Teaching cybersecurity: the evaluation of Nabbovaldo and blackmail from space

Giorgia Bassi[1], Stefania Fabbri[1] and Angela Franceschi[1,2]

[1] Istituto di Informatica e Telematica (IIT), Consiglio Nazionale delle Ricerche
Via Giuseppe Moruzzi 1, 56124 – Pisa, Italy
[2] Department of Education, Languages, Interculture, Literature and Psychology (FORLILPSI), University of Florence
Via di San Salvi, 12 – Padiglione 26, 50135 – Florence, Italy

Corresponding author: angela.franceschi@iit.cnr.it

Abstract. Interventions to raise awareness and promote cybersecurity behaviors have recently become widespread, but much still needs to be done to broadcast this knowledge on a large scale. Video games (i.e., serious games), can represent a valuable way of building digital skills because they are shown to improve learning through active involvement, by increasing and motivating emotional connection to content. The Ludoteca del Registro .it developed a video game named "Nabbovaldo and blackmail from space". In this study, 270 students (M_{age} = 12.66, SD = .70) from four different schools in Tuscany were involved in a project aiming: (a) to evaluate the video game in terms of satisfaction and usability, (b) to understand the effectiveness in improving cybersecurity knowledge. The results show that the video game was appreciated by the students. A great improvement emerges in the student's cybersecurity knowledge, particularly for those who have played the videogame. Video games represent an extremely important educational tool, to be exploited and further integrated within our schools. Future studies have to replicate these results, adding a control group to reach a more structured research design.

Keywords: Videogame, Serious Game, Cybersecurity.

1 Introduction

Children and adolescents spend a lot of time on the Internet, an instrument used for many different activities: studying, watching movies and/or TV series, making new friends, and keeping in touch with others [1, 2]. The usage of Internet, with its numerous benefits, opens up space for new possibilities of communication and learning, but it is also important to underline the different risks and dangers that come with it [3]. A survey by EUKids online [4], conducted on 25.101 children between the ages of 9 and 16 and belonging to nineteen European countries, shows that 11% of participants reported data abuse. Although there are differences between the countries, these data tell us that most children are often not aware of online problems. In Italy, communication and interaction skills in young people are well developed; on the contrary, those related to content creation and navigation are still low [5].

But it is precisely by surfing the Internet in an unsafe way that you can be vulnerable to cyber-attacks. If children spend so much time on the Internet, they must be aware of cybersecurity. Indeed, even on the Internet, there are rules to follow and to respect, to protect both the users and the website integrity. However, the terms of conditions and use of a website are hardly ever read by those who surf within the websites [6]. If this is true for adults, it is even more true for children. As well documented in some studies [7], this is due to several factors: indeed, users struggle to grasp all the implications of the clauses they find and often end up not reading them, but still accepting the terms of use to be able to access the website. This is an example of insufficient attention we often have when browsing online, and it is precisely this lack of focus that makes us potentially vulnerable to cyber-attacks.

Interventions to raise awareness and promote cybersecurity behaviors have recently become widespread, but much still needs to be done to broadcast this knowledge on a large scale [8]. While many prevention programs for online dangerous behaviors (i.e., cyberbullying, online sexual exploitation, etc.) have been developed, few frameworks have focused on issues such as online fraud, hacking, and identity theft. These kinds of problems should not be underestimated [9].

Among the many skills that a child or adolescent must develop, learning to navigate the Internet safely should be included. Although in the first phase of the Internet's usage parents can use some parental control tools, the development of autonomy is one of the key points in the growth of young people [10]. Moreover, is not easy to understand the practical implications of personal information's promulgation. In many cases, people don't realize how much sensitive private content is shared online, and how this can represent a source of vulnerability [11].

Video games (i.e., serious games), can represent a valuable way of building digital skills because they are shown to improve learning through active involvement, by increasing and motivating emotional connection to content. Furthermore, they are easily adaptable to different types of learning [12, 13]. These games are based on experiential learning, which favors "learning by doing" [14]. Thanks to the usage of video games, children can be more involved in learning and testing their skills in a safe environment.

