Safe Digital Teens: an App to Address Technology-Related Risks for Adolescents

Valentina Fietta
valentina.fietta.1@phd.unipd.it
Department of General Psychology
University of Padua
Padua, Italy

Mirko Franco*
mifranco@math.unipd.it
Department of Mathematics
University of Padua
Padua, Italy

Erika De Santis
erika.desantis@studenti.unipd.it
Department of General Psychology
University of Padua
Padua, Italy

Merylin Monaro
merylin.monaro@unipd.it
Department of General Psychology
University of Padua
Padua, Italy

Claudio E. Palazzi
cpalazzi@math.unipd.it
Department of Mathematics
University of Padua
Padua, Italy

Ombretta Gaggi
gaggi@math.unipd.it
Department of Mathematics
University of Padua
Padua, Italy

ABSTRACT

The diffusion of Internet-enabled devices (e.g., smartphones, game consoles, virtual reality (VR) headset, etc.) among adolescents and children has raised several concerns about users' safety, as well as about their awareness on potential online dangers. Besides the numerous digital education initiatives, we believe that learning by facing real-life situations would be more effective in understanding safe and correct ways to engage with others online. In this context, we propose *Safe Digital Teens*, an application composed of different scenarios inspired by real-life situations through which users can learn to face potentially harmful circumstances in a virtual and protected environment. We also present and discuss the results of a preliminary user study.

CCS CONCEPTS

• **Human-centered computing** → **User interface programming**; **User studies**; • **Applied computing** → **E-learning**.

KEYWORDS

mobile app, safe technologies, human-computer interaction

ACM Reference Format:
Valentina Fietta, Mirko Franco, Erika De Santis, Merylin Monaro, Claudio E. Palazzi, and Ombretta Gaggi. 2024. *Safe Digital Teens*: an App to Address Technology-Related Risks for Adolescents. In *International Conference on Information Technology for Social Good (GoodIT '24), September 4–6, 2024, Bremen, Germany*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3677525.3678679

1 INTRODUCTION

Interaction with technology is an increasingly widespread and precocious reality among adolescents and, in some cases, even among children [5]. Children and adolescents, approaching the digital world, expose themselves to a broad spectrum of online content and interactions [13]. Furthermore, this growing tendency proves significant for parents, who often face the complexity of representing constructive and instructive "digital" reference models and regulating their children's use of such devices [36]. This scenario poses educational and safety challenges, highlighting the importance of developing a responsible and aware entrance into the digital world for the adolescent user. An effective response could be adopting a psycho-educational approach based on responsibility [12]. Teaching young adolescents the importance of conscious use of technology and its potential dangers can be essential in training a new generation of digital users and citizens [17, 32]. This education is not limited to the mere technical understanding of the digital environment [11] but includes the promotion of critical and aware thinking about the contents provided to the web and that it provides to us [13].

Going into specifics, young people are exposed to various dangers when they enter the digital world, including online solicitation, both for sexual purposes and to steal content and data. In the literature and recent reports at the global level, it is documented that approximately 13-19% of girls and boys fall into catfish traps with fake profiles or are involved in grooming [38] and these numbers are growing exponentially: 10.2 million reports related to online child exploitation in only 2017 [34]. Sexting may also generate non-consensual pornography problems, developing into anxiety and depression [18] in addition to legal consequences. Furthermore, adolescents fall victim to having personal data stolen from their accounts. Then this data is used through online scams to steal money, or they are exposed to phishing [12, 31] because they provide personal and sensitive data without concerns about their accessibility to everyone. Facilitated access to unsafe content is demonstrated on some platforms that allow minors to access deep web portals where they can purchase anything, including weapons and drugs, or they can have access to pornographic content. For example, Telegram is emerging as a new digital criminal marketplace [28].

The idea of online sharing is also supported by constant geolocation, which allows teenagers to know where they are and with whom. On the one hand, this function can be employed benevolently, such as by parents to monitor the whereabouts of their

*Corresponding author.

GoodIT '24, September 4–6, 2024, Bremen, Germany

ACM ISBN 979-8-4007-1094-0/24/09
https://doi.org/10.1145/3677525.3678679

children. On the other hand, this can represent a severe privacy problem and a good tool for those with bad intentions, like stalking them and letting them know where they are in real time [20].

The net makes people increasingly connected but can also represent a means of disconnection. More and more teenagers demonstrate that they have many online friendships but little in-person contact. Online gaming can lead to isolation and alterations in the sleep-wake cycle, leading to depression if carried out without regulation by parents [26]. This phenomenon has also worsened due to the COVID-19 pandemic, which has forced all adolescents into lockdown at home [14] and at the extreme it leads to the hikikomori phenomenon [21]).

Bullying also moved to social media and online, with 20-40% of American youth experiencing cyberbullying at least once in life [37]. Negative comments and verbal violence are displayed on public pages even more extensively than in school environments, with grave consequences for the victims: they are ridiculed and attacked by multiple bullies hiding under false nicknames and fake profiles. Instead, the famous group of spectators is often the entire social channel [7], so the victim remains helpless, and the virtual crowd, including victims themselves, often does not report abuse [33]. Also new social phenomena are emerging, presenting potential dangers. Adolescents, motivated by the desire for increased social media followers or influenced by peer pressure, may engage in life-threatening challenges [4].

Last, the use of social media leads adolescents to control partners and create friendships incorrectly, with unwritten rules of personal disclosure [8]. Often, these kids could argue or end friendships over a like or a comment on social media for the wrong person or whether they are included in a particular online group [40].

Social media offers opportunities for building relationships when used wisely with guidance and education. Thus, the new generations require support from schools or parents due to the potential dangers they face. However, traditional methods might not be sufficient or engaging. To address this issue, we propose and test an innovative and interactive approach, i.e., an app, *Safe Digital Teens*, about online dangers. This app would teach young people to face potentially harmful situations in a virtual, protected environment. *Safe Digital Teens* acts as an educational and reflection tool for adolescents regarding the dangers deriving from the use of technology. The app aims to help adolescents (15-16 y.o.) to fully understand the consequences and challenges connected to the use of social media and the more general sharing of online content. The app also wants to stimulate critical reflection on the choices carried out daily during interaction with digital platforms. The final aim is to obtain an app for a language suitable for a wider target age group of teenagers exposed to online opportunities and also risks, like boys and girls from 11 years to 16 years [27].

