Tools4LEAs

**A project of the European Anti-Cybercrime Technology Development Association (EACTDA)**

EACTDA

# Dx.y Title-of-the-deliverable

Co-funded by the European Union

| | | |
|---|---|---|
| **Version:** | 0.1 | |
| **Delivery date:** | Month Year (e.g., July 2021) | |
| **Dissemination level:** | Public<br>or<br>CONFIDENTIAL (only for members of the consortium; including the Commission services) | |
| **Status** | DRAFT | |
| **Nature:** | Report | |
| **Main author(s):** | Full-name | EACTDA |
| **Contributor(s):** | | |
| | | |
| | | |

**DOCUMENT CONTROL**

| Version | Date | Author(s) | Change(s) |
|---|---|---|---|
| 0.1 | dd/mm/yyyy | Full-name (EACTDA) | TOC and initial text |
| 0.2 | dd/mm/yyyy | Full-name (EACTDA) | First version for all sections completed. Requested contributions from EACTDA members and key stakeholders. |
| 0.3 | dd/mm/yyyy | Full-name (EACTDA) | Updated with received feedback |
| 1.0 | dd/mm/yyyy | Full-name (EACTDA) | Final version, ready to be submitted |



Co-funded by the European Union

TABLE OF CONTENTS





Co-funded by the European Union

Co-funded by the European Union

# 1. Introduction

## 1.1. Overview of the Tools4LEAs project

EACTDA is the acronym of the European Anti-Cybercrime Technology Development Association, which is a private non-profit association, established in San Sebastian, Spain. The members of the Association include European Union (EU) public entities fighting cybercrime, universities and research technology organisations, for-profit private companies, and other relevant actors in the field of the EU security research and innovation.

The Tools4LEAs projects are a series of projects that receive a Direct Award under the ISFP programme, and which main goal is to facilitate and promote the uptake of innovative technologies by EU public entities fighting cybercrime. EACTDA, via the Tools4LEAs projects, aims at further developing pre-existing assets, mainly from EU-funded security research and development projects, so that they are offered with no license cost and with access to the source code to EU public entities fighting cybercrime.

In the first Tools4LEAs project (v1; Jul'21 to Jun'23), the focus was on designing and setting up the infrastructures, processes, and governance / decision-making mechanisms, whilst delivering the first set of "fully-tested and operational-ready" tools via Europol's Tool Repository. Though 11 tools were further developed in the v1 project, it is expected that 3 of them will not be released to their targeted audience as they do not pass the pre-established quality threshold of "operational-ready". Also, an End-User Advisory Board (EUAB) composed as of Jul'23 by 23 members from 14 EU member states and co-chaired by two Europol units (EC3 and Innovation Lab) was established and it is the body responsible for identifying and prioritising end-user needs and which has veto right over the decisions done by EACTDA/Tools4LEAs with regard to the tool development roadmap.

In the second Tools4LEAs project (v2; Jul'23 to Jun'25), it is proposed to double the number of tools delivered. Also, the repository of tools implemented in v1, and currently used to host the results of the Tools4LEAs projects, will be enhanced and reused to host the results of EU-funded security research projects (when relevant in the field of cybercrime). EACTDA will play the role of custodian of these results, and the technical, IPR, and administrative aspects needed to create this new repository of security research results will be put in place. In addition, the v2 project will include a pilot to proof the concept of initial and limited support&maintenance periods for a selection of tools. Besides, a pilot of the concept of EACTDA national nodes will be included, with nodes planned in LT, FR, ES, and maybe one or two more. Also, a platform for end-users to evaluate online tools will be implemented. Finally, the v2 project will include activities to further build the community of Tools4LEAs stakeholders and to promote the creation and/or adoption of technical blueprints, and in general, of commonly accepted best practices.

## 1.2. Main objective of this document

Nowadays, a wide range of cyber threats exist that affect a significant portion of the global population. Several groups within society remain unaware of these threats and of the potential risks they pose, particularly adolescents and minors aged between 10 and 16 years. Identified risk factors may increase the prevalence of cyber threats. To examine these risks, the present study utilizes a serious game called RAYUELA, together with the collection of sociodemographic data and questionnaires related to external support and prior experiences of cyberbullying.



Co-funded by the European Union

This deliverable presents an exploratory analysis of data collected during the first edition of the Cybersecure Mission (2024–2025), involving a sample of 5432 participants. The analysis focuses on the prevalence and risk factors associated with four key cyber threats: cyberbullying (CB), phishing, online grooming (OG), and the sharing or spreading of fake news (FNs). The methodology is innovative, combining data collection with an interactive and engaging video game experience. The purpose of this deliverable is to use these data to better understand how different forms of digital victimization occur among minors, and to identify the psychological, behavioral, and contextual factors that place them at greater risk. Ultimately, this work aims to lay the foundation for a comprehensive interdisciplinary analysis of digital threats affecting young people.

In the contemporary digital era, minors are deeply embedded in online environments that shape their socialization, education, and personal identity. Emerging vectors—such as social media platforms, the so-called "manosphere," artificial intelligence tools, and gamified learning environments—are transforming both how young people may be recruited into crime and how they may become victims of online harm (Bokolo & Liu, 2024; Wolbers et al., 2025; Franklin-Paddock et al., 2025). While these digital spaces provide unprecedented opportunities for connection and learning, they also expose young users to diverse and rapidly evolving threats. Among the most prevalent are cyberbullying, phishing, online grooming, and exposure to fake news, which together constitute a broad spectrum of cyber threats that significantly affect children and adolescents.

One of the primary objectives of this work is to support the development of prevention and awareness campaigns in schools aimed at mitigating these cyber threats. Many minors remain unaware of the harm their online behavior can cause to other minors or classmates. Education is therefore a key area of intervention, as fostering a safe environment in schools is essential. Families also play a crucial role, as minors' behavior across different social contexts is strongly influenced by their relationships with their parents or caregivers.

Targeted training programs can be implemented in schools to help identify vulnerabilities among minors and to promote critical evaluation of online content and interactions. In addition, the findings of this deliverable can inform policymaking within educational contexts, supporting the integration of child safety features, privacy protections, and transparent reporting systems. In cases where serious risks or harms are identified, law enforcement agents (LEAs) can be engaged to carry out appropriate interventions when necessary.

## 1.3. Relation to other deliverables

This deliverable is closely related to the following deliverable:

- **Dx.x PT Report**: Missão Cibersegura.??

## 1.4. Structure of the deliverable

Section 2 of this document provides a conceptual overview of several cyber threats affecting minors, with a particular focus on the Portuguese case study. Section 2.1 identifies the risk factors associated with the cyber threats examined.

Section 3 describes the methodology of this study, presenting an innovative and multidisciplinary approach that combines insights from psychology, criminology, and media studies. It focuses on the research design, sample, ethical approval, and data collection and analysis procedures.


Co-funded by the European Union

Section 4 presents the results of the exploratory analysis regarding the prevalence of different cyber threats and their associated risk factors.

Section 5 provides a brief discussion of the main findings for each cyber threat and the corresponding risk factors.

Finally, section 6 summarises which is the goal and key aspects of this document, and it acknowledges that there is still work to be done to improve the document.



Co-funded by the European Union

# 2. Conceptual Overview of Cyber Threats

Cyberbullying represents one of the most prevalent forms of online victimisation, defined by the intentional use of technological devices to harm or intimidate others (Slonje & Smith, 2008). Unlike traditional bullying, cyberbullying transcends physical and temporal boundaries, often resulting in persistent psychological harm such as anxiety, depression and diminished self-esteem (Waasdorp & Bradshaw, 2015).

A further and increasingly sophisticated threat to minors is phishing, a cybercrime that employs deceptive digital messages to obtain sensitive personal information, including passwords or financial details. Although traditionally associated with adult victims, recent research demonstrates that children are frequently targeted due to their limited awareness of online security and their tendency to trust digital communications (Ali et al., 2022). Exposure to phishing can lead not only to direct privacy violations, but also to broader harms such as identity theft and psychological distress following the realisation of deception.

Although less prevalent, online sexual grooming is nevertheless highly relevant due to the seriousness of the problem. Sexual grooming refers to a manipulative relational process through which an offender cultivates trust and psychological and emotional proximity with a vulnerable individual, typically a child or an at-risk adult, to facilitate sexual abuse or exploitation (Craven et al., 2006; Jeglic et al., 2023). The one addressed in this study refers to the exploitation of digital platforms by an adult, manipulating a child's trust to redefine their perceptions of safety and appropriate interaction, while subsequently leveraging fear and shame as mechanisms of control and secrecy.

Finally, the proliferation of fake news compounds shapes how young users perceive and interpret information. As minors increasingly consume news through social media, they often struggle to differentiate between reliable and false content, rendering them vulnerable to manipulation (Molina-Cañabate et al., 2023). This does not only affect information consumption. The fact that young people are increasingly unable to distinguish between false and true information also makes them more susceptible to manipulation, such as that underlying grooming or phishing. In addition, fake news can influence children’s attitudes, exacerbate polarization and undermine critical thinking skills.

Together, these phenomena—cyberbullying, phishing, online grooming and fake news—demonstrate the complex nature of cybercrime and its significance and impact in the lives of minors. Furthermore, these online threats are not static. Instead, they evolve alongside technological innovation, creating new and more complex challenges for young users. Therefore, it is essential to outline forward-looking prevention strategies, including enhanced education, robust regulatory frameworks and proactive monitoring mechanisms.