The ability to actively explore reality allows you to convey messages much more effectively than theoretical lectures. Within the game it is also possible to act in a "protected" space: both because one can make mistakes without encountering consequences that have too much impact on the person, and because one can act without being judged, and this favors the most spontaneous choice [15]. The game has always been a privileged modality to convey educational messages, and in this logic, videogames represent nothing more than their "extension" in the virtual world.

1.1 Serious game on cybersecurity: state of art and the novelty of Nabbovaldo

Some video games aiming to educate on cybersecurity have already been developed. For example, CyberCIEGE [16], sponsored by the US Navy and used by government agencies and universities; BigBro [17] and CyberCraft [18], developed by engineering

students. All these video games aiming to train the player on cybersecurity, with multiple choice quizzes and a progress monitoring system. However, they require a fairly good basic knowledge of the topics.

Another example is the video game Cybercity Chronicles [19], set in a hypothetical reality of the year 2088 with special agents fighting powerful hackers, a captivating scenery but no adherent to the real and daily online life experiences of the children.

The video game "Nabbovaldo and blackmail from cyberspace" is therefore included in this field, and have some strengths: scenarios and situations presented recall the online life of today's teenagers. Furthermore, it is designed to be brought into the classroom, and therefore to work at school level, and for this reason a desktop version has also been designed. It therefore represents a unicum in the panorama of educational resources dedicated to these topics.

1.2 Ludoteca del Registro .it

The Ludoteca del Registro .it is a digital education project that was born in 2011 as part of the Registro .it, the Registry of Italian domains. In 2013 Ludoteca received the patronage of the Guarantor for Children and in 2019 became a member of the advisory board of the Safer Internet Center Italy [20]. Since 2011, the staff of Ludoteca has met more than 16,000 students, all over Italy and beyond. The mission of Ludoteca del Registro .it is to spread the culture of the Internet to new generations, from primary school to high school. Over time, the goal has always been to find fun ways for teaching the correct use of the Internet, the main topic of this project: its functioning and resources, its history, and its organization. Without knowing the Internet, students cannot fully appreciate its opportunities. The Ludoteca has developed various tools, including the Internetopolis web app and the comics of Nabbovaldo. Recently, the focus shifted to cybersecurity, which is becoming crucial in all contexts of daily life. The idea of developing a framework for IT security arises from the need to promote the culture of IT security in young people, stimulating the adoption of "IT hygiene" practices based on a preventive approach, and knowledge of risks. It is increasingly important to protect) devices and data, to recognize and intervene on cyberspace’s risks. To achieve these skills, it is necessary to have some basic techniques: knowledge about threats and computer systems; main types of attacks; countermeasures. But how can young people be actively involved in this type of learning?

1.3 Design Implementation and Development of “Nabbovaldo and blackmail from cyberspace”

Before designing the videogame, a feasibility study was implemented. The type of game chosen for the study was a graphic adventure with multiple-choice dialogues, alternated with puzzle and/or arcade-style mini-games, for a total duration of about 1 hour of continuous gameplay. The feasibility study led to the creation of a Game Design Document (GDD) including all the elements required to develop the videogame. Then,

the development of the game was entrusted to a specialized company (Grifo Multimedia S.r.l). The illustrator and screenwriter collaborated with the external company to ensure the final product matched with the original project, and to guarantee good usability, excellent and faster-paced gameplay (see Fig. 1 and Fig. 2). The implementation of the video game was carried out in different stages. First mini-games were created, to test their performance, then, the Internetopolis scenario was designed. This was followed by the addition of the scenes in which dialogues and actions take place and the creation of the dialogues themselves; the scenes also include a written text designed to assist deaf people and help users retain fundamental concepts - in line with the educational nature of the video game. The dialogue creation provided for a chance to revise their content and make it suitable for the fast-paced rhythm of a video game.

Both the implementation and the design stage involved the skills of several professionals: communication and educational aspects were supervised by Ludoteca educators, scientific validation of the contents was provided for by CNR-IIT researchers, Giovanni Eccher (scriptwriter) worked on dialogues and storyboard, game design experts took care of the Game Design Document (GDD), Gabriele Peddes (cartoonist) worked on illustrations, and game developers allowed the creation of the final product.