The remainder of this paper is organized as follows. Section 2 presents a review of the relevant literature. Section 3 discusses the methodological aspects of our research, including the app develpment and the methodology used to test the app usability and user experience (UX). Section 4 presents the results on usability and UX, which are discussed in Section 5. Finally, we draw our conclusions and present some future research directions in Section 6.

2 RELATED WORK

According to a report written by the Pew Research Center in 2023 [1], the percentage of teenagers who are almost constantly online has doubled since 2015, raising several concerns about their online safety while using electronic devices (e.g., smartphones, game consoles, virtual reality (VR) headset, etc.) and online social networks (OSNs). In this context, Wisniewski *et al.* [39] analyzed 42 features of 75 Android applications designed to promote adolescent online and mobile safety, mapping them against the proposed framework, namely Teen Online Safety Strategies (TOSS), composed of parent mediation and teen self-regulation strategies. Their findings showed that most of the considered applications adopted parental control over teen self-regulation, failing to teach teenagers the skills needed to engage correctly and safely in online spaces.

Indeed, the perception of the boundaries of teens' privacy widely differs between parents and adolescents, with the latter feeling that their electronic devices (and the content stored within, e.g., text messages) should be private [9]. Moreover, parents often underestimate - or are even unaware of - the children's use of electronic devices and the applications installed in them, including the (online) social circle of the adolescent (i.e., group of people who are socially connected) [3]. In this scenario, Gosh *et al.* [15] observed that parental control applications have a low adoption rate, confirming that teenagers often dislike them as they are considered too restrictive and invasive for privacy.

Considering the issues of parental control applications, some authors investigated how to balance adolescents' need for privacy and their safety and security. For example, McNally *et al.* [29] - acknowledging that children are stakeholders in monitoring applications - involved 12 children aged 7-12 in two co-design workshops to envision future monitoring software designed to be acceptable by children and adolescents while offering privacy and teen-centric features, i.e., methods to cope with risks or notifications in case of harmful behaviors. Gosh *et al.* [16] proposed *Circle of Trust*, an Android app that splits contacts into safe and unsafe and introduces machine learning (ML) based technology (e.g., Amazon Comprehend and Amazon Rekognition) to detect toxic and harmful content in adolescents' communication. In this way, *Circle of Trust* shows the content of the communications to parents only in some cases, i.e., those from or to untrusted contacts, messages flagged as harmful, thus increasing the teenagers' trust and control over their privacy.

Beyond the use of external strategies, education remains a strong weapon in developing a responsible generation able to face the ever-new challenges posed by online spaces (e.g., the metaverse, etc.) [10]. In this context, the scientific community and companies have shared several digital citizenship tools and educational programs, such as Google's "Be Internet Awesome", Meta's Messanger Kids, and Common Sense's Digital Citizenship Curriculum. In this direction, our work advances the current state-of-the-art, presenting *Safe Digital Teens*, an educational app based on direct and acyclic graphs representing scenarios inspired by real-life situations through which users learn safe behaviors and correct ways to engage with others (online).

3 METHODS

In this section, we provide some details about *Safe Digital Teens*, and present the experimental procedure to test usability and UX of the app in a sample of teenagers.

3.1 App Development

Safe Digital Teens is an app developed in Flutter, the cross-platform framework released by Google in 2018. The application provides users with some cards (e.g., Scenario 1, Scenario 2, etc.), each representing a scenario based on real-life situations (e.g., "*You are added to a Whatsapp group where many of your friends are. You didn't expect that. How do you react?*"). Once the user starts a scenario, after a brief initial presentation, he/she can proceed by choosing one of the available answers (e.g., "*It's ok for me, I stay in*", "*I exit from the group*', etc.) (see Figure 1a). Based on that choice, the application shows the next step. This sequence is repeated until the final step is reached, which can have either a positive (e.g., *"I talk to my parents and we report the user"*) or negative outcome (e.g., *"I closed my account, and I'll no longer do that, even if I liked"*). Once the final step is reached, the application provides users with a brief explanation of the outcome with a view on education and risk prevention (see Figure 1b). Finally, users can review all their choices, each with an indication of severity (green, yellow, or red) and, in some cases, even with a motivation (e.g., "*I'm asking my friend to do an unfair action*"). A comprehensive example is presented in Figure 1. The topics of the scenarios are briefly described below.

(1) New Whatsapp Group: this scenario investigates the social dynamics within WhatsApp groups, focusing on peer exclusion and friend loyalty themes, such as online discussions or collateral screenshots exchange interactions.
(2) New Follower: this scenario examines the potential risks of online grooming, including exposure to non-consensual pornography and possible catfishing or stalking in the real world.
(3) Cyberbullying: in this scenario, an adolescent faces hypothetical negative comments and online insults directed at their content. The individual must decide how to respond to such cyberbullying through aggression, thereby perpetuating a negative cycle, or by taking appropriate security measures, and maintaining their interest in posting content.
(4) Loyalty Test: it explores the social dynamics within a teenage couple, where one partner attempts to control the other's behaviour and test their loyalty using fake profiles or involving friends. The final message is that using social media for such purposes is generally dysfunctional and disrespectful to the partner, regardless of their loyalty.
(5) Online Gaming: this scenario presents various choices in online gaming that could expose adolescents to phishing, downloading viruses, or illegal and age-inappropriate content (such as violent or pornographic videos). Additionally, it explores the impact on real-life friendships and the potential disruption of sleep/wake cycles and academic progress due to late-night gaming.
(6) Stealing content: users are prompted to carefully consider the public sharing of their online content and the risks associated with the dissemination of their content by others, including identity theft.
(7) Real-time Geolocation: this scenario involves sharing personal location information with unknown users on Snapchat, potentially leading to physical stalking or actual theft while the user is away from home.
(8) Exes and Social Networks: Ttis scenario explores the situation of an ex-partner who engages in online stalking and threatens to inflict non-consensual pornography.
(9) Challenge: this scenario begins with the Black Out challenge on TikTok, which poses potential life-threatening risks. It presents various choices, including whether or not to participate in the challenge, influenced by personal motivations and peer pressure.

