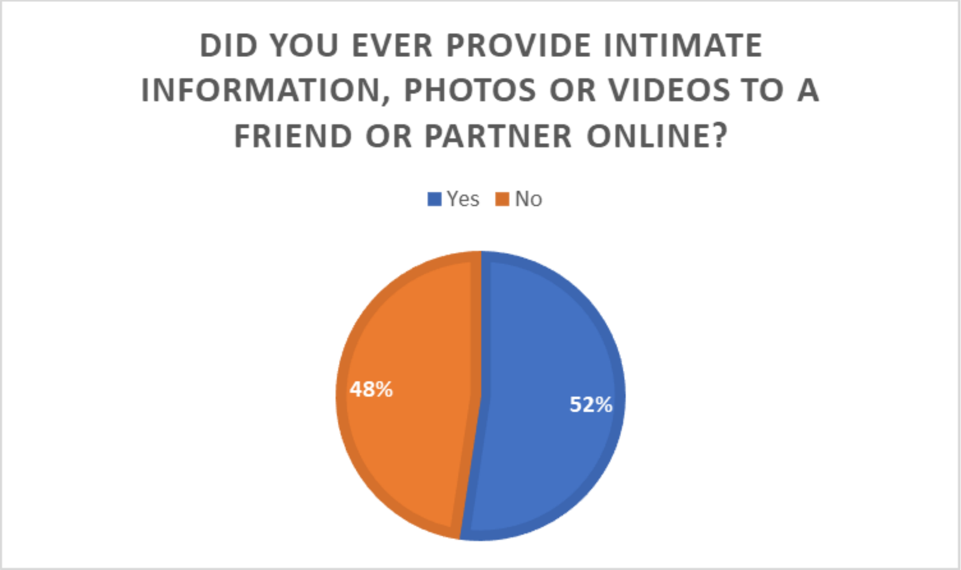
Regarding ethnicity, 31 respondents are Greek, while 11 respondents identified as "other."

Concerning internet use, 32 respondents access the internet daily, while 10 respondent access it several times a week.

Risky and preventive behavior

On the question of providing information to strangers online with whom they have no institutional affiliation, 31% of the respondents replied that they have shared no information and 14% have shared identification information and information about their location among other.

A total of 22 respondents (52%) shared intimate information, photos, or videos with a friend or partner online.



Manifestation of online risks

In terms of online incidents, 21 respondents (50%) reported never being victims of cybercrime. Among those who experienced online incidents, 6 fell victim to online harassment or trolling, and 2 fell victim to cyberstalking.

The data obtained from the survey with young people indicates that a significant number of respondents are cautious about sharing personal information with strangers online, yet a considerable number still share specific information. However, when it comes to sharing personal information with people they know, such as friends and family, a high percentage of respondents reported providing intimate information, photos, or videos.

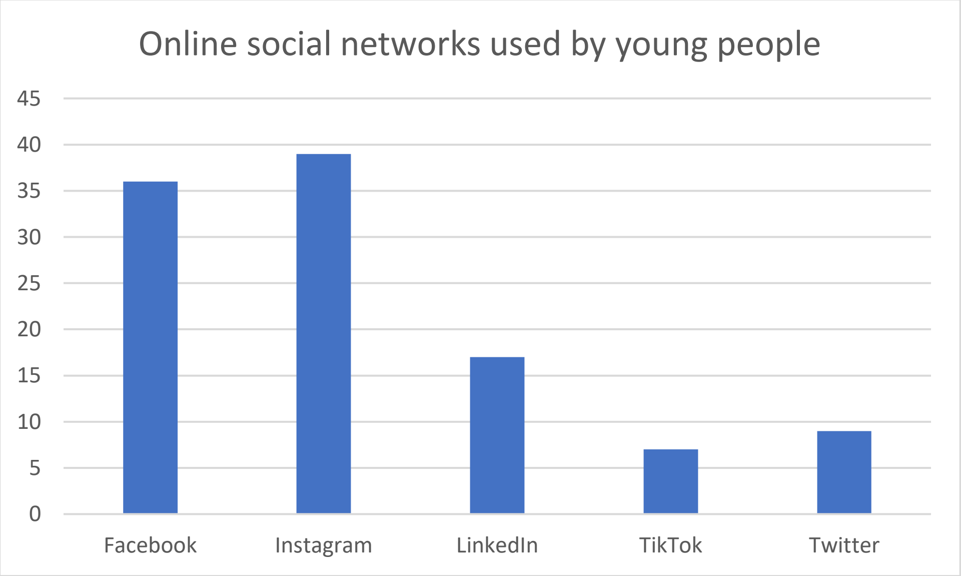
Gender seems to play a role in the type of cybercrime experienced by respondents. Females were slightly more likely than males to experience online harassment, while males were more likely to be targets of cyberbullying and online threats. TikTok appears to be more female-oriented, while a similar number of males and females use social media such as Instagram, Facebook, and LinkedIn.