The choice to develop "Nabbovaldo and blackmail from cyberspace", entirely dedicated to cybersecurity, represents a push towards the adoption of innovative teaching methods. In fact, "learning by playing" is becoming an increasingly widespread method also in the school environment, useful to make learning more engaging together with promoting the development of transversal skills such as collaboration, problem-solving and critical thinking. "Nabbovaldo and blackmail from cyberspace" is a serious single-player game, conceived as an adventure divided into chapters. The protagonist is Nabbovaldo, a young inhabitant of Internetopolis, passionate about the online world but naive and not really aware of the possible risks. The character's name comes from the italian-slang word "Nabbo", which refers to a person who can't do something well online, and from “Marcovaldo”, the protagonist of a novel written by Italo Calvino [21] (see Fig. 3). The game provides a hybrid structure between the "fixed path" and "open world": the player can move freely within the Map, talk to the characters and solve the Mini-games in the order they prefer. Alongside this structure, the plot of the game develops in four main chapters, plus an epilogue. The player moves within five main sections: 1) Settings: external and internal scenarios of the Internet city; 2) Map: the set of various environments on which Nabbovaldo can be geolocated; 3) Mini-games: arcade and game of intuition on cybersecurity issues; 4) Nabbopedia: a small dictionary in which the definitions of technical terms are collected. In addition, he can converse with other characters (Linda, Ada, Dr. Kappersky, etc.), in linear or multiple choice mode.

Fig. 1. The Registro.it in the videogame

Fig. 2. A dialogue scene in the videogame

Fig. 3. The protagonist of videogame: Nabbovaldo

2 Methodology

The aim of this work is twofold: first of all, to evaluate the video game in terms of satisfaction and usability by the students of middle schools, and secondly to understand to what extent the video game is effective in improving cyber security knowledge of students.

2.1 Procedure

Participants were students of four middle schools from Tuscany, coming from Livorno, Pisa and Lucca. The schools were contacted through a presentation letter for the project, which explained both the temporal organization of the meetings and the contents and training objectives. The schools have voluntarily chosen to participate.

In January, the teachers of the involved classes attended video game training held by the Staff of the Ludoteca. Subsequently, the classes involved took part in a workshop, conducted by the Staff, where they were explained how the video game works and cybersecurity key concepts were provided. Subsequently, the teachers were able to organize training meetings with their classes, where they could delve into the previously introduced cybersecurity issues. The Staff of the Ludoteca has always remained available for remote support. To assess the impact and effectiveness of the video game, a self-report questionnaire was administered to the students before the first meeting with the Staff and after the conclusion of the project. The survey was anonymous and data were analyzed in an aggregate way. The questionnaire, lasting 30 minutes, was completed via Google Forms. Since the students were under years 14 of age, the parents filled out an informed consent form to authorize the compilation. This project received the approval of the Ethics Commission of the University of Florence.

2.2 Self-report Questionnaire

The questionnaire inquired socio-demographic aspects (age, gender, nationality, etc.), the use of Social Network and videogames [22] by the students (both in terms of frequency and type), knowledge relating to IT security aspects (both general, cybersecurity specific, and technical-practical), and surfing habits on the Net. In addition, liking-related questions on the video game were included. Questionnaires were created ad hoc. About the cybersecurity knowledge, nineteen items were created, divided into the knowledge of general aspects (eg "I know what online privacy is") and the knowledge of more specific aspects of cybersecurity (eg "I know what a VPN is", "I know what a denial of service attack is"). The scale showed a good reliability index ($\omega = .91$) [23].

2.3 Sample

270 students (mean age = 12.66, SD = .70) of four schools in Tuscany participated in the project. 38% of the sample is female, while 3% prefer not to specify it. The sample is well balanced, with 53% of participants attending the third year of lower secondary school and 47% attending the second. 96% of the respondents are of Italian nationality.

2.4 Data Analysis

Descriptive analyses were carried out using the SPSS software [24]. The results were analyzed by comparing the level of incoming knowledge (ex-ante) with that of outgoing knowledge (ex-post), using ANOVA. Any differences related to gender, age, and effective use of videogame were checked.