In general, the positive outcomes of the scenarios involved asking for help, at least from friends and parents, to deal with online difficulties, even by turning to the authorities or to secure oneself by removing oneself from a possible danger.

The application already supports both Italian and English, depending on the system language of the mobile device where it is running. Scenarios can be written in any language.

3.2 Participants

Data collection occurred at a local scientific high school in North Italy on 13th May 2024. We recruited 22 teenagers from a second-year class to test the app (13 females = 59% and 9 males = 41%; age M = 15.45, SD = 0.51; years of education = 10). The research activities took place in their classroom during school hours. Data collection was carried out in agreement with the institutions and with the consent of the parents of minor users. Parents have received and provided the Informed Consent for participation of their children in the study. The experimental procedure was approved by the Ethics Committee for Psychological Research of University of Padua.

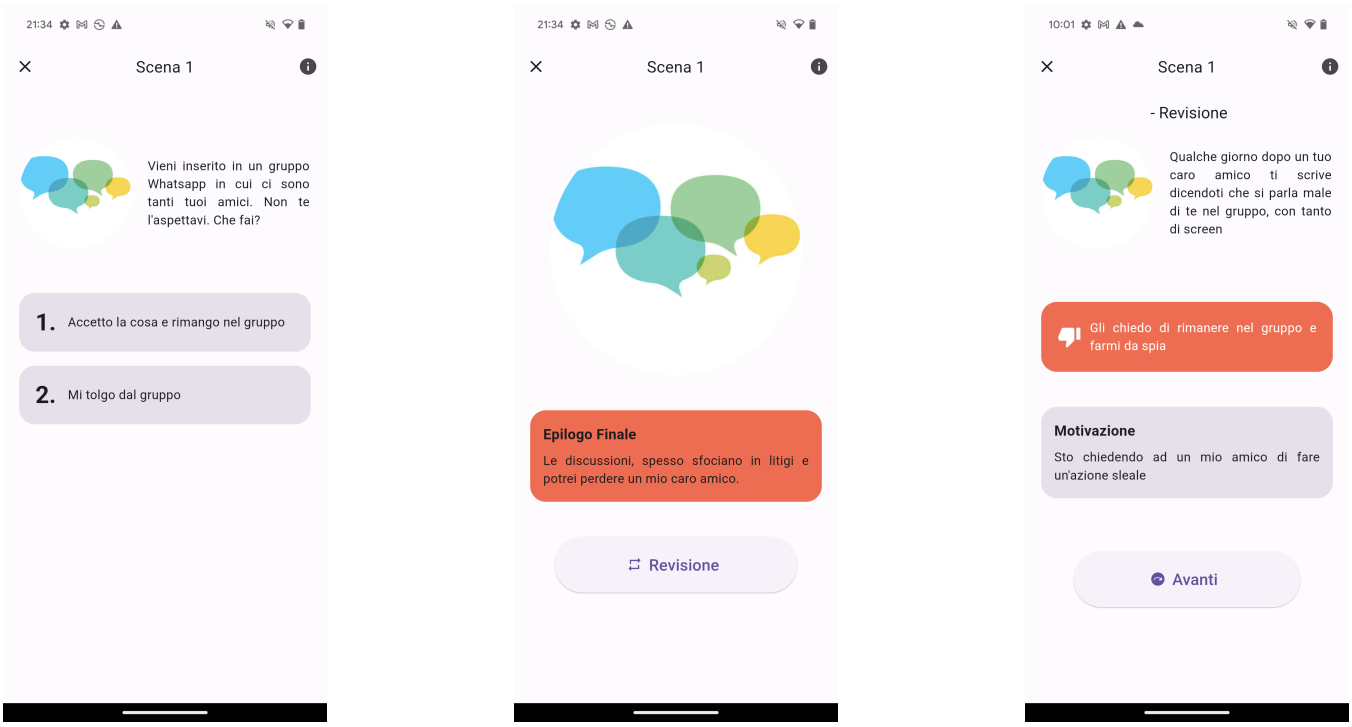
3.3 Experimental Procedure

The users' test of the app was articulated in three main phases, as follows.

3.3.1 PHASE 1: use of Safe Digital Teens. After a short presentation of the project, the adolescents tested the application. The class received 11 smartphones with preinstalled *Safe Digital Teens*. Students were then divided into couples and provided with a phone. Adolescents were free to interact with the application and consult each other regarding the answers to the different scenarios. This phase ended when all groups of users completed the available scenarios.

3.3.2 PHASE 2: questionnaires' administration. Teenagers were asked to answer to the following questionnaires to collect personal information and obtain feedback about their overall experience with the app:

- the ad-hoc demographic questionnaire collects information such as gender, age, ownership of digital devices, freedom of use of these technological tools, number and type of social accounts, and time spent online on various devices (e.g., mobile phone/tablet/PC/VR headset/game console) for social or gaming purposes;



(a) (b) (c)

Figure 1: Scenario 1 of *Safe Digital Teens*: (a) First Step (b) Final Step (c) Feedback. The situation presented in the first step is "*You are added to a WhatsApp group where many of your friends are. You didn't expect that. How do you react?*". The available answers are "*It's ok for me, I stay in*" and "*I exit from the group*". The presented final (negative) outcome is "*Discussions often result in arguments, and I may lose a close friend.* ". In some cases, the application motivates the outcome of an answer. In the presented case, the situation is "*A few days later, a close friend of yours informs you that someone is talking ill of you in the group and sends you the screenshots*" and the user's answer is "*I ask my friend to stay in the group and let me know what they say*". This answer is not a fair choice among those available and the motivation is "*I am asking a friend of mine to do an unfair action*".