## 2.1. Common Risk Factors for Different Cyber Threats

Risk factors are individual, social and contextual conditions that increase the likelihood that minors will be exposed to or negatively affected by harmful online behaviours such as cyberbullying, phishing, online grooming and fake news. They do not determine that a negative outcome will occur, but they create vulnerabilities that make certain children and adolescents more susceptible to online risks. Understanding these factors is essential because they help identify which groups may require targeted support and allow for the development of more effective prevention and intervention strategies. In parallel, it is equally important to consider protective factors, which are the personal skills, social resources and environmental conditions that protect young people from harm and promote resilience in digital environments. Together, analysing both risk and protective factors provides a comprehensive


Co-funded by the European Union

framework for understanding minors' online experiences and for designing informed, evidence-based approaches to safeguarding them.

Risk factors associated with cyberbullying among minors are complex, including individual, social and contextual dimensions. At the individual level, adolescents with lower self-esteem and higher impulsivity are more likely to engage in or become victims of cyberbullying (Kowalski et al., 2019). Sociodemographic aspects such as gender, sexual orientation and migrant background have also been found to be risk factors (Reneses 2024b). Social environments characterised by conflict, lack of parental supervision and limited peer support further amplify vulnerability. The anonymity afforded by digital platforms also facilitates aggressive behaviour, as perpetrators experience a reduced sense of empathy for victims (Runions et al., 2021).

Among adolescents, susceptibility to phishing is influenced by an interplay of demographic, cognitive, social and emotional factors. Age is a relevant determinant, as younger users with less digital experience tend to engage in more impulsive online behaviours (Algarni et al., 2015). The amount of personal information shared online—such as photos, preferences, locations and social connections—also amplifies exposure, since cybercriminals can use this data to craft more convincing and personalized phishing messages (Jagatic et al., 2007).

Online grooming risk factors include emotional loneliness, limited parental monitoring and the search for validation typical of adolescent development (Whittle et al., 2014). Groomers exploit these vulnerabilities through gradual manipulation, often by providing attention, empathy or material incentives. Adolescents who experience mental health problems, previous abuse or lack of self-esteem are more likely to engage with strangers online, increasing their susceptibility (Gámez-Guadix et al., 2021). The information accessible through minors' online profiles—such as photographs, personal interests, frequently visited locations and even shared emotional or family issues—enables online groomers to tailor their strategies with greater precision. In addition, differential perceptions of online risk suggest that males are less frequently contacted by groomers but, when targeted, are more likely to experience grooming (Reneses et al., 2024a).

Exposure to fake news and misinformation represents a distinct yet complementary threat to minors' cognitive and social development. Risk factors include insufficient media literacy, limited critical thinking skills and strong reliance on social media as a primary news source (Molina-Cañabate et al., 2023). Adolescents are especially susceptible to confirmation bias, tending to believe information that aligns with their pre-existing opinions or peer group narratives (Pennycook & Rand, 2019). Furthermore, not only impulsivity, but also being swayed by the form and aesthetics of a news item and its scientific appearance increases the likelihood of sharing false news (Reneses et al, 2024b).

In summary, taken together, these risk factors reveal that the four phenomena—cyberbullying, phishing, online grooming, and fake news—are interconnected through shared structural and psychological vulnerabilities. Across all cases, limited digital literacy, emotional immaturity and inadequate adult supervision emerge as central determinants. Moreover, the design of online platforms—optimised for engagement rather than safety—creates systemic conditions that enable exploitation. A holistic understanding of these risks requires integrating individual, social and technological perspectives, recognising that effective prevention must combine education, policy regulation and platform accountability.

Table 1. Risk Factors Identified in Previous Research.

| Phenomenon | Individual Factors | Social / Contextual Factors | Technological / Platform Factors |
|---|---|---|---|



Co-funded by the European Union

| | | | |
|---|---|---|---|
| **Cyberbullying** | Low self-esteem, high impulsivity; gender, sexual orientation, or migrant background | Conflictive environments, parental supervision, low peer support | Anonymity reduces empathy and facilitates aggression |
| **Phishing** | Younger age, impulsivity, limited digital experience | Sharing of personal information. | Highly personalized phishing messages crafted from online data |
| **Online Grooming** | Emotional loneliness, low self-esteem, mental health problems, prior abuse | Insufficient parental monitoring; adolescents' search for validation | Access to personal data enables tailored manipulation |
| **Fake News / Misinformation** | Low critical thinking, confirmation bias, impulsivity, low media literacy | High reliance on social media as a news source | Appealing or "scientific" design increases credibility and sharing of false content |


Co-funded by the European Union

# 3. Methodology

## 3.1. Research Design and Rationale

To comprehensively approach the study of the CB, phishing, OG and FNs phenomena we designed a series of cyberadventures based on extensive preliminary research at European level, which consisted of combining four complementary data collection strategies: analysis of court sentences (Riberas et. al, 2024), in-depth interviews with experts, offenders and victims (Reneses et.al, 2024a), focus groups with adolescents (Reneses et.al,20024b) and a survey (Reneses et. al, 2025b). Then, we designed scenarios that measured risk situations and risk factors. In addition, we included both validated questionnaires and sociodemographic questions at the beginning of the game.

Due to ethical reasons, the likelihood of becoming an offender was measured only in two situations: one regarding cyberbullying and another about homophobic cyberbullying. Cyberbullying victimisation was not measured in the game, but through the validated questionnaires. For the rest of the potential criminal phenomena, the likelihood of victimisation was measured through concrete risk situations. For online grooming, by accepting a stranger's friendship request and by sending photos. Phishing was measured by clicking a fake link. Fake news was measured by considering the wrong ways of checking the veracity of the information. In this case, placing importance on the information appearing accurate, for example, with sufficient graphics and statistics, and on the professional appearance of the website (style, images, design, etc.) was considered less advisable and more risky than other strategies such as checking the source itself: whether it is a well-known newspaper/website or an unknown site, or searching the Internet to verify the information.

Table 2. Risk factor Variables.

| **Risk factors** | |
|---|---|
| **Questionnaires and registration** | **In-game scenarios** |
| CB's previous victimisation | CB's previous victimisation |
| CB's previous offending | CB's previous offending |
| Family support | Family communication |
| Social support | |
| Self esteem | |
| Gender | |
| Age | |
| Time spent online | Time spent online |
| Sociability | Sociability |
| | Personal Information Online |
| Type of school | |

These in-game measures are validated through construct (Shrestha, N., 2021) and criterion validity (Marengo, D., and Settanni, M., 2024). The first is related to measuring an underlying latent factor that we do not observe, in this case, the in-game scenarios are attempting to measure each cybercrime. The second is related to prediction, examining how well the in-game variables predict the constructs not observed.


Co-funded by the European Union

## 3.2. Participants

The initial sample involved 5852 participants, but only 1984 were retained for analysis after excluding those who indicated in the control question, applied at the end of the game, that they had not played as they would have behaved in real life. This final sample included 998 boys, 950 girls, and 7 non-binary students aged between 10 and 16 years in Portugal. Moreover, the students who participated in the study were enrolled in various types of schools: 1809 in public schools, 167 in private schools, and 8 in other types of schools. Participants were recruited through schools participating in the Policia Judiciaria programme “Missão Cibersegura”.

## 3.3. Ethical Approval

We obtained the ethics committee's approval and all participants (and their families when necessary) signed an informed consent form displaying full information about the objectives of the study.

## 3.4. Data Collection Procedure

The video game was played during school hours in the classrooms, under the supervision of a teacher responsible for its implementation. A pre-established protocol was followed, which included three main stages: first, preparation, installation of the game and collection of consent forms; second, presentation to the students, student registration and instructions for playing the six adventures; and finally, a series of questions for guided discussion with students, which included practical information on how to report incidents or seek help in specific situations.

## 3.5. Data Analysis

After data collection, we exported the data and analysed it with the RStudio, version 2024.09.0-375 (which is an integrated development environment for the R programming language). We carried out a descriptive analysis of simple frequencies and performed a bivariate analysis using contingency tables and the Chi-square test, verifying the statistical significance between pairs of variables through the corrected typed residuals. We also conducted a logistic regression in order to test the different risk factors simultaneously, together with a collinearity analysis.


Co-funded by the European Union

# 4. Results

## 4.1. Cyberbullying

### 4.1.1. Offending

In order to avoid exposing participants to simulated victimisation, the analysis examined the likelihood of becoming a cyberbully. Two scenarios were evaluated within the game: sharing an offensive meme about a classmate (N = 1717) and laughing at a homophobic joke directed at another (N = 1166).

Both situations showed a similar prevalence: approximately 17.9% of participants engaged in aggressive behaviour. Importantly, when asked to reflect on their actions, around 69.5% of those who had acted as aggressors recognized that their behaviour was wrong and many explicitly identified it as bullying.