Online activity

Regarding online activities, 36 respondents search for information, 34 chat with friends and family, 28 shop, 36 watch movies or listen to music, 24read political and current events news, 18 participate in educational programs or work from home, 26 play games, and 17 participate in online discussions. Only a few respondents search for friends or partners (12) and blog or vlog (8), while none reported practicing online gambling.

However, in response to a question about engaging in gambling in the past two years, 7 individuals confirmed that they had, while 35 noted that they had not.

Concerning social network usage, 39 respondents use Instagram, 36 use Facebook, 17 use LinkedIn, 7 use TikTok, and 9 use Twitter.



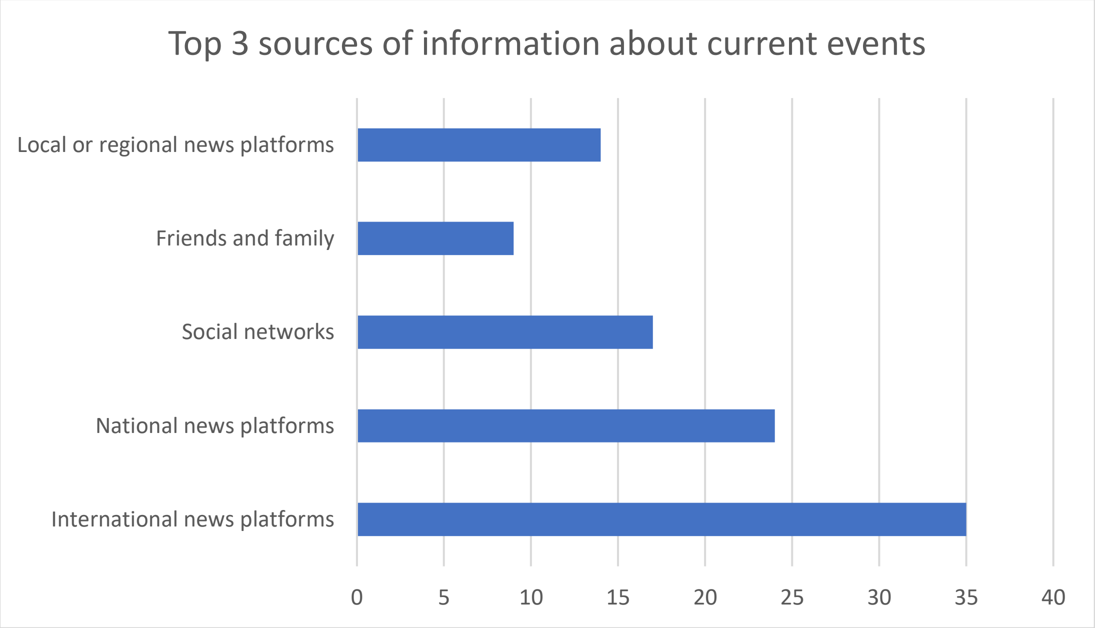
Fake news

With regard to reading news about politics and current events, 16 respondents read the news on a daily basis, while 14 individuals read them once every few days. 10 respondents read the news once a week, and 2 read them once a month. Interestingly, 63% of respondents mentioned that they only read the title and the first paragraph, while only 27% read the whole article.