- the ad-hoc evaluation questionnaire consists of a series of items with answers on a 5-point Likert scale from 1 ("*not at all*") to 5 ("*yes, a lot*") that collect the opinions of users on the application (e.g., whether the app addresses current issues and is useful for the target group of teenagers);
- the System Usability Scale (SUS) [6] evaluates the usability of the app and consists of 10 items evaluated on a 5-point Likert scale to report agreement with sentences, ranging from 1 ("*strongly disagree*") to 5 ("*strongly agree*"). It provides an overall score that reflects the ease of use and applicability of the system with sentences such as "I found the system very simple to use";
- the User Experience Questionnaire (UEQ) [25, 35] provides a comprehensive view of the experience with the interactive product. The 26 items are made up of pairs of adjectives with opposite meanings divided into 6 topics: efficiency, perspicuity, reliability, novelty, stimulus, attractiveness (e.g., *"impractical – practical", "boring – exciting"*), with a response scale of seven points. Results can be interpreted by comparing the obtained scores with a benchmark data set containing data from 20190 users from 452 studies concerning different products (business software, web pages, web shops, social networks);
- the User Engagement Scale-Short Form (UES-SF) [30] measures user engagement with digital technology across four factors: focused attention, perceived usability, aesthetic appeal, and reward factor. It is a self-report measure composed of 12 items rated on a 5-point Likert scale, ranging from 1 ("*strongly disagree*") to 5 ("*strongly agree*"). A total score and scores for each of the four subscales are calculated by summing the single item scores.

3.3.3 PHASE 3: Focus group. Focus group on the effects of the use of technology was led by an expert psychologist. Teenagers' suggestions supported the research to be as current as possible and aligned with the needs of modern adolescents, as well as to improve any critical issues and weaknesses. The social scenarios with which the participants interacted while using *Safe Digital Teens* were explored and discussed in a participatory manner. Specifically, the scenarios in which users have previously interacted were represented as decision trees, similar to hierarchical diagrams that

provide a visual guide to the choices required while using the app (as previously illustrated in Figure 1). Focus group investigated the scenarios' comprehensibility (clarity of language).

The data collection was carried out on a single occasion for a total duration of 2 hours. The individual steps will last approximately 1 hour for the test, 15 minutes for the questionnaires and approximately 30 minutes for the focus group.

3.4 Data Analysis

Data analysis was conducted using the JASP software [19]. Descriptive statistics were adopted to investigate the distribution of the sample's answers. The one-sample t-test (t) and the corresponding non-parametric Wilcoxon signed rank test (V) [2] were performed concerning the evaluation questionnaire and the UES-SF measures to determine whether the sample's true mean (σ) statistically differed from the central value of the Likert scale (3 = neutral attitude). The significance threshold of the p-value was set to 0.05.

4 RESULTS

In this section, we report the data about the usability and UX of the application, the results emerging from the questionnaires, and some insights from the focus group.

4.1 Behavioural Data

Each group (of two users) completed each scenario once. In two cases (Scenario 6 and Scenario 9), all the groups ended the scenario in a step with a positive outcome. Conversely, in the case of Scenario 3 and Scenario 4, most groups ended the scenario with a negative outcome. The average completion time of scenarios ranges from 27.07s to 112.40s. A comprehensive summary is reported in Table 1.

4.2 Questionnaire Results

4.2.1 Technology use. Every user in the sample owns at least one technological device to a maximum of four devices among mobile phones, PCs, tablets, VR headsets or game consoles, with a mean per person of 2.68 devices (SD = 0.78). In particular, only 1 teenager owns 1 device (4.55%), 8 teenagers own 2 devices (36.36%), 10 teenagers own 3 devices (45.46%), and 3 teenagers own 4 devices (13.64%).

Regarding the regular use of the above-mentioned devices, all adolescents regularly use their mobile phones (n = 22, 100%), almost all use their PCs (n = 21, 95.45%), a minority of them regularly use tablets (n = 8, 36.36%) and game consoles (n = 5, 22.73%), and only 1 adolescent (4.55%) regularly uses the VR headset.

The majority of the sample feel free to use their mobile phones (63.64%), PCs (63.64%), and tablets (72.73% of users who own them) without parents' control. Instead, the use of VR headsets is more monitored by parents (33.33% no control by parents) and a balanced result is obtained for controlled game console use (50%). To note, that the number of devices is limited in these last two cases (see Figure 2a).

Every adolescent has from a minimum of 2 to a maximum of 9 social networks' accounts with a mean 5.05 accounts (SD = 2.19) per person. The more common socials are WhatsApp (100.00%), Instagram (95.45%), TikTok (68.18%), Snapchat (54.55%) and BeReal (50.00%). Less widespread are YouTube (45.45%), Threads (27.27%), Facebook (22.73%), Twitter (22.73%), Telegram (9.09%), Reddit (4.55%), and Discord (4.55%). Social networks' distribution is reported in Figure 2b.

The time of utilization per day of devices for social networking or gaming online is reported in Table 2 varying from "*never*" to "*more than 6 hours*".

4.2.2 Evaluation questionnaire. From the evaluation questionnaire *Safe Digital Teens* significantly resulted appreciated, not boring, currently targeted about thematic and population to whom it is proposed. Users have a neutral opinion about dialogues and endings as possibly realistic. About usefulness, they think they did not learn many new things about socials and the app did not warn them about situations they were not prepared for. They report the app would be useful to other adolescents of their age but it was not particularly useful for them. All average scores, standard deviations, and Wilcoxon test results are reported in Table 3.

4.2.3 Usability and user experience questionnaires. Regarding standardised questionnaires, SUS scorings range from 65 to 95 with an average score of 84.09 (SD= 7.54). This mean score stands out in the evaluation range of good to excellent evaluation of *Safe Digital Teens* usability, our sample resulted as promotor of the app.

As concerns UX, the six dimensions measured by the UEQ have obtained the following scores: Attractiveness = 1.02 (SD = 0.73), Perspicuity = 2.76 (SD = 0.32), Efficiency = 1.86 (SD = 0.70), Dependability = 1.60 (SD = 0.57), Stimulation = 0.42 (SD = 0.71), Novelty = 0.75 (SD = 0.95). Comparing these scores with those of the benchmark data set, it should be noted that the *Safe Digital Teens* is evaluated as excellent for Perspicuity and good for Efficiency and Dependability (see Figure 3). It is above average compared to other products for Novelty. Instead, Attractiveness is just below average and Stimulation is evaluated as bad.