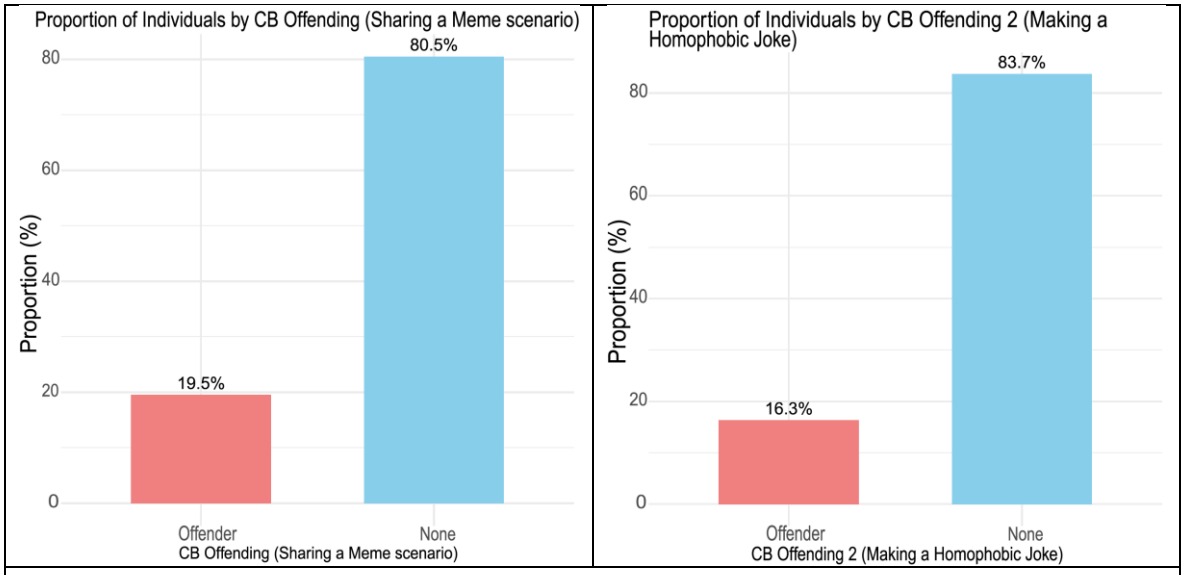


Figure 1. Proportion of Individuals by CB Offending

The relationship between these variables is quite high as they are measured in-game, though in different adventures related to cyberbullying. (Chi-squared coeff. of 50.197 (**stronger association**), and a p-value less than $1.39\text{x}10^{-12}$ (**highly significant**)).

### 4.1.2. Victimisation

Although victimisation was not measured directly in the game, it was estimated using a questionnaire on previous victimisation (N = 1984), which showed a prevalence of 28.3%.



Co-funded by the European Union

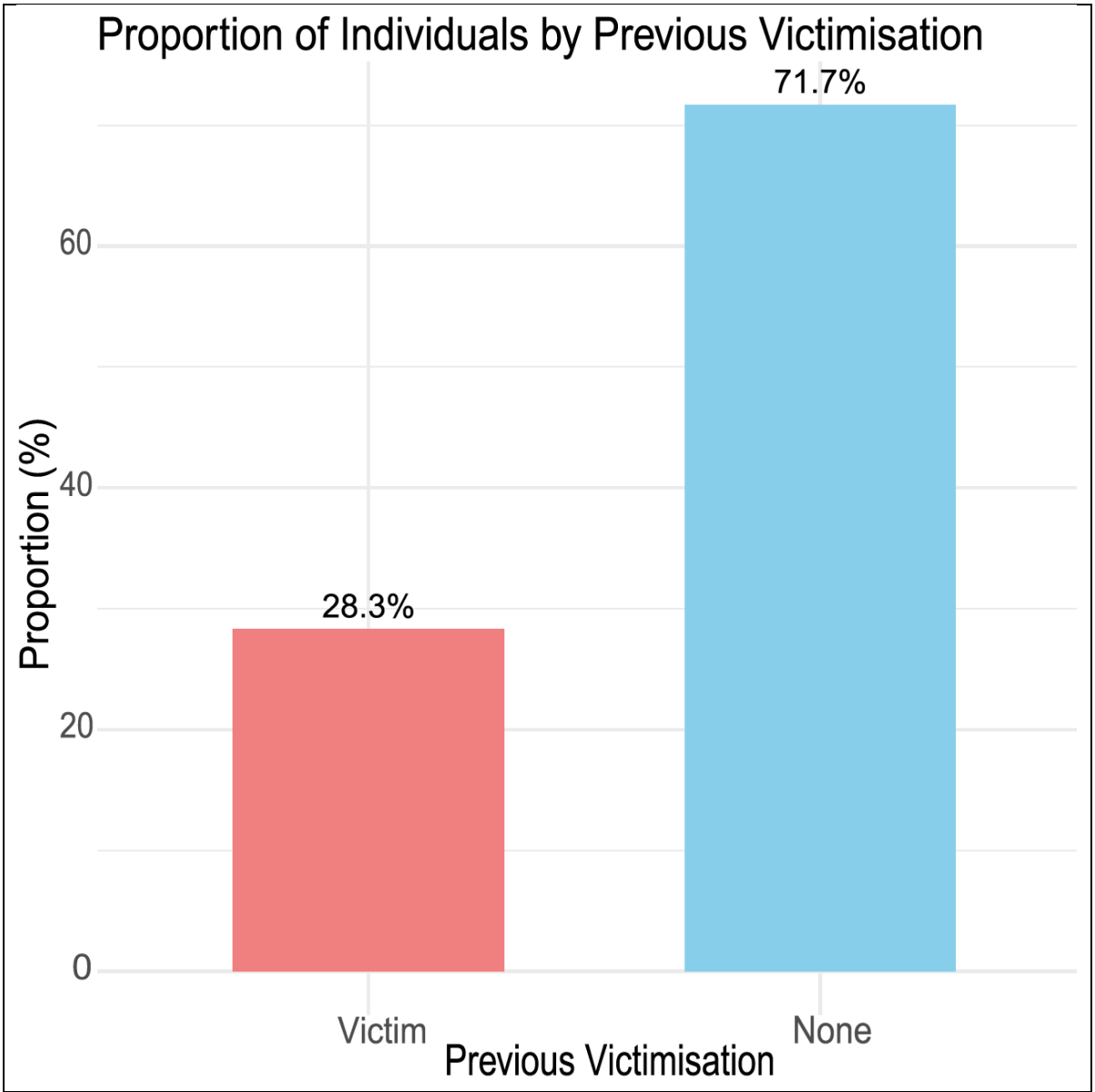


Figure 2. Proportion of Individuals by Previous Victimisation

## 4.2. Phishing

Although phishing often receives less attention in prevention programs, it emerged as the most frequent cybercrime among participants with a potential prevalence of 41% (N = 1046).


Co-funded by the European Union

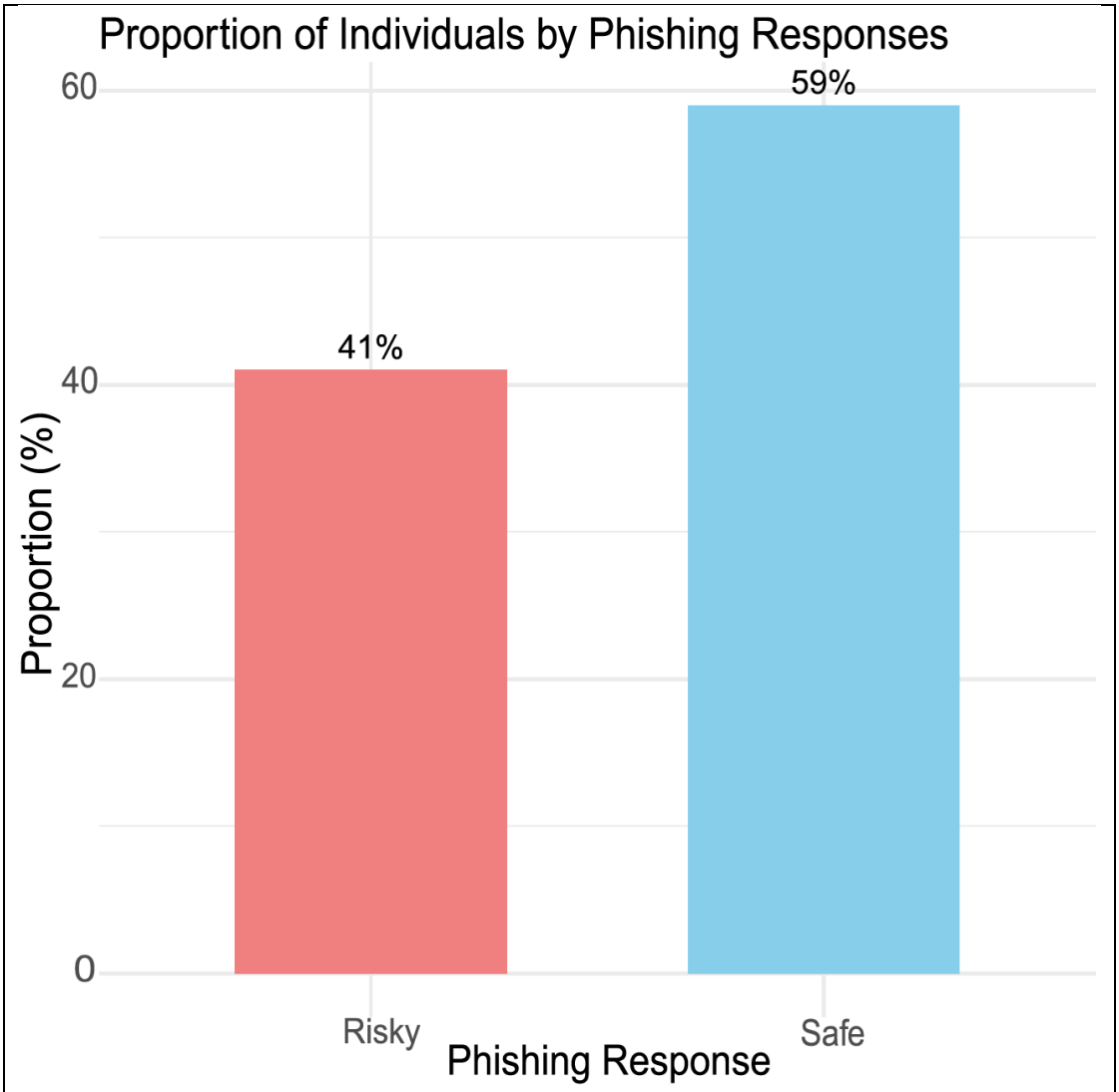


Figure 3. Proportion of Individuals by Phishing Victimisation

## 4.3. Online Grooming

Exposure to online grooming was evaluated through two scenarios: accepting a friend request from a stranger on a social network (N = 1295) and sending photographs after receiving a request from that stranger, who posed as a photographer offering to create a modeling portfolio (N = 1293).