3 Results

3.1 Descriptive

Most students spend more than an hour online a day. Excluding online lessons, 43% of participants spend at least 3-4 hours a day online, 20% say they spend at least 5-10 hours online and 7% are always connected. The Internet is mainly used for chatting with friends, listening to music and/or watching online videos, and looking for news or information. Less often, however, Internet's usage involves activities such as installing a program or using a social network to make new friends. Almost all the students (98.5%) have a smartphone, and the most used messaging service is WhatsApp. Most of them (79%) have a profile on at least one Social Network, and 20% have a public profile. The most used Social Networks are YouTube, Tik-Tok, Instagram and Twitch (a live streaming platform that allows real-time sharing of gaming sessions for the most popular video games).

The students were asked if they had ever had any problems surfing the Net: 9% of them told us that their device was infected with a virus (malware, ransomware, etc.) and 15% were victims of an online scam. Some students (29%) reported some Internet problem but not specify the typology.

3.2 Video Games

As for the use of videogames, 45% of students play videogames more than 1 hour for a day, and boys are more likely to play videogames than girls are ($F_{(1, 174)} = 21{,}210$; $p = <.001$; $\eta p^2 = .11$). The preferred types of videogames are Shooter, Sport, Strategy and Sandbox (a video game where the player has a large degree of freedom to explore, interact with, or modify the game environment) or Action - Adventure; and most of students use preferably PS4 or PS5, Xbox or others consoles and smartphones to play.

3.3 “Nabbovaldo and blackmail from space”: satisfaction and usability

Most of the students who participated in the project played the video game (60%). Some students report to have never played: they may have been absent during the workshop meeting with the Staff of the Ludoteca, or they may simply have decided not to play the videogame if the teacher gave it as homework. Anyway, the player group uses the videogame a couple of times a month, only managing to complete the first chapter.

Also, the boys mostly played home alone. In general, the video game was rated by the children as useful, with easy-to-understand game mechanics and operation, and original graphics. The video game was interesting, as well as the issues addressed, and with an engaging story. Through play, students were able to learn new things, including cybersecurity practices and terms they did not know before. In any case, all the students participated in the in-depth meetings conducted in class by the teacher.

3.4 Ex-Ante Results

Regarding the knowledge of cybersecurity, the level of general knowledge is just above sufficient (*M = 6.52; SD = 1.63)*, while the more specific knowledge is an insufficient level (*M = 4.90; SD = 1.96*). The most well-known topics are in fact: "I know what a fake profile is", "I know what online privacy is", while the lesser-known ones are: "I know what hate speech is", "I know what is the IP address” (see Fig. 4, 5). The average level of knowledge differs between males and females only as regards the more specific knowledge: although males also have an insufficient average score (*M = 5.08; SD = 2.13*), females seem to know even less (*M = 4.56; SD=1.63*). Furthermore, these levels of knowledge have a very high variability: some students seem to be very prepared, while others seem to know almost nothing. In this phase, there are no differences between the player group and students who have not played the videogame, both for *general knowledge* ($F_{(1, 212)} = 1.257; p = .263$) and for *specific knowledge* ($F_{(1, 212)} = 1.715; p = .192$).