Regarding political orientation, 12 respondents identified as moderate left-wing, 17 as apolitical or not interested in politics, 7 as moderate right-wing, and 6 were uncertain of their political orientation.

86% of respondents never comment on news platforms, while 14% comment once a week.

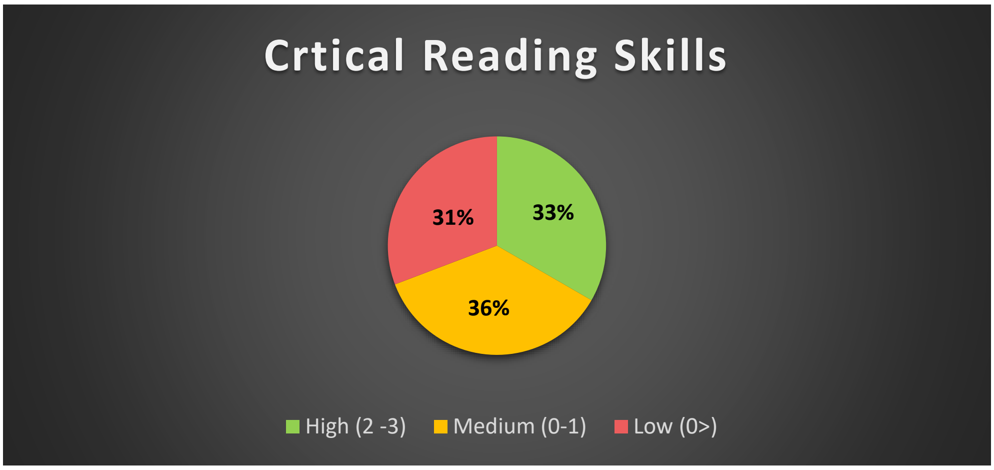
Concerning the top sources of information on politics and current events, 35 respondents rely on international news platforms, 24 read national news platforms, and 17 use social networks. Additionally, 9 individuals learn information from friends and family, and 14 people from local or regional news platforms.



The analysis of responses related to reading news about politics suggests that those who read the news every day tend to read the entire article or at least the title and first paragraph.

No connection between political orientation and fake news was found in our survey.

The majority of participants displayed good critical reding skills and this have the ability to understand the meaning of the text. However, there were some cases where the participants demonstrated low critical thinking skills. Age could potentially be a factor influencing critical thinking skills, as it appears that most respondents with higher scores were aged 23-30. However, the number of respondents in the younger age groups was limited, and no conclusions could be drawn.



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

The interviewees noted that young people are often careless and unaware of the risks involved in their online behavior, but are also more aware of different aspects of society due to their online access.

The COVID-19 pandemic has had a significant impact on youth online behavior, leading to increased exposure to hate comments and an increased reliance on the online environment due to lockdowns.

The interviewees discussed the factors that influence young people's willingness to share personal information online, including a lack of distinction between the virtual and real worlds, peer pressure, and a perception that sending intimate media content is the norm. They also noted that young people are often victims of online incidents due to a lack of education on how to behave in online environments and protect themselves.

According to the interviewees, fake news can spread false or misleading information, which can lead individuals to make decisions based on inaccurate or incomplete information. Moreover, fake news can contribute to polarization and division within society by spreading biased or extremist views, and by encouraging individuals to seek out only information that confirms their existing beliefs.

The interviewees identified the need for media literacy and online literacy courses, specific training on harassment and hate speech, education on human rights and sensitivity to issues related to sexual orientation and gender, and workshops on critical thinking, online behavior, and website safety. They also stressed the importance of a holistic approach to education on these topics, involving schools, television, and society as a whole.

Conclusions

The absence of preventive campaigns and education, such as internet and sexual education, as well as training to enhance critical reading skills, contributes to the emergence of several online risks that are associated with youth activities. These risks include but are not limited to identity theft, online gaming/gambling addiction, cyberbullying, the spread of fake news and misinformation, and revenge porn or other forms of image-based sexual abuse.