Findings revealed that 22.5% of participants accepted the request without checking the stranger profile. In addition, among those who checked the profile, 16.4% still accepted the request, as the account included realistic cues commonly used by perpetrators as mutual friends, old posts, comments and real photos. Finally, 10.4% of the total sample ultimately agreed to send photos.



Co-funded by the European Union

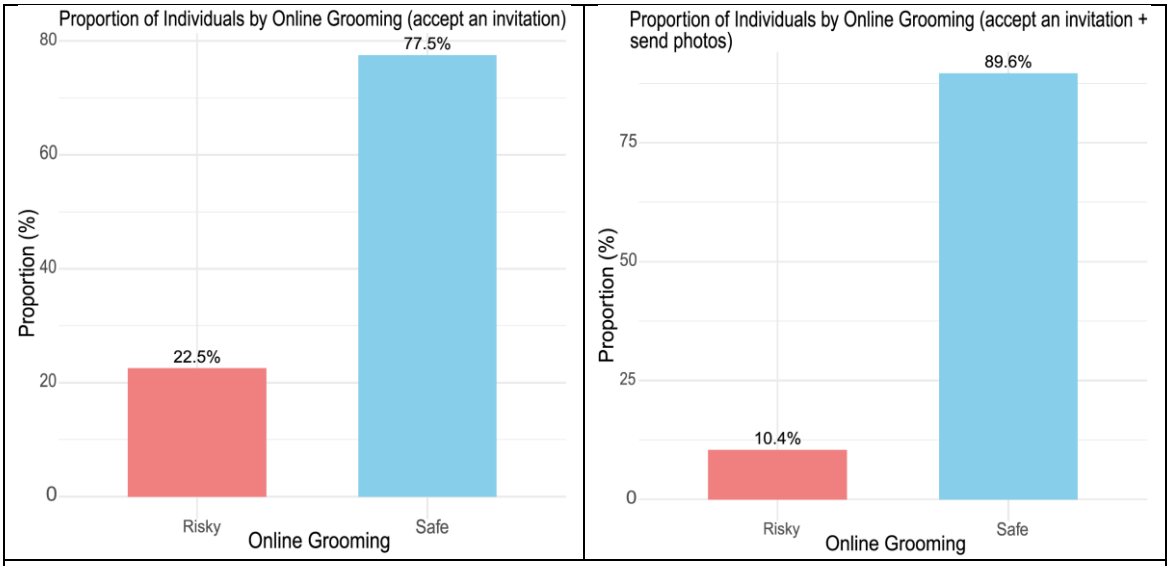


Figure 4. Proportion of Individuals by Online Grooming

## 4.4. Fake News

The risk of falling in fake news was measured through a scenario in which players had to decide the best ways of checking the veracity of the information (related with refugees) (N = 1118). If they choose as the first option the information appearing accurate, for example, with sufficient graphics and statistics, and the professional appearance of the website (style, images, design, etc.) they were considered as at risk. On the other hand, if they chose to check the source itself or to search the Internet to contrast the information, they were considered unrisky.

The results show that around two-thirds responded with confident answers to avoid this type of deception. However, one-third decided that it was best to trust the most superficial aspects of the news, rather than conducting more in-depth investigations.


Co-funded by the European Union

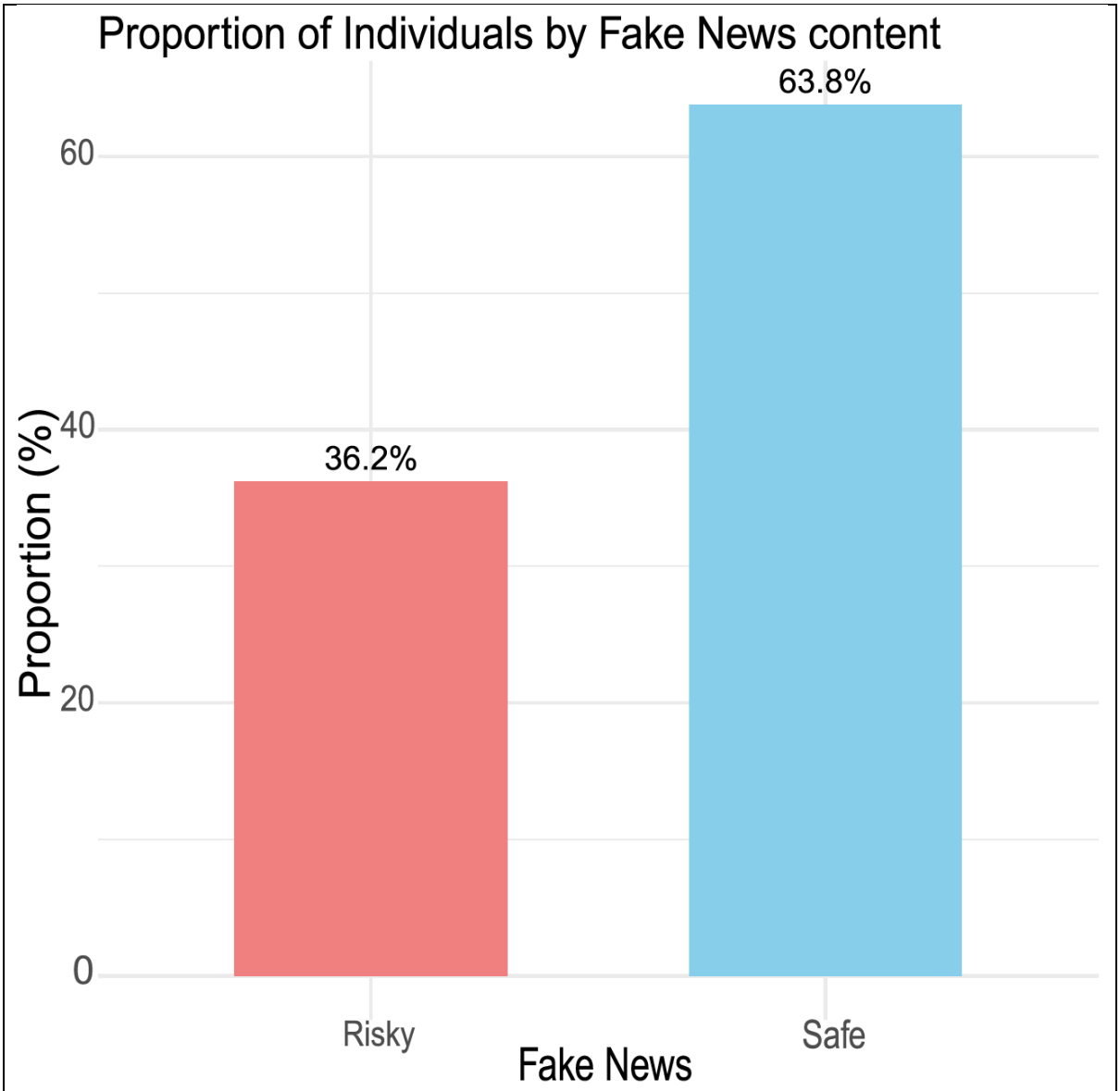


Figure 5. Proportion of Individuals by Fake News

## 4.5. Risk Factors Across All Cyber Threats

One of the most significant findings is the overlap of risk factors across all four cyber threats, suggesting that targeted prevention strategies can have broad protective effects. Key factors include:

Table 3. Risk Factors Across Cyber Threats

| | | CB Offending * | CB victimisation | Phishing | O. Grooming | Fake news |
|---|---|---|---|---|---|---|
| Gender | | Male | X | Male | Male | Male |
| Age | | Older | Older | X | Older | X |
| Self - esteem | | Low | Low | Low | X | Low |
| Social & other support | | Low | Low | X | Low | Low |
| Time spent online | In game | High | High | High | High | X |
| | In regist. | X | High | High | X | X |
| Family support | In game | Low | Low | Low | Low | Low |



Co-funded by the European Union

| | | | | | | |
|---|---|---|---|---|---|---|
| | In Quest. | Low | Low | Low | X | X |
| Personal information online | Profile | Public | X | Public | Public | Public |
| | Place | Real | Real | Real | Real | Real |
| | Photo | Real | Real | Real | Real | Real |
| | Password | Insecure | X | Insecure | Insecure | Insecure |
| Sociability trait | In game | High | X | X | X | X |
| | In Quest. | High | X | X | X | X |
| Type of School | In Quest. | Public | Public | Public | Public | X |

*The Sharing a Meme scenario is being assessed. Moreover, considering the Homophobic Joke scenario, the same risk factors are relevant, except for Age, Self-Esteem and Sociability (in-game).