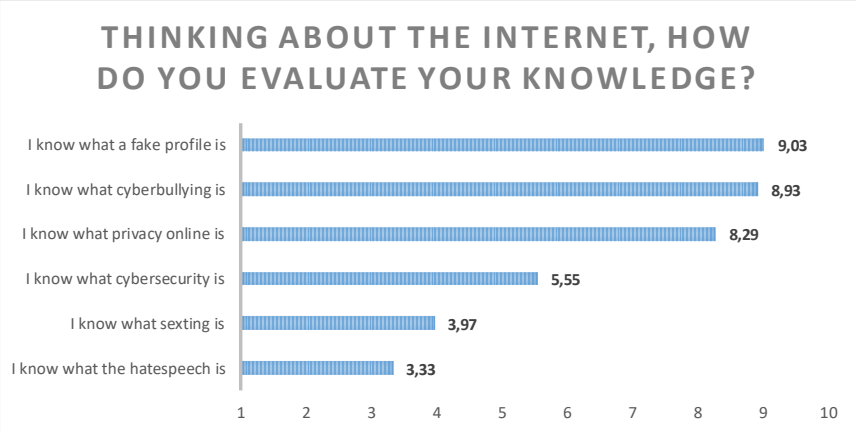


Fig. 4. Ex-Ante Level of General Knowledge

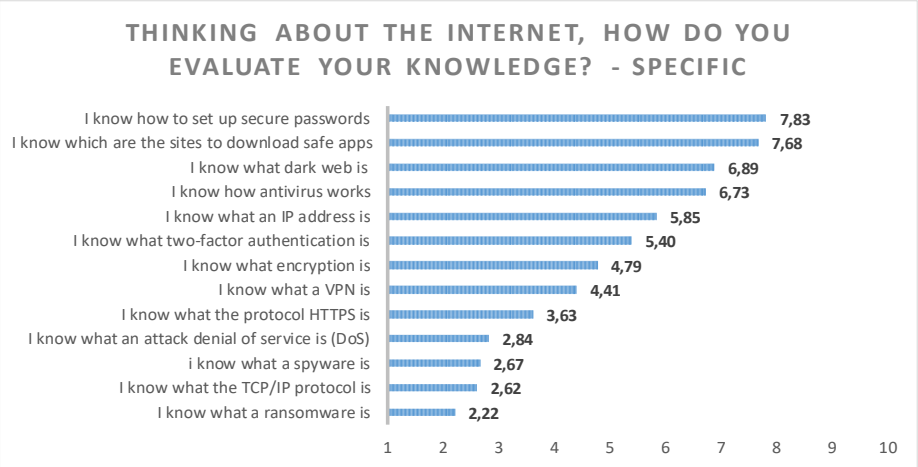


Fig. 5. Ex-Ante Level of Specific Knowledge

3.5 Ex-Post Results

At the end of the project the average level both in terms of general knowledge and specific cybersecurity knowledge increase (Figure 6, 7 - $F_{(1, 204)} = 109.327$; $p=<.001$; $\eta p^2=.35$; $F_{(1, 204)} = 112.625$; $p=<.001$; $\eta p^2=.35$). Moreover, the improvement is greater in player group. Students who have not played the video game improve their cybersecurity knowledge, but less strongly than students who have played (Figure 8 – *General Knowledge:* $F_{(1, 210)} = 97.334$; $p=<.001$; $\eta p^2=.32$, $F_{(1, 210)} = 5.431$; $p=<.05$; $\eta p^2=.02$; *Specific knowledge:* $F_{(1, 210)} = 103.571$; $p=<.001$; $\eta p^2=.33$, $F_{(1, 210)} =5.542$; $p=<.05$; $\eta p^2=.03$). The knowledge that improves the most concerns many technical aspects of the Net, i.e.: "I know what spyware is", "I know what ransomware is", "I know what a denial of service attack is". Furthermore, the difference between the two groups at the end of the project is statistically significant (*General Knowledge:* $F_{(1, 261)} = 11.984$; $p=<.001$; $\eta p^2=.04$; *Specific knowledge:* $F_{(1, 261)} = 15.847$; $p=<.001$; $\eta p^2=.06$).