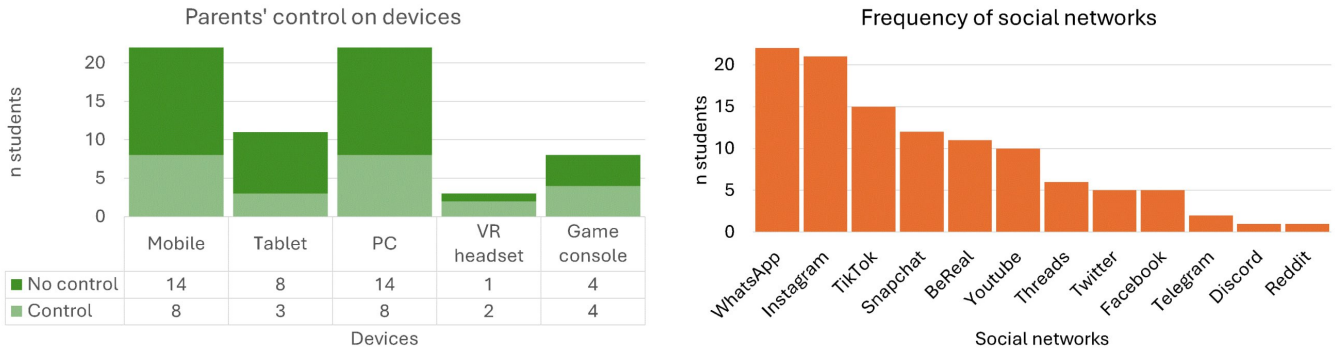
In the UES-SF questionnaire the class reported a significant total high level of engagement; in particular significant positive scores were registered in scales of Perceived Usability and Reward Factor. Instead there were not significant results for Focused Attention and Aesthetic appeal, so the average scores were not significantly different to neutral score of 3. Average UES-SF results and related analysis are reported in Table 4.

4.3 Focus Group Results

The data collected through focus group highlighted several criticisms and suggestions for improving the app. The comments indicate that high school adolescents might not use the app more than once, as they reported the scenarios content as "limited". Due to the perception of having already experienced many situations or knowing how to behave, high school teenagers find the app more suitable for middle school adolescents: "*We have already experienced many of the situations presented in the app or, in any case, how to act in response to them; perhaps it would be more suitable for the little ones, better for middle schools; in high school, you are already an expert.*" They perceive that app's usefulness varies depending on the gender and age of the user, being more suitable for younger boys and girls. Boys might not take it seriously at 15/16 years old, while some situations are more relevant for girls due to higher risks: "*The app's usefulness depends on the user. Some may not take it*

Table 1: Percentage of Positive and Negative Outcomes and Average Completion Time for Each Scenario

Scenario	Title	Positive Outcomes (%)	Negative Outcomes (%)	Average Completion Time (s)
1	New Whatsapp Group	50	50	103.96
2	New Follower	90.91	9.09	67.93
3	Cyberbullying	27.27	72.73	99.12
4	Loyalty Test	9.09	90.91	112.40
5	Online Gaming	72.73	27.27	48.34
6	Stealing Content	100	0	88.16
7	Real-time Geolocation	90	10	27.07
8	Ex and Social Networks	70	30	92.93
9	Challenge	100	0	91.30



(a) (b)

Figure 2: (a) Sample perception of parents' control on technological devices (b) Frequency distribution of social networks' use in the sample

Table 2: Freqeuncy distribution of daily time spent on socials or gaming

Time per day of socials or gaming	Mobile		Tablet		PC		VR headset		Game console	
	n	%	n	%	n	%	n	%	n	%
never	0	0	1	4.55	3	13.64	0	0	0	0
few minutes	0	0	4	18.18	7	31.82	0	0	3	13.64
less than 1 hour	2	9.09	2	9.09	6	27.27	1	4.55	0	0
from 1 to 2 hours	8	36.36	1	4.55	4	18.18	0	0	5	22.73
from 2 to 6 hours	10	45.45	1	4.55	2	9.09	0	0	0	0
more than 6 hours, I can't measure it	2	9.09	0	0	0	0	0	0	0	0

seriously. Certain risks are more prevalent for women." Additionally, it was suggested to advise talking to a responsible adult, not only parents, given the variability of family relationships: "*The advice to talk with parents is not always applicable to everyone. Many people may not do so because they don't have a good relationship with their parents. It might be better to seek guidance from a responsible adult instead.*".

The app was considered helpful for consultation, with the suggestion to integrate it into a chat on a social network to allow users to ask for advice on how to behave in specific situations in real time, functioning as an integrated extension or chatbot. Moreover, they suggested more sophisticated and dynamic tools. The app's interface was judged sparse. It was suggested that AI-generated images or animations be included to make the app more dynamic and game-like. The app's use was extremely simple, with clear feedback for various combinations and options, defined deadlines, and final reviews. However, the importance of providing reasons for all feedback, including less negative ones, was emphasized. Further improvements were proposed, such as introducing different colors for intermediate severity revisions and selecting gender at the beginning of the app to tailor scenarios to the user's gender.

Table 3: Evaluation questionnaire scores and their related one-sample Wilcoxon tests.

Evaluation Questionnaire						95% CI for Hodges-Lehmann Estimate				95% CI for Rank-Biserial Correlation	
Items	Mean	SD	V	p	Hodges-Lehman Estimate	Lower	Upper	Rank-Biserial Correlation	SE Rank-Biserial Correlation	Lower	Upper
Did you like the app?	3.41	0.67	50.00	**<.05**	1.00	0.00	1.50	0.82	0.34	0.42	0.95
Was the app boring?	2.27	0.83	15.00	**<.01**	-1.00	-1.50	-1.00	-0.80	0.27	-0.93	-0.51
Do you think the issues addressed are current?	4.41	0.59	231.00	**<.001**	1.50	1.00	1.50	1.00	0.24	1.00	1.00
Do the issues addressed concern boys and girls of your age?	4.18	0.73	171.00	**<.001**	1.50	1.00	1.50	1.99	0.26	1.00	1.00
Are the issues addressed outdated and no longer current?	1.77	0.87	5.00	**<.001**	-1.50	-2.00	-1.00	-0.95	0.26	-0.98	-0.86
Are the dialogues and conclusions to which the app leads you realistic?	3.27	0.83	41.00	0.16	1.00	-0.5	1.00	0.49	0.34	-0.16	0.84
Did the app help you learn new things?	2.18	0.66	0	**<.001**	-1.00	-1.50	-1.00	-1.00	0.29	-1.00	-1.00
Is the app useful for you?	2.41	0.85	4.00	**<.01**	-1.50	-1.50	-0.5	-0.88	0.33	-0.97	-0.61
Is the app useful for other adolescents of your generation?	3.59	0.80	73.00	**<.01**	1.00	1.00	1.50	0.87	0.32	0.60	0.96
Did the app warn you about situations you were not prepared for?	2.41	1.14	32.50	**<.05**	-1.00	-1.50	-53.13	-0.58	0.27	-0.83	-0.11

Table 4: UES-SF scores and their related one-sample t-tests and Wilcoxon tests. Note: For the Student t-test (t), effect size is given by Cohen's d; the location difference estimate is given by the sample mean difference d; the alternative hypothesis specifies that the mean is different from 3. For the Wilcoxon test (V), effect size is given by the matched rank biserial correlation; the location difference estimate is given by the Hodges-Lehmann estimate and the alternative hypothesis specifies that the median is different from 3.