See Table in the Appendix to know the numerical association.

- Gender: Boys were more likely to become cyberbullies (especially in homophobic contexts), to fall victim to phishing, fake news and even more so to online grooming.
- Disclosure of personal information: In a simulated social network, participants were asked whether to make their profile public, share personal photos, publish their place of residence and choose a password. All four behaviours were associated with an increased risk in all the cyber threats.
- Family communication: Weak communication at home appeared as a common factor across all cyber threats. Low family support answered through the validated questionnaire was significant as well.
- Time spent online: Confirming earlier observations, heavy online use emerged as the most relevant risk factor for all four cyber threats. This happened when directly questioned and through an in-game situation.


Co-funded by the European Union

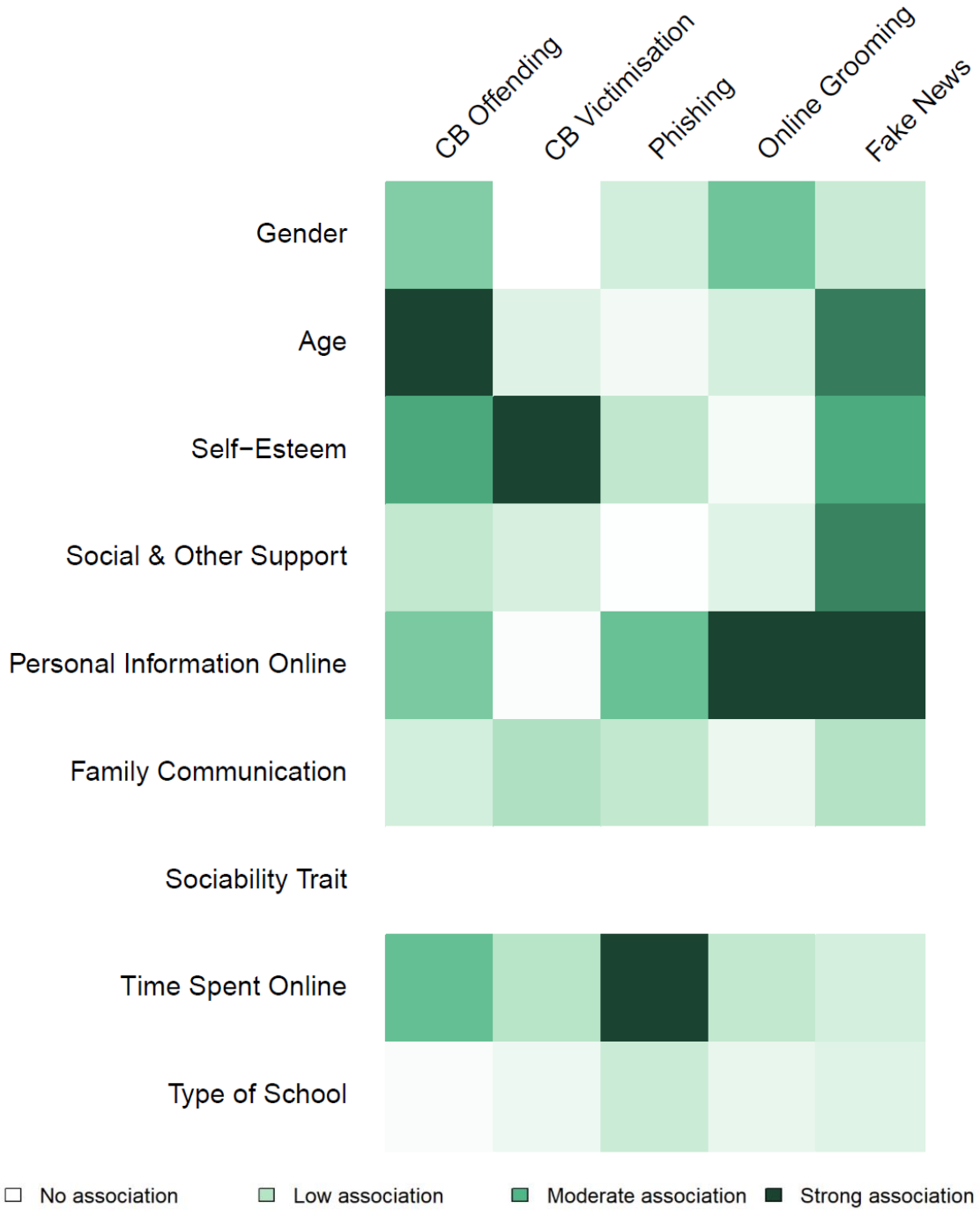


Figure 6. Association Between Cyber Threats and Risk Factors


Co-funded by the European Union

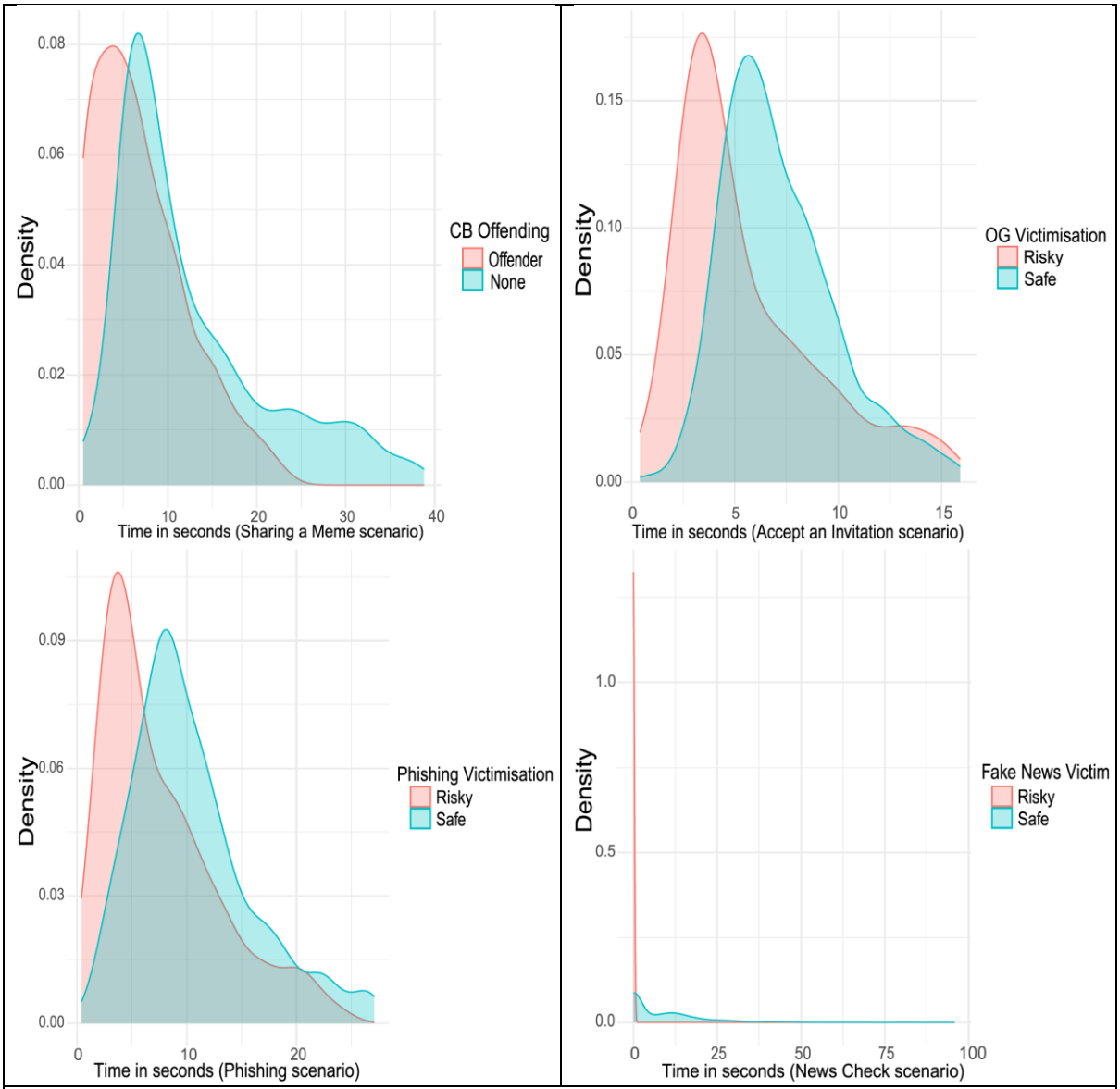


Figure 7. Time Spent during Gameplay

The time spent by offenders and victims on each cyber-threat scenario, compared with individuals who do not fall into these categories, differs significantly. Regarding the time spent on the different serious game scenarios, as shown in Figure 7, both victims (of different cyber threats) and offenders completed the adventures in less time during gameplay. Consequently, the hypothesis that the time required to respond to the game scenarios varies across groups is supported.


Co-funded by the European Union

# 5. Discussion

## 5.1. Cyber Threats

There are two main findings. First, the prevalence rates for the different cybercrimes are quite high (which is worrying when it comes to a relatively controlled situation, such as a normal classroom). And second, there is overlap between risk factors and crimes. The following section discusses each of the cybercrimes and their associated risk factors, followed by a joint discussion.