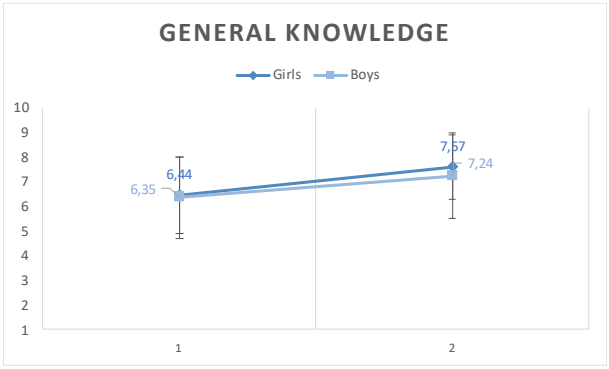


Fig. 6. Pre-post level of specific cybersecurity knowledge – Boys and Girls

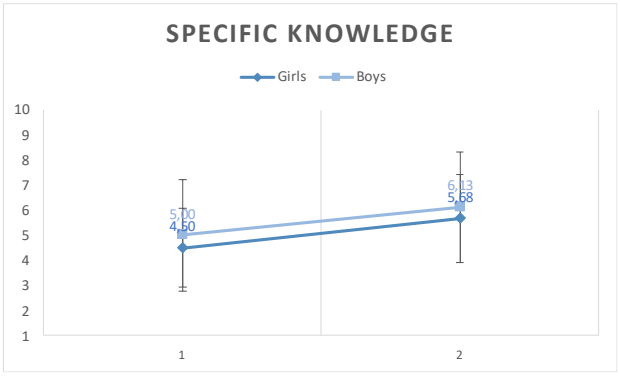
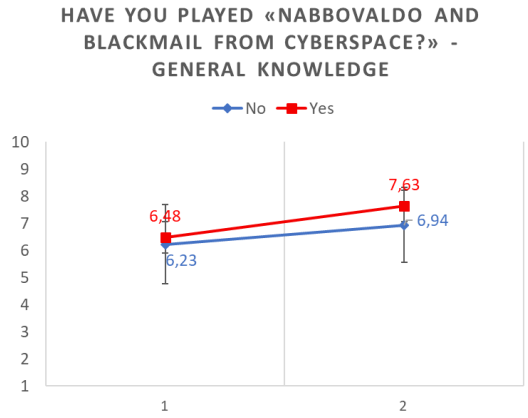


Fig. 7. Pre-post level of specific cybersecurity knowledge – Boys and Girls



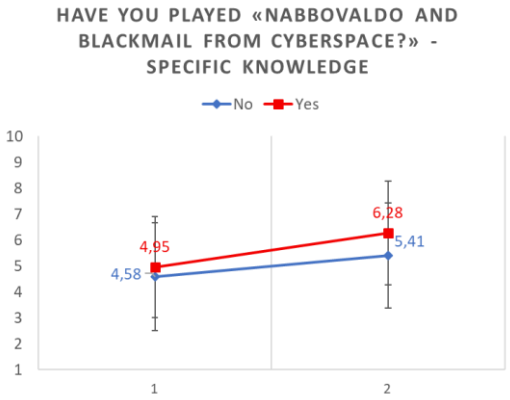


Fig. 8. Pre-post level of general knowledge and specific cybersecurity knowledge – Students who played and Students who not

4 Conclusion

The aim of this study was to evaluate the video game "Nabbovaldo and blackmail from cyberspace", one of the first video games entirely dedicated to cybersecurity to enter Italian schools. Together with the evaluation of the video game, it was possible to collect some data on student's Internet usage and new technologies. A good part of the students stays online at least 3-4 hours for a day, almost all of them have a smartphone and therefore have the ability to connect to the Internet wherever and however they want. Young people's perception is being active online 3-4 hours a day, but if we think about it, the simple fact of owning a smartphone (which is usually carried around with us) means that we are actually constantly connected.

Indeed, it's not uncommon to run into various kind of problems, such as viruses and cyber-type threats, and students don't always know how to solve the problem. Often, students ask for help from their parents or friends (sometimes even teachers), or simply "shut everything down". This shows that, despite surfing daily, in many cases they have a limited and superficial knowledge of how the web works.

For this, knowledge and awareness of cyber hygiene practices should be one of the main objectives of any online risk prevention program.

As shown in the results of this study, video games represent an extremely important educational tool, to be exploited and further integrated within our schools. Through playing the students could explore cybersecurity situations and scenarios, test their knowledge, and learn new terms while having fun. The possibility to download the game on your mobile device or use the web app version also allows teachers to use it in the classroom and favors group work.

Playing the video game, students show a major improvement in cybersecurity knowledge. Furthermore, those who actually played improved more than those who did not play. This comparison was possible because a question was added into the self-report questionnaire asking the students if they actually played the video game.

4.1 Theoretical and practical implications

The results of this study help to popularize gaming as an education and learning tool. The possibility of exploring and learning about situations of potential IT security risk allows you to get to know more deeply concepts and situations that are now part of the daily life of children. Furthermore, even just the theoretical study of certain terminologies allows you to be more prepared in "real" life. It is therefore important to continue working and investing in serious games, to spread this learning method within schools and to train teachers more about the use of these tools.