UES-SF								95% CI for Location Difference				95% CI for Effect Size	
	M	**SD**	**Test**	**Statistic**	**df**	**p**	**Location Difference**	**Lower**	**Upper**	**Effect Size**	**SE Effect Size**	**Lower**	**Upper**
Total	3.32	0.34	t	4.39	21	**<.001**	0.32	0.17	0.48	0.94	0.26	0.42	1.43
Focused Attention	3.14	0.75	t	0.86	21	0.40	0.14	-0.20	0.47	0.19	0.22	-0.24	0.60
Perceived Usability	3.61	0.62	V	171.00		**<.01**	0.83	0.67	1.00	0.80	0.26	0.53	0.92
Aesthetic Appeal	2.69	0.50	t	-0.43	21	0.67	-0.05	-0.27	0.18	-0.09	0.21	-0.51	0.33
Reward Factor	3.59	0.60	V	193.00		**<.001**	0.67	0.33	1.00	0.84	0.25	0.61	0.94

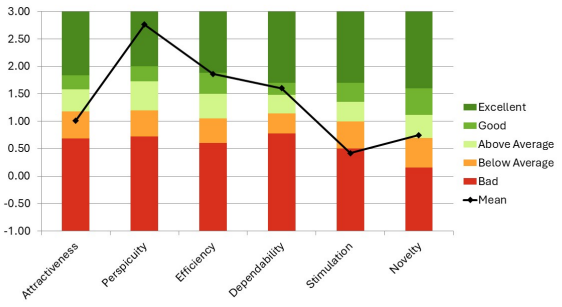


Figure 3: UEQ results compared to the benchmark data set.

Finally, new scenes were suggested to make the app more complete and realistic: scenarios of profile hacking through a link, recognizing fake friendships on social media, peer pressure to do "*foolish things*", avoiding people who cause fights, consequences of threats on social media, and scenarios for those who might unknowingly cause harm to others.

5 DISCUSSION

The data collected from this study provide considerable insights for the future development of the *Safe Digital Teens* app and, more broadly, on the experiences of the adolescents in terms of technological device use and perception of dangers related to the web, social media and online gaming. Parental control is infrequent for mobile phones and PCs, which are teenagers' most regularly used devices. This reveals the significant discrepancy between teenagers' need for independence in using these devices and the protective measures taken by parents. Given that every teenager now possesses at least one device, they are consistently connected to the digital world, exposing them to opportunities as well as potential dangers, even more without parental support [22]. This reality is further highlighted by the fact that all sampled teenagers are active on at least two social networks. Specifically, messaging apps like WhatsApp and multimedia-sharing platforms like Instagram and Snapchat are the most widely used among participant teenagers. These results underscore the importance of the selected scenarios developed for our app, which accurately reflect the current usage of social networks. From the collected data, the perceived time spent on different devices varies, but it is evident that mobile phones are the most used, with usage times ranging from just under an hour to more than six hours for some users. PCs and tablets also have

significant usage times, ranging from a few minutes to over six hours daily. This variation underscores the personal nature of device use among teenagers and highlights that mobile phones are the primary means for connecting and playing online. Consequently, our mobile app is well-suited for availability on teenagers' mobile phones as a feasible everyday tool.

Evaluation questionnaires indicate that the prototype of our app is perceived as engaging and relevant to ongoing social situations among adolescents. However, some feedback suggests that the realism of the proposed scenarios could be improved. Moreover, adolescents deemed that the represented situations would not possibly affect them. Indeed, they thought they already knew how to act in the situations proposed and that this app would be useful for younger generations. In addition, they stated that this app could be more beneficial for other teenagers of their age but not for them. In psychological terms, there is a sort of unconsciousness and distance from the probability that a dangerous, risky and grave situation could happen directly to them. These phenomena are called optimistic bias and subjective invulnerability [23]. Furthermore, even considering the possibility it could happen to them, they assume (as reported) to know how to act and control the situation appropriately. However, from the preliminary results, an average percentage of 32.2% (range from 0% to 90.91%) of the responses came out as unfavourable from our app. In other words, they are not actually prepared to act appropriately when they face all online risky situations. For example, 72.73% and 90.91% of the groups ended Scenario 3 and Scenario 4 with a negative outcome, respectively, while 100% of the groups successfully completed Scenario 6 and Scenario 9 with a positive outcome. Furthermore, the focus group's opinions supported the app's usefulness more for girls and young adolescents. This widespread phenomenon also emerges from the literature according to which older and male adolescents underestimate the risks associated with social networks [24]. For this reason, they must be targeted through engaging apps and tools like *Safe Digital Teens*, to convince them that they are not immune to possible risky situations online. This optimistic bias, prevalent among adolescents, may lead them to appear disinterested. However, creating a more engaging app could be beneficial towards our objectives of increasing safety.

From a research point of view, it could be helpful in future to propose a pre- and post-measurement of the perception of the dominance of a risky online situation, of the fundamental knowledge of "*how to act if...*" and the perception also of the possible dangers in socials and gaming online. This measurement could be valuable in exploring the probable discrepancy between self-reported confidence and the results of the app, as well as the efficacy of the psychoeducation given by the app *Safe Digital Teens*.