### 5.1.1. Cyberbullying

The results for cyberbullying correspond to two different measures.

The measure of previous victimisation is based on a validated questionnaire and refers to victimisation throughout life. Thus, around one third of respondents reported having been victims of cyberbullying, a worrying figure even when considering lifetime measures.

The figures for aggression (measured directly through the video game) are also worrying for two reasons. First, a prevalence of 17.9% for aggression is high. Second, when asked to reflect on their actions, around 69.5% of those who had acted as aggressors recognized that their behaviour was wrong, and many explicitly identified it as bullying.
Prevalence should be assessed only in terms of young people at risk of becoming aggressors, and not as actual aggressors, because despite the game's high ecological validity, the absence of real harm to others may slightly inflate participants' responses.

### 5.1.2. Phishing

Although phishing often receives less attention in prevention programs, it emerged as the most prevalent cybercrime among participants, affecting nearly half of the sample. Importantly, age was not a significant factor (as previously observed by Algarni et al., 2015), indicating that, within our large sample, young people are not developing the necessary skills to manage this risk as they grow.

### 5.1.3. Online Grooming

The high prevalence of risky decisions presented in the online grooming scenarios underlines the need to rethink how prevention messages are framed. Traditional recommendations such as "don't accept strangers" or "don't send photos" are necessary, but clearly insufficient when more than one in ten participants were willing to send pictures to someone they had never met offline. The progression observed in the game from accepting a request to ultimately sharing photos mirrors the gradual escalation typical of real online grooming processes. In addition, it shows how quickly adolescents' boundaries can be pushed once initial trust or curiosity is established. Crucially, the fact that many participants accepted a seemingly well constructed profile (with mutual friends, posts and comments) indicates that young people are not simply ignoring advice, but rather overestimating their ability to detect fake or malicious accounts, which has direct implications for the design of educational campaigns.


Co-funded by the European Union

### 5.1.4. Fake News

In the case of fake news, as in the previous cases, it was not the direct prevalence that was measured, but rather the risk of falling for fake news through belief in unreliable criteria of veracity, which are often considered valid: affinity or trust in the person sharing the content (e.g., a close friend who unknowingly shares fake news), the degree of sophistication in the design of the information source (Herrero-Diz et al., 2020), and also when the content is sponsored and includes data and statistics (McGrew et al., 2017, Reneses et al., 2024b).

## 5.2. Risk Factors

The study illustrates the relationship between individual, social and contextual variables as risk factors and their connection to different cybercrimes, highlighting that these risk factors are largely shared across all types of cybercrime.

- Disclosure of personal information: One of the strongest associations in the heatmap appears between personal information online and both phishing and online grooming, confirming that higher levels of digital self-disclosure significantly increase vulnerability. Behaviours such as making one's profile public, sharing photos, publishing one's residence or school and using weak passwords were all linked to greater risk. This supports previous research stressing the importance of privacy settings and cautious self-presentation online (Walrave et al., 2012). The strongest association between sharing personal information and online grooming and phishing must be due to the fact that the two crimes are highly dependent on information exploitation. Prevention should then prioritize privacy literacy and control over self-presentation, teaching adolescents about how to audit their digital footprint, including visibility of profiles, photos, school information and location.
- Time spent online: Within the study, time spent online emerged as the second most important risk factor, demonstrating its strongest association with phishing. Excessive online presence has been previously linked to impulsive behaviour, reduced self-regulation and exposure to social or emotional stressors (Ribeiro et al., 2024). This finding connects with ongoing debates about the relationship between intensive online activity, social isolation, mental health challenges and difficulties in self-regulation. It suggests that impulsivity and reduced control over online behaviour may increase vulnerability to phishing and other crime attempts.
  Another finding was that potential victims and offenders spent less time answering the video game questions, which shows a tendency to act impulsively instead of following the "think before you click" approach. Prevention should focus on self-regulation, attention control, and healthy digital routines, such as "micro-delay" strategies (e.g., pausing 3–5 seconds before clicking or responding), media-use agreements at home with structured times for online activities and balanced digital routines promoted from school.
- Gender: Gender appears moderately associated with cyberbullying (CB) offending, online grooming and, to a lesser extent, with phishing, matching our findings and earlier work (Kavvadias & Kotsilieris, 2025). Boys' higher risk may be influenced by gender norms linked to risk-taking, overconfidence or the belief that digital threats are minimal. This highlights the importance of addressing gender roles in prevention, particularly the notion — often tied to masculinity — that there is "nothing to fear", even online.
- Age: This variable as a risk factor showed a differentiated pattern depending on the type of cybercrime. In our data, age was associated with both cyberbullying (CB) aggression and victimisation, as well as with online grooming (OG). This aligns with previous research,


Co-funded by the European Union

showing that early to mid-adolescence (particularly the years close to puberty) is a period marked by increased emotional reactivity, identity exploration, peer dependence and, in the case of online grooming, heightened sexual curiosity. These developmental characteristics can intensify both perpetration (e.g., impulsivity, status-seeking, reduced empathy) and vulnerability (e.g., desire for social acceptance, susceptibility to online attention) (Kowalski et al., 2019; Whittle et al., 2014). Interestingly, age did not decrease vulnerability to phishing or fake news, contrary to expectations that adolescents would progressively learn to avoid online deception. Instead, there is limited natural learning or protective experience with these risks, meaning that getting older does not automatically translate into better detection of fraudulent messages or misinformation. Overall, these findings indicate that cyberbullying and online grooming risks peak during developmental transitions, while phishing and misinformation risks remain consistently high across adolescence, underscoring the need for explicit instruction on digital deception rather than expecting age-related improvement.

- Family communication/support: Weak family communication/support shows a consistent but moderate presence across all cyber threats, suggesting that it functions as a general vulnerability factor. This matches the literature on parental mediation and digital safety: although direct links to phishing remain scarce, several studies report that low family supervision and poor communication increase exposure to online victimisation and risky behaviour (Akter et al., 2022; Dittus et al., 2023).
  This risk factor was present across victimisation in online grooming, phishing and even exposure to fake news. The findings suggest that open dialogue within families is more effective than control or restrictions, in both preventing and detecting cyber threats. Lack of guidance in digital practices seems to be involved in these risky interactions or impulsive clicks. Interventions should reinforce open dialogue, not surveillance, focusing on conversation rather than control, encourage co-use and family routines where adolescents feel safe reporting strange messages. Schools might offer parent workshops focusing on digital norms, scams, grooming signs and phishing tactics.
- Self-esteem: This variable as a risk factor displays a strong association with victimisation and a moderate link with phishing. Although previous evidence has connected low self-esteem primarily with general cybervictimisation (Álvarez-García et al., 2025), our results suggest that its indirect psychological effects—need for validation, emotional vulnerability, indecision—may also make individuals more susceptible to phishing attempts. In fact, and while self-esteem is not generally related to all forms of cyber threats, it is distinctly associated with vulnerability to being targeted or deceived, rather than with becoming a perpetrator. Thus, not only digital literacy programs should be approached, but also social and emotional learning programs. Education about how offenders exploit insecurity and use manipulation strategies would be useful as well.
- Social support: A particularly strong association appears between low social support levels and cyberbullying victimisation, and a notable association with fake news susceptibility. This suggests that weaker support networks may leave adolescents more vulnerable to manipulation or exclusion. Social support is thus a protective buffer, especially for emotionally driven risks. Prevention should aim to strengthen belonging and peer networks.
- Type of school: A moderate association between type of school (public) and phishing has been identified, reinforcing our interpretation that environmental and structural differences—such as fewer cybersecurity resources or lower digital literacy—may play a key role. This aligns with Jerrim's (2023) findings that adolescents from disadvantaged backgrounds are more likely to respond to phishing emails due to weaker cognitive skills or academic performance. School type does not uniformly affect all cyber threats, but is specific to information-manipulation


Co-funded by the European Union

contexts, especially phishing. Free, standardized digital literacy curricula across schools should ensure equal access to cybersecurity education.

## 5.3. Limitations

Despite the breadth and ecological validity of the video game, several limitations must be acknowledged. First, although the use of an immersive video game provides a realistic environment for observing adolescents' online behaviours, simulated scenarios cannot perfectly reproduce the emotional, social and contextual pressures of real digital interactions. This may lead to slight overestimation or underestimation of risk-taking behaviours, such as clicking on suspicious links or engaging with strangers. Second, the design relies as well on self-reported measures for some variables (e.g., previous victimisation, family support), which are inherently affected by recall bias and social desirability. Having both measures (validated questionnaires and in game situations) try to improve both biases. Lastly, although a wide range of variables was included, additional structural or psychological factors were not captured and could enrich future analyses.


Co-funded by the European Union

# 6. Summary

## 6.1. Conclusion

The results of this exploratory study demonstrate that cyberbullying, phishing, online grooming, and exposure to fake news constitute pervasive and interconnected threats affecting minors. Even in a controlled school environment, a substantial proportion of participants engaged in or were vulnerable to harmful digital behaviours, indicating that young people are navigating online spaces without sufficient preparation or support. The innovative methodology based on the video game allowed for direct observation of decision-making processes in realistic scenarios, revealing patterns that might remain hidden in traditional survey-based research. This approach highlights the value of interactive, experiential tools for understanding how adolescents perceive and respond to digital risks.