4.2 Limits and future directions

Lastly, this study has limitations: the project was carried out in a very short time frame, and the teachers had a lot of freedom in organizing lessons and classroom activities: which may have affected the results. In addition, some students have told us that

video games, while very interesting, may be more suitable for younger children in primary schools. Future studies should therefore bring video games into primary schools, creating more detailed and structured material for teachers and adding a control group to more rigorously test the effectiveness of the video game.

References

1. Smith, P. K., & Steffgen, G. (Eds.): Cyberbullying through the new media: Findings from an international network. Psychology Press (2013).
2. Stein, C. H., Osborn, L. A., & Greenberg, S. C.: Understanding young adults' reports of contact with their parents in a digital world: Psychological and familial relationship factors. Journal of Child and Family Studies, 25(6), 1802–1814 (2016).
3. Tokunaga, R. S. Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior, 26(3), 277–287 (2010).
4. Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U.: EU Kids Online 2020: Survey results from 19 countries. EU Kids Online (2020).
5. Mascheroni G. & Cino D.: Risultati della prima somministrazione della survey ySKILLS Italia (2021). KU Leuven, Leuven: ySKILLS, https://zenodo.org/record/6376258#.YnvBBhBxPY, last accessed 2022/10/12.
6. Obar, J. A.& Oeldorf-Hirsch, A. The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. Inf Commun Soc, 23(1), 128–147 (2020).
7. Guarino, A., Lettieri, N., Malandrino, D. et al. A machine learning-based approach to identify unlawful practices in online terms of service: analysis, implementation and evaluation. Neural Comput & Applic 33, 17569–17587 (2021).
8. Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J. & Weintrop, D.: Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. Simulation & Gaming, 51(5), 586–611 (2020).
9. Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A.: Youth Internet Safety Education: Aligning Programs with the Evidence Base. Trauma, Violence, & Abuse, 22(5), 1233–1247 (2021).
10. Zaccagnino, R., Capo, C., Guarino, A. et al. Techno-regulation and intelligent safeguards. Multimed Tools Appl 80, 15803–15824 (2021).
11. Guarino, A., Malandrino, D. & Zaccagnino, R. An automatic mechanism to provide privacy awareness and control over unwittingly dissemination of online private information, Computer Networks, 202, ISSN 1389-1286 (2022).
12. Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T. & Boyle, J. M.: A systematic literature review of empirical evidence on computer games and serious games. Computers & Education, 59(2), 661–686 (2012).
13. Clark, D., Tanner-Smith, E. & Killingsworth, S. Digital Games, design, and learning: A systematic review and meta-analysis. Review of Educational Research, 86(1), 79–122. (2016).
14. Arnab, S. et al., Framing the Adoption of Serious Games in Formal Education, in Electronic Journal of e-Learning, 10 (2), 159-171 (2012).
15. Serious Games, University Press of America (1987), ISBN 978-0819161482.
16. CyberCIEGE: https://nps.edu/web/c3o/cyberciege

17. BigBro, https://bitbucket.org/BlackDavid/securityseriousgame/src/master/gaetano/BigBro/
18. CyberCraft, https://github.com/luyangshang/CyberCraft
19. https://www.sicurezzanazionale.gov.it/sisr.nsf/cybercity-chronicles.html
20. Safer Internet Center Italia: https://www.generazioniconnesse.it/site/it/safer-Internet-centre/, last accessed 2022/10/12.
21. Calvino, I. Marcovaldo ovvero Le stagioni in città. Einaudi, Italia (1963).
22. Donati, M., Sanson, F., Mazzarese, M. & Primi, C. Assessing Video Game Habits and Pathological Behaviour in Children through a New Scale: Psychometric Properties of the Video-Gaming Scale—For Children (VGS-C). Psychology, 10, 2190-2208 (2019).
23. McDonald, R. P. Test theory: A unified treatment. Mahwah, NJ: Laurence Erlbaum Associates (1999).
24. IBM Corp. IBM SPSS Statistics for Windows, Version 27.0. Armonk, NY: IBM Corp. https://hadoop.apache.org, last accessed 2022/10/12.