Some young people share personal information online, with a higher percentage sharing with people they know. Gender plays a role in the type of cybercrime experienced.

The majority of respondents read news about politics and displayed good critical thinking skills. The interviewees noted that young people are unawareness of risks in online behavior. They also mentioned the impact of the COVID-19 pandemic and the need for education on media literacy, harassment, human rights, and critical thinking, involving schools, television, and society.

Recommendations

To enhance training in this area, it is advisable to engage professionals like psychologists, as well as influencers and individuals who can share personal experiences or connect with the audience. Participatory teaching methods and non-formal education techniques should be utilized to actively involve young people. Moreover, the information should be presented in a manner that directly involves and relates to young people, fostering a sense of connection to the content.

Training for youth workers, trainers and parents is also necessary, so that they are better prepared to react and handle risks, to supervise online activity where required and better understand the context and risks coming together with online behavior.

It is advisable to incorporate practical instances and real-life situations into online learning resources like e-learning platforms and games to better illustrate the potential dangers to young individuals. The technical features should be optimized for mobile devices, unless there are other primary devices used by the target audience to access the internet. Games should also include avatars and social rewards that appeal to young people, such as the option to share online. To maximize engagement, educational games may be more effective when played individually rather than in a group setting.

To promote safe and responsible online behavior among young people, it is important to take a multi-faceted approach. This can include educating youth on online safety and the risks associated with online behavior, as well as encouraging responsible digital citizenship and modeling positive behavior. Setting boundaries around online use can also help young people maintain a healthy balance between their online and offline lives. Additionally, promoting media literacy skills can help young people navigate the complex world of online information and avoid falling prey to false or misleading content. By working together to create a healthy and informed online culture, we can help young people develop the skills and habits they need to succeed in the digital world while minimizing the risks associated with online behavior.

Recommendations per category of online risks for youth:

1. **Cyberbullying**:

- Educate youth on the harmful effects of cyberbullying and how to report it.
- Encourage young people to practice empathy and respect in online interactions.
- Encourage youth to seek help and support from a trusted adult if they are experiencing cyberbullying.
- Promote positive online behavior and encourage youth to be an ally for those who are being bullied.

2. Image-based sexual abuse:

- Educate youth on the risks of sharing personal information and images online.
- Encourage young people to seek out age-appropriate and safe online communities.
- Teach youth how to block and report inappropriate content or contacts.

3. Online predators:

- Educate youth on the tactics used by online predators and how to avoid them.
- Encourage young people to only communicate with people they know in real life and to be cautious of online strangers.
- Teach youth how to block and report suspicious or inappropriate online contacts.
- Set privacy settings on social media profiles to limit the amount of personal information that is visible to strangers.

4. Addiction:

- Encourage young people to take breaks from screens and engage in offline activities.
- Model healthy technology use and limit screen time in the household.
- Encourage young people to seek help if they are struggling with addiction.
- Promote offline activities and hobbies that promote well-being, such as exercise and socializing with friends in person.

5. Privacy and security:

- Educate youth on the importance of strong passwords and how to protect their personal information.
- Encourage young people to be cautious of phishing attempts and to avoid clicking on suspicious links or downloading unknown files.
- Teach youth how to set privacy settings on social media profiles and to limit the amount of personal information that is shared online.
- Promote safe and responsible online behavior, such as avoiding sharing personal information or images online.

References

Antoniadou, Nafsika, and Constantinos M. Kokkinos. 2015. “A Review of Research on Cyber-Bullying in Greece.” *International Journal of Adolescence and Youth* 20 (2): 185–201. https://doi.org/10.1080/02673843.2013.778207.

———. 2018. “Empathy in Traditional and Cyber Bullying/Victimization Involvement From Early to Middle Adolescence: A Cross Sectional Study.” *Journal of Educational and Developmental Psychology* 8 (1): 153. https://doi.org/10.5539/jedp.v8n1p153.