A central finding of the study is the significant overlap of risk factors across the four cyber threats. Variables such as time spent online, weak family communication, low self-esteem, limited social support and the disclosure of personal information emerged repeatedly as predictors of vulnerability. This convergence suggests that online risks do not occur in isolation; rather, they stem from shared developmental, emotional and contextual mechanisms. Particularly striking is the role of impulsivity, indicating that adolescents often make rapid decisions without evaluating potential consequences. Similarly, the strong association between personal information online and both online grooming and phishing underscores the extent to which offenders exploit minors' digital footprints.

Another important conclusion pertains to age. While cyberbullying and online grooming risks peaked during early adolescence, an expected pattern reflecting developmental transitions, phishing and susceptibility to fake news did not decline with age. This lack of improvement suggests that adolescents do not naturally acquire the skills needed to detect digital deception, highlighting a critical gap in current educational practices. The persistence of vulnerabilities across age groups reinforces the need for explicit instruction in recognizing manipulative design cues, emotional persuasion strategies and the deceptive tactics used in fraud and misinformation.

## 6.2. Evaluation

The findings highlight the need for a comprehensive and complex approach to online safety education and policymaking. Prevention strategies should move beyond generic messages and instead incorporate targeted training, addressing the nuanced psychological and contextual vulnerabilities identified in this study. Schools should adopt digital literacy programs that emphasize privacy management, critical evaluation of online content, and recognition of grooming and phishing cues. At the family level, interventions should prioritize open communication, co-use of digital technologies and guidance rather than surveillance, empowering adolescents to seek help when confronted with risks. Policymakers and platform designers should also take responsibility by integrating child safety features, default privacy protections and transparent reporting systems. Overall, the overlap of risk factors across different cyber threats suggests that interventions addressing core elements such as impulsivity, emotional vulnerability and digital self-disclosure may generate broad protective effects across multiple online threats.


Co-funded by the European Union

## 6.3. Future work

The findings of this work underscore the need for designing prevention programs that integrate emotional, cognitive and digital competencies. Effective interventions must address not only technical skills, but also the psychological needs and social environments that shape adolescents' online behaviour. The program "Missão Cibersegura" provides an important foundation for this goal, offering insights that can guide future research, inform policy development and support the growth of resilient, critically minded digital citizens.


Co-funded by the European Union

# Appendix

| | | CB Offending | CB victimisation | Phishing | O. Grooming | Fake news |
|---|---|---|---|---|---|---|
| Gender | | Male 11.9% | Male 14.6% | Male 24.0% | Male 15.5% | Male 20.5% |
| | | Female 7.5% | Female 13.6% | Female 16.4% | Female 7.2% | Female 15.6% |
| | | $\chi = 15.761$, $p < 0.001$ | $\chi = 0.051$, $p = 0.822$ | $\chi = 7.846$, $p = 0.005$ | $\chi = 38.19$, $p = 0.00$ | $\chi = 3.17$, $p = 0.075$ |
| | | CC = 0.096 | CC = 0.005 | CC = 0.087 | CC = 0.171 | CC = 0.054 |
| Age | | 10, 2.1% | 10, 2.1% | 10, 3.4% | 10, 1.1% | 10, 2.4% |
| | | 11, 4.5% | 11, 4.3% | 11, 7.4% | 11, 4.1% | 11, 7.4% |
| | | 12, 4.3% | 12, 5.7% | 12, 6.5% | 12, 5.7% | 12, 6.3% |
| | | 13, 3.1% | 13, 5.5% | 13, 7.8% | 13, 4.4% | 13, 5.9% |
| | | 14, 2.8% | 14, 6.7% | 14, 10.0% | 14, 4.2% | 14, 9.8% |
| | | 15, 1.8% | 15, 2.8% | 15, 4.4% | 15, 2.3% | 15, 3.2% |
| | | 16, 0.9% | 16, 1.1% | 16, 1.7% | 16, 1.0% | 16, 1.1% |
| | | $\chi = 25.111$, $p < 0.001$ | $\chi = 19.676$, $p = 0.003$ | $\chi = 2.431$, $p = 0.876$ | $\chi = 13.192$, $p = 0.04$ | $\chi = 9.163$, $p = 0.165$ |
| | | CC = 0.121 | CC = 0.1 | CC = 0.049 | CC = 0.101 | CC = 0.091 |
| Self- esteem | | Low 2.9% | Low 8.8% | Low 9.3% | Low 4.0% | Low 7.9% |
| | | Medium 9.7% | Medium 12.4% | Medium 17.1% | Medium 9.5% | Medium 15.2% |
| | | High 6.8% | High 7.1% | High 14.6% | High 9.0% | High 13.1% |
| | | $\chi = 19.631$, $p < 0.001$ | $\chi = 129.359$, $p = 0.00$ | $\chi = 10.381$, $p = 0.006$ | $\chi = 3.396$, $p = 0.183$ | $\chi = 7.833$, $p = 0.02$ |
| | | CC = 0.106 | CC = 0.247 | CC = 0.099 | CC = 0.051 | CC = 0.083 |
| Social & other support | | Low 1.3% | Low 2.6% | Low 2.5% | Low 1.7% | Low 3.2% |
| | | Medium 6.5% | Medium 8.7% | Medium 12.4% | Medium 7.4% | Medium 11.2% |
| | | High 11.7% | High 17.0% | High 26.1% | High 13.4% | High 21.8% |
| | | $\chi = 11.528$, $p = 0.003$ | $\chi = 24.157$, $p = 0.00$ | $\chi = 0.514$, $p = 0.773$ | $\chi = 10.049$, $p = 0.007$ | $\chi = 8.975$, $p = 0.011$ |
| | | CC = 0.082 | CC = 0.11 | CC = 0.022 | CC = 0.088 | CC = 0.089 |
| Time spent online | In game | <4h, 10.8% | <4h, 18.2% | <4h, 25.9% | <4h, 13.6% | <4h, 26.9% |
| | | >4h, 7.0% | >4h, 8.6% | >4h, 14.3% | >4h, 8.3% | >4h, 9.5% |



Co-funded by the European Union

| | | | | | | |
|---|---|---|---|---|---|---|
| | | χ = 27.68, p = 0.00 | χ = 14.059, p < 0.001 | χ = 52.019, p = 0.00 | χ = 33.432, p = 0.00 | χ = 2.247, p = 0.134 |
| | | CC = 0.157 | CC = 0.109 | CC = 0.23 | CC = 0.176 | CC = 0.05 |
| | In regist. | <4h, 14.5% | <4h, 19.0% | <4h, 29.7% | <4h, 17.0% | <4h, 27.4% |
| | | >4h, 5.0% | >4h, 9.4% | >4h, 11.3% | >4h, 5.6% | >4h, 8.9% |
| | | χ = 7.543, p = 0.11 | χ = 70.418, p = 0.00 | χ = 19.147, p < 0.001 | χ = 4.543, p = 0.338 | χ = 3.107, p = 0.54 |
| | | CC = 0.066 | CC = 0.185 | CC = 0.134 | CC = 0.059 | CC = 0.053 |
| Family support | In game | Low 3.8% | Low 6.1% | Low 8.8% | Low 5.3% | Low 8.0% |
| | | Medium 3.5% | Medium 5.7% | Medium 7.2% | Medium 4.0% | Medium 6.3% |
| | | High 10.2% | High 17.0% | High 24.1% | High 12.7% | High 22.8% |
| | | χ = 5.889, p = 0.053 | χ = 13.103, p < 0.001 | χ = 12.252, p = 0.002 | χ = 12.788, p = 0.002 | χ = 6.8, p = 0.033 |
| | | CC = 0.069 | CC = 0.101 | CC = 0.115 | CC = 0.101 | CC = 0.087 |
| | In Quest. | Low 1.6% | Low 2.9% | Low 3.1% | Low 1.3% | Low 2.1% |
| | | Medium 4.2% | Medium 7.5% | Medium 8.3% | Medium 3.7% | Medium 7.4% |
| | | High 13.6% | High 17.9% | High 29.6% | High 17.5% | High 26.7% |
| | | χ = 14.303, p < 0.001 | χ = 80.723, p = 0.00 | χ = 8.04, p = 0.018 | χ = 0.261, p = 0.878 | χ = 1.532, p = 0.465 |
| | | CC = 0.091 | CC = 0.198 | CC = 0.087 | CC = 0.014 | CC = 0.037 |
| Personal information online | Profile | Public 5.9% | Public 6.9% | Public 9.1% | Public 8.5% | Public 9.4% |
| | | Private 11.9% | Private 22.6% | Private 30.2% | Private 14.0% | Private 28.3% |
| | | χ = 21.564, p = 0.00 | χ = 1.096, p = 0.295 | χ = 2.986, p = 0.084 | χ = 58.799, p = 0.00 | χ = 6.403, p = 0.011 |
| | | CC = 0.131 | CC = 0.029 | CC = 0.059 | CC = 0.211 | CC = 0.086 |
| | Place | Risky 4.6% | Risky 5.8% | Risky 8.3% | Risky 8.0% | Risky 7.0% |
| | | Safe 13.2% | Safe 23.7% | Safe 31.1% | Safe 14.6% | Safe 30.6% |
| | | χ = 17.211, p < 0.001 | χ = 3.575, p = 0.059 | χ = 17.058, p < 0.001 | χ = 101.136, p = 0.00 | χ = 6.144, p = 0.013 |