The SUS, UEQ, and UES-SF questionnaires' results comprehensively depict the *Safe Digital Teens* app's usability and UX. The high SUS score demonstrates overall solid usability, confirmed by the UES-SF results about high perceived usability and reward. The UEQ scores highlight strengths in perspicuity, efficiency, and dependability while pointing out areas for improvement in attractiveness and stimulation, as well as similar results obtained in the focused attention and aesthetic appeal scales of the UES-SF. Overall, while the *Safe Digital Teens* app is well-regarded for its ease of use and rewarding experience, improving visual appeal, engagement, and innovative features could elevate the UX from good to excellent across all dimensions.

Finally, discussions from the focus group provide valuable insights for contextualizing and enhancing the quantitative findings. Participants suggested that while the app has high usability, its content, design, and interface may not sufficiently engage older teens or repeat users. For instance, introducing more gamification and animation content or integrating the app as a supporting chatbot could be helpful. These comments align with the low stimulation scores and indicate a need to enhance the app's long-term engagement and visual appeal attractiveness strategies. Instead, positive comments reinforced the high perspicuity, efficiency, and dependability scores from the UEQ and, generally, the app's clarity and ease of use.

6 CONCLUSION AND FUTURE DIRECTIONS

Safe Digital Teens was developed as a prototype to test its level of acceptability and perceived usefulness. Future developments will align with the feedback provided by teenagers: incorporating more dynamic and interactive elements, improving the visual appeal, and integrating social media features could significantly enhance user satisfaction and engagement, making the app more appealing to broader and more diverse user populations. Furthermore, in future, the research's next steps will focus on testing the efficacy of the app and its utility after modifying and integrating the usability aspects that emerged from the prototype test described here. For example, future developments include the introduction of gamification elements, such as avatars, points, and badges, as well as enhanced progress monitoring with feedback messages about the improvements made using the app.

Indeed, with the synergistic collaboration between professionals in the IT and psychological fields, our research group aims to create an accessible and exciting application for adolescents. Considering our future target population (11-16 years), the application will be designed with a language suitable for the age group, ensuring the content is relevant and understandable for all users. In addition to being more interactive and engaging, the app could contribute to responsible technological education and the safest use of social media by the individual adolescent user. To conclude, our future challenges will consist of creating an app that can help train a generation of aware, responsible and resilient users online, counting on teenagers' precious suggestions and feedback presented in this study.

ACKNOWLEDGMENTS

The authors would like to thank all the students of the "Liceo Tron Zanella" who participated in the research. The authors would also like to thank Alessandro Cavaliere for the app development. This research was supported by the Department of Mathematics of the University of Padua (SID project: "*A tool to spread accessibility culture through gamification*"). Responsibility of the content resides with the authors.

REFERENCES

[1] Monica Anderson, Michelle Faverio, and Jeffrey Gottfried. 2023. Teens, Social Media and Technology | Pew Research Center. https://www.pewresearch.org/

internet/2023/12/11/teens-social-media-and-technology-2023/. Accessed 4th June 2024.

[2] Andy P. Field and Jeremy Miles and Zoe Field. 2012. *Discrovering Statistics Using R.* SAGE Publications Ltd.: Southend Oaks,.

[3] Lindsay Blackwell, Emma Gardiner, and Sarita Schoenebeck. 2016. Managing Expectations: Technology Tensions among Parents and Teens. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (San Francisco, California, USA) *(CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 1390–1401. https://doi.org/10.1145/2818048.2819928

[4] Gianluca Bonifazi, Silvia Cecchini, Enrico Corradini, Lorenzo Giuliani, Domenico Ursino, and Luca Virgili. 2022. Investigating community evolutions in TikTok dangerous and non-dangerous challenges. *Journal of Information Science* 0, 0 (2022), 01655515221116519. https://doi.org/10.1177/01655515221116519

[5] Elena Bozzola, Giulia Spina, Rino Agostiniani, Sarah Barni, Rocco Russo, Elena Scarpato, Antonio Di Mauro, Antonella Stefano, Cinthia Caruso, Giovanni Corsello, and Annamaria Staiano. 2022. The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks. *International Journal of Environmental Research and Public Health* 19 (08 2022), 9960. https://doi.org/10.3390/ijerph19169960

[6] John Brooke. 1996. *SUS – a quick and dirty usability scale.* 189–194.

[7] Margaret Anne Carter. 2013. Third Party Observers Witnessing Cyber Bullying on Social Media Sites. *Procedia - Social and Behavioral Sciences* 84 (2013), 1296–1309. https://doi.org/10.1016/j.sbspro.2013.06.747 The 3rd World Conference on Psychology, Counseling and Guidance, WCPCG-2012.

[8] Rui Chen. 2013. Living a private life in public social networks: An exploration of member self-disclosure. *Decision Support Systems* 55, 3 (2013), 661–668. https://doi.org/10.1016/j.dss.2012.12.003

[9] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 19–35. https://www.usenix.org/conference/soups2014/proceedings/presentation/cranor

[10] Dominic DiFranzo, Yoon Hyung Choi, Amanda Purington, Jessie G. Taft, Janis Whitlock, and Natalya N. Bazarova. 2019. Social Media TestDrive: Real-World Social Media Education for the Next Generation. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3290605.3300533

[11] Stefan C. Dombrowski, John W. LeMasney, Chikezie Emmanuel Ahia, and Shannon A. Dickson. 2004. Protecting Children From Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations. *Professional Psychology: Research and Practice* 35 (2004), 65–73.

[12] Munita Dunn-Coetzee. 2015. A psycho-educational strategy as tool for educating adolescents on internet safety. *The Social Work Practitioner-Researcher* 27, 3 (2015), 306–321. https://doi.org/10.10520/EJC186401

[13] David Finkelhor, Kerryann Walsh, Lisa Jones, Kimberly Mitchell, and Anne Collier. 2021. Youth Internet Safety Education: Aligning Programs With the Evidence Base. *Trauma, Violence, & Abuse* 22, 5 (2021), 1233–1247. https://doi.org/10.1177/1524838020916257

[14] Jeff Gavin and Mark Brosnan. 2022. The Relationship Between Hikikomori Risk and Internet Use During COVID-19 Restrictions. *Cyberpsychology, Behavior, and Social Networking* 25, 3 (2022), 189 – 193. https://doi.org/10.1089/cyber.2021.0171

[15] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr, and Pamela J. Wisniewski. 2018. Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (, Montreal QC, Canada,) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173698

[16] Arup Kumar Ghosh, Charles E. Hughes, and Pamela J. Wisniewski. 2020. Circle of Trust: A New Approach to Mobile Online Safety for Families. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (, Honolulu, HI, USA,) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376747

[17] Benjamin Gleason and Sam von Gillern. 2018. Digital citizenship with social media: Participatory practices of teaching and learning in secondary education. *Educational Technology and Society* 21 (01 2018), 200–212.