Aslanidou, Sofia, and George Menexes. 2008. “Youth and the Internet: Uses and Practices in the Home.” *Computers & Education* 51 (3): 1375–91. https://doi.org/10.1016/j.compedu.2007.12.003.

Athanasiades, Christina, Anna Costanza Baldry, Theocharis Kamariotis, Marialena Kostouli, and Anastasia Psalti. 2016. “The ‘Net’ of the Internet: Risk Factors for Cyberbullying among Secondary-School Students in Greece.” *European Journal on Criminal Policy and Research* 22 (2): 301–17. https://doi.org/10.1007/s10610-016-9303-4.

Athanasiades, Christina, Harris Kamariotis, Anastasia Psalti, Anna C Baldry, and Anna Sorrentino. n.d. “INTERNET USE AND CYBERBULLYING AMONG ADOLESCENT STUDENTS IN GREECE: THE ‘TABBY’ PROJECT,” 27.

Barkoukis, Vassilis, Lambros Lazuras, Despoina Ourda, and Haralambos Tsorbatzoudis. 2016. “Tackling Psychosocial Risk Factors for Adolescent Cyberbullying: Evidence from a School-Based Intervention: A School-Based Intervention Against Cyberbullying.” *Aggressive Behavior* 42 (2): 114–22. https://doi.org/10.1002/ab.21625.

Best, Paul, Roger Manktelow, and Brian Taylor. 2014. “Online Communication, Social Media and Adolescent Wellbeing: A Systematic Narrative Review.” *Children and Youth Services Review* 41 (June): 27–36. https://doi.org/10.1016/j.childyouth.2014.03.001.

Economou, M., Souliotis, K., Malliori, M., Peppou, L. E., Kontoangelos, K., Lazaratou, H., Anagnostopoulos, D., Golna, C., Dimitriadis, G., Papadimitriou, G., & Papageorgiou, C. (2019). Problem Gambling in Greece: Prevalence and Risk Factors During the Financial Crisis. Journal of gambling studies, 35(4), 1193–1210. https://doi.org/10.1007/s10899-019-09843-2

Gounopoulos, Elias, Stavros Valsamidis, Ioannis Kazanidis, and Sotirios Kontogiannis. 2020. “A Longitudinal Analysis of Internet Use. The Case of Greece.” *International Journal of Society Systems Science* 12 (3): 198. https://doi.org/10.1504/IJSSS.2020.111344.

Magkos, Emmanouil, Eleni Kleisiari, Panagiotis Chanias, and Viktor Giannakouris-Salalidis. n.d. “Parental Control and Children’s Internet Safety: The Good, the Bad and the Ugly,” 18.

Nikolopoulou, Myrto. n.d. “Young People’s Social Media Practices in Greece: Developing Identities Online and Shaping Future Aspirations,” 329.

Siafarika, Evangelia, Elisabeth Andrie, Chara Tzavara, Athanasios Thirios, Loretta Thomaidis, and Maria Tsolia. 2021. “High Risk Internet Behaviors and Psychosocial

Well-Being among Greek Preadolescents." *Developmental and Adolescent Health*, October. https://doi.org/10.54088/678j.

Stratigopoulou, Eleni, Klimis Ntalianis, Vasiliki Kikili, and Filotheos Ntalianis. 2020. "Risks Inherent in Inaccurate or Inadvertent Use of Social Networks in Greece." *International Journal of Education and Information Technologies* 14 (November): 108–14. https://doi.org/10.46300/9109.2020.14.13.

Tsitsika, Artemis K., Eleni C. Tzavela, Mari Janikian, Kjartan Ólafsson, Andreea Iordache, Tim Michaël Schoenmakers, Chara Tzavara, and Clive Richardson. 2014. "Online Social Networking in Adolescence: Patterns of Use in Six European Countries and Links With Psychosocial Functioning." *Journal of Adolescent Health* 55 (1): 141–47. https://doi.org/10.1016/j.jadohealth.2013.11.010.

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.vitecoelearning.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 Centrul 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.