Co-funded by the European Union

| | | | | | | |
|---|---|---|---|---|---|---|
| | | CC = 0.117 | CC = 0.052 | CC = 0.14 | CC = 0.273 | CC = 0.085 |
| | Photo | Risky 12.1% | Risky 18.2% | Risky 25.5% | Risky 17.7% | Risky 23.0% |
| | | Safe 5.8% | Safe 11.2% | Safe 13.9% | Safe 4.8% | Safe 14.7% |
| | | $\chi$ = 12.272, p < 0.001 | $\chi$ = 6.078, p = 0.014 | $\chi$ = 20.674, p = 0.00 | $\chi$ = 74.81, p = 0.00 | $\chi$ = 6.052, p = 0.014 |
| | | CC = 0.099 | CC = 0.068 | CC = 0.153 | CC = 0.237 | CC = 0.084 |
| | Password | Insecure 4.0% | Insecure 3.8% | Insecure 9.1% | Insecure 5.5% | Insecure 7.3% |
| | | Secure 13.5% | Secure 23.0% | Secure 31.9% | Secure 16.2% | Secure 28.5% |
| | | $\chi$ = 13.88, p < 0.001 | $\chi$ = 0.076, p = 0.783 | $\chi$ = 44.287, p = 0.00 | $\chi$ = 32.446, p = 0.00 | $\chi$ = 24.96, p = 0.00 |
| | | CC = 0.121 | CC = 0.009 | CC = 0.202 | CC = 0.188 | CC = 0.162 |
| Sociability trait | In game | Sociable 11.7% | Sociable 15.1% | Sociable 21.7% | Sociable 12.3% | Sociable 20.3% |
| | | Shy 7.7% | Shy 13.8% | Shy 18.4% | Shy 10.4% | Shy 17.8% |
| | | $\chi$ = 5.031, p = 0.025 | $\chi$ = 1.144, p = 0.285 | $\chi$ = 0.517, p = 0.472 | $\chi$ = 0.184, p = 0.668 | $\chi$ = 0.143, p = 0.706 |
| | | CC = 0.054 | CC = 0.026 | CC = 0.024 | CC = 0.012 | CC = 0.012 |
| | In Quest. | Sociable 9.1% | Sociable 14.6% | Sociable 20.9% | Sociable 11.2% | Sociable 17.7% |
| | | Shy 10.4% | Shy 13.7% | Shy 20.1% | Shy 11.4% | Shy 18.5% |
| | | $\chi$ = 7.28, p = 0.007 | $\chi$ = 0.335, p = 0.563 | $\chi$ = 0.039, p = 0.844 | $\chi$ = 0.55, p = 0.458 | $\chi$ = 1.175, p = 0.278 |
| | | CC = 0.065 | CC = 0.013 | CC = 0.006 | CC = 0.021 | CC = 0.032 |
| Type of School | | Public 18.5% | Public 26.9% | Public 38.4% | Public 21.4% | Public 33.9% |
| | | Private 0.9% | Private 1.5% | Private 2.6% | Private 1.2% | Private 2.3% |
| | | $\chi$ = 6.721, p = 0.01 | $\chi$ = 10.323, p = 0.001 | $\chi$ = 8.812, p = 0.003 | $\chi$ = 7.211, p = 0.007 | $\chi$ = 2.189, p = 0.139 |
| | | CC = 0.063 | CC = 0.072 | CC = 0.092 | CC = 0.075 | CC = 0.044 |



Co-funded by the European Union

# References


Akter, M., Godfrey, A. J., Kropczynski, J., Lipford, H. R., & Wisniewski, P. J. (2022). From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals?. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW1), 1-28.

Algarni, A., Xu, Y., & Chan, T. (2015). An empirical study on the susceptibility to social engineering in social networking sites: The case of phishing. *Information & Computer Security, 23*(4), 367–388. https://doi.org/10.1108/ICS-05-2014-0029

Álvarez-García, D., García, T., & Betts, L. (2025). Anxiety and self-esteem as causes and consequences of cyber-victimization in preadolescence: a longitudinal study. *European Journal of Psychology Applied to Legal Context*, *17*(1), 1-9.

Bokolo, B. G., & Liu, Q. (2024). Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. Electronics, 13(9), 1671. https://doi.org/10.3390/electronics13091671

Craven, S., Brown, S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of sexual aggression*, *12*(3), 287-299.

Dittus, P. J. (2023). Parental monitoring and risk behaviors and experiences among high school students—Youth Risk Behavior Survey, United States, 2021. *MMWR supplements*, *72*.

Franklin-Paddock, B., Platow, M.J. & Ryan, M.K. (2025). From Privilege to Threat: Unraveling Psychological Pathways to the Manosphere. Arch Sex Behav 54, 1325–1340. https://doi.org/10.1007/s10508-025-03114-5

Gámez-Guadix, M., De Santisteban, P., & Resett, S. (2021). Sexting among Spanish adolescents: Prevalence and association with sexual grooming and cyberbullying victimization. Computers in Human Behavior, 120, 106761. https://doi.org/10.1016/j.chb.2021.106761

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

Jeglic, E. L., Winters, G. M., & Johnson, B. N. (2023). Identification of red flag child sexual grooming behaviors. *Child Abuse & Neglect*, *136*, 105998.

Jerrim, J. (2023). Who Responds to Phishing Emails? An International Investigation of 15-Year-<? a3b2 show [nbs]?> Olds<? a3b2 show [/nbs]?> Using PISA Data. *British Journal of Educational Studies*, *71*(6), 701-724.

Kavvadias, A., & Kotsilieris, T. (2025). Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review. *Applied Sciences*, *15*(4), 2236.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. *Psychological bulletin*, *140*(4), 1073.

Kowalski, R. M., Limber, S. P., & McCord, A. (2019). A developmental approach to cyberbullying: Prevalence, consequences, and risk factors. Journal of Youth and Adolescence, 48(9), 1767–1781. https://doi.org/10.1007/s10964-019-01099-4

Marengo, D., & Settanni, M. (2024). Examining the postdictive validity of self-report Big Five personality traits with objective recordings of online behaviors: a ten-year retrospective study using Facebook Page Likes. Heliyon, 10(12).




Co-funded by the European Union

Molina-Cañabate, J. P., González-Esteban, J. L., & López-Rico, C. M. (2023). Children and fake news: Media literacy and digital education in the age of disinformation. Education Sciences, 13(8), 763. https://doi.org/10.3390/educsci13080763

Pennycook, G., & Rand, D. G. (2019). Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. Cognition, 188, 39–50. https://doi.org/10.1016/j.cognition.2018.06.011

Reneses, M., Riberas-Gutiérrez, M., & Bueno-Guerra, N. (2024a). "He flattered me". A comprehensive look into online grooming risk factors: Merging voices of victims, offenders and experts through in-depth interviews. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 18(4).

Reneses, M., Riberas-Gutierrez, M., & Bueno-Guerra, N. (2024b). Who shares fake news? The consumption and distribution of information among adolescents and its relationship to hate speech. Revista de educación, (406), 265-291.

Reneses, M., Riberas-Gutiérrez, M., & Bueno-Guerra, N. (2025a). "It's just a joke": gender, sexuality and trivialisation in adolescent online violence such as cyberhate, cyberbullying, and online grooming. Humanities and Social Sciences Communications, 12(1), 1-14.

Reneses, M., Parder, M. L., Riberas-Gutiérrez, M., & Bueno-Guerra, N. (2025b). Cyberbullying and cyberhate as an overlapping phenomenon among adolescents in Estonia and Spain: Cross-cultural differences and common risk factors. Children and Youth Services Review, 172, 108285.

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *Computers & Security*, *136*, 103558.

Riberas-Gutiérrez, M., Reneses, M., Gómez-Dorado, A., Serranos-Minguela, L., Bueno-Guerra, N. (2024). Online grooming: factores de riesgo y modus operandi a partir de un análisis de sentencias españolas. Anuario de Psicología Jurídica. Vol. 34, nº. 1, pp. 119 – 131.

Runions, K. C., Bak, M., & Shaw, T. (2021). Cyberbullying perpetration and victimization: The role of social–emotional competence and moral disengagement. Aggressive Behavior, 47(5), 530–541. https://doi.org/10.1002/ab.21959

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying?

Scandinavian Journal of Psychology, 49(2), 147–154. https://doi.org/10.1111/ j.1467-9450.2007.00611.x

Shrestha, N. (2021). Factor analysis as a tool for survey analysis. American journal of Applied Mathematics and statistics, vol. 9, nº 1, pp. 4-11.

Waasdorp, T. E., & Bradshaw, C. P. (2015). The overlap between cyberbullying and traditional bullying. Journal of Adolescent Health, 56(5), 483–488. https://doi.org/10.1016/j.jadohealth.2014.12.002

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *6*(1).

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2014). A review of online grooming: Characteristics and concerns. Aggression and Violent Behavior, 19(1), 62–70. https://doi.org/10.1016/j.avb.2013.11.007



Co-funded by the European Union

Wolbers, H., Cubitt, T., & Cahill, M. J. (2025). Artificial intelligence and child sexual abuse: A rapid evidence assessment. Trends and Issues in Crime and Criminal Justice, 711, 1-18. https://search.informit.org/doi/10.3316/informit.T20250130000125016737888879



Co-funded by the European Union