[18] Manuel Gámez-Guadix, Estibaliz Mateos-Pérez, Sebastian Wachs, Michelle Wright, Jone Martínez, and Daniel Íncera. 2022. Assessing image-based sexual abuse: Measurement, prevalence, and temporal stability of sextortion and nonconsensual sexting ("revenge porn") among adolescents. *Journal of Adolescence* 94, 5 (2022), 789–799. https://doi.org/10.1002/jad.12064

[19] JASP Team. 2020. JASP. https://jasp-stats.org. Accessed 4th June 2024.

[20] Alice Karanja, Daniel W. Engels, Ghizlane Zerouali, and Ariel Francisco. 2018. Unintended consequences of location information: Privacy implications of location information used in advertising and social media. *SMU Data Science Review* 1, 3 (2018).

[21] Takahiro A. Kato, Shigenobu Kanba, and Alan R. Teo. 2019. Hikikomori: Multidimensional understanding, assessment, and future international perspectives. *Psychiatry and Clinical Neurosciences* 73, 8 (2019), 427–440. https://doi.org/10.1111/pcn.12895

[22] Govindappa Lakshmana, Sekar Kasi, and Mubarak Rehmatulla. 2017. Internet use among adolescents: Risk-taking behavior, parental supervision, and implications for safety. *Indian Journal of Social Psychiatry* 33 (01 2017), 297. https://doi.org/10.4103/0971-9962.218603

[23] Daniel K. Lapsley and Patrick L. Hill. 2010. Subjective invulnerability, optimism bias and adjustment in emerging adulthood. *Journal of Youth and Adolescence* 39, 8 (2010), 847 – 857. https://doi.org/10.1007/s10964-009-9409-9

[24] Arkaitz Lareki, Juan Ignacio Martínez de Morentin, Jon Altuna, and Nere Amenabar. 2017. Teenagers' perception of risk behaviors regarding digital technologies. *Computers in Human Behavior* 68 (2017), 395–402. https://doi.org/10.1016/j.chb.2016.12.004

[25] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and Evaluation of a User Experience Questionnaire. *USAB 2008* 5298, 63–76. https://doi.org/10.1007/978-3-540-89350-9_6

[26] Sakari Lemola, Serge Brand, Nicole Vogler, Nadine Perkinso-Gloor, Mathias Allemand, and Alexander Grob. 2011. Habitual computer game playing at night is related to depressive symptoms. *Personality and Individual Differences* 51 (04 2011), 117–122. https://doi.org/10.1016/j.paid.2011.03.024

[27] Sonia Livingstone and Ellen Helsper. 2010. Balancing opportunities and risks in teenagers' use of the internet: the role of online skills and internet self-efficacy. *New Media & Society* 12, 2 (2010), 309–329. https://doi.org/10.1177/1461444809342697

[28] D.L.M. Lummen. 2023. Is Telegram the new Darknet? A comparison of traditional and emerging digital criminal marketplaces. http://essay.utwente.nl/94687/

[29] Brenna McNally, Priya Kumar, Chelsea Hordatt, Matthew Louis Mauriello, Shalmali Naik, Leyla Norooz, Alazandra Shorter, Evan Golub, and Allison Druin. 2018. Co-designing Mobile Online Safety Applications with Children. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (, Montreal QC, Canada,) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3173574.3174097

[30] Heather O'Brien, Paul Cairns, and Mark Hall. 2018. A Practical Approach to Measuring User Engagement with the Refined User Engagement Scale (UES) and New UES Short Form. *International Journal of Human-Computer Studies* 112 (04 2018). https://doi.org/10.1016/j.ijhcs.2018.01.004

[31] Rosemary Cosmas Tlatlaa Panga, Janeth Marwa, and Jema David Ndibwile. 2022. A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania. *Journal of Cybersecurity and Privacy* 2, 3 (2022), 466–489. https://doi.org/10.3390/jcp2030024

[32] Luci Pangrazio and Lourdes Cardozo-Gaibisso. 2020. Beyond cybersafety: The need to develop social media literacies in pre-teens. *Digital Education Review* (06 2020), 49–63. https://doi.org/10.1344/der.2020.37.49-63

[33] Erin Peebles. 2014. Cyberbullying: Hiding behind the screen. *Paediatrics & child health* 19 (12 2014), 527–8. https://doi.org/10.1093/pch/19.10.527

[34] Tatiana R. Ringenberg, Kathryn C. Seigfried-Spellar, Julia M. Rayz, and Marcus K. Rogers. 2022. A scoping review of child grooming strategies: pre- and post-internet. *Child Abuse & Neglect* 123 (2022), 105392. https://doi.org/10.1016/j.chiabu.2021.105392

[35] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. 2014. Applying the User Experience Questionnaire (UEQ) in Different Evaluation Scenarios. In *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience*, Aaron Marcus (Ed.). Springer International Publishing, Cham, 383–392.

[36] Nili Steinfeld. 2021. Parental mediation of adolescent Internet use: Combining strategies to promote awareness, autonomy and self-regulation in preparing youth for life on the web. *Education and Information Technologies* 26 (03 2021). https://doi.org/10.1007/s10639-020-10342-w

[37] Robert S. Tokunaga. 2010. Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior* 26, 3 (2010), 277–287. https://doi.org/10.1016/j.chb.2009.11.014

[38] Helen Whittle, Catherine Hamilton-Giachritsis, Anthony Beech, and Guy Collings. 2013. A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior* 18, 1 (2013), 62–70. https://doi.org/10.1016/j.avb.2012.09.003

[39] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 51–69. https://doi.org/10.1145/2998181.2998352

[40] Elena Zheleva and Lise Getoor. 2009. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th International Conference on World Wide Web* (Madrid, Spain) *(WWW '09)*. Association for Computing Machinery, New York, NY, USA, 531–540. https://doi.org/10.1145/1526709.1526781