Papers need to be written in English, the length of the paper should not exceed 5 pages AND 2000 words (abstract and references included). The length of the abstract should not exceed 350 words.

Cybersecurity education: a gamification approach

Giorgia Bassi*, Stefania Fabbri*, Anna Vaccarelli*

*Institute of Informatics and Telematics of CNR, Italy

Abstract

This paper deals with Ludoteca del Registro .it, a digital education project by Registro .it, the registry of Italian domain names, aimed at schools and focused on cybersecurity. In particular, two Ludoteca edutainment tools on cybersecurity will be presented: a videogame, called "Nabbovaldo and the cyber blackmail", aimed at children aged 11 to 14 in order to encourage the adoption of preventing behaviors and the event "Cyber Park", held during the last edition of Internet Festival (Pisa, October 6-9, 2022).

Keywords: *gamification, game based learning, videogame, serious game, applied game, cybersecurity education*

1. Introduction: children, internet and cybersecurity

The new information and communication technologies have now become a part of adult life, in work and personal contexts, but also of children's lives. Children and adolescents spend a lot of time on the Internet, a medium used for many different activities: studying, watching movies and/or TV series, making new friends, staying in touch with others. According to the EU Skills Agenda For Sustainable Competitiveness, Social Fairness And Resilience (European Commission, 2020a), the pandemic has accelerated the digital transition, with online learning becoming a reality for millions of students in the EU. A recent EUKids online survey (Smahel et al, 2020) of 25101 children, aged 9-16 from 19 European countries, reveals that 11% of respondents reported data abuse. Although there are differences in relation to the reference country, these data tell us that most children are often unaware of online risks. In Italy, young people access the Internet mainly through smartphones: 84% of children aged between 9 and 17 (ranging from 51% of children aged 9 to 10 to 97% of adolescents aged 15 to 17) use their smartphone at least once a day to go online (Mascheroni & Ólafsson, 2018). As a result, the place and context in which the Internet is used is becoming more and more embedded in daily life: while the home is still the most common place for Internet use (88% of children go online every day at home), 44% use the Internet every day on the go (increase to 74% in the 15-17 age group). For all these reasons, cybersecurity has become a major concern for our societies at large, including children. In fact, despite the usage limits by age activated by many online platforms, children increasingly start to be active online from the age of 8 (EIT Digital Academy, 2020), and this exposes them to different types of online threats, especially related to privacy (i.e unauthorized use of webcam or social media accounts, phishing) or malware.

1.2 Ludoteca del Registro .it: cybersecurity education

Ludoteca del Registro .it is an educational section of Registro .it, the registry of Italian domains, that works within the Institute for Informatics and Telematics of Italian National Research Council (CNR-IIT). This project (freely offered to the schools involved and supported by the Italian Authority for Children and Adolescents) promotes the internet culture across educational establishments of all types and at all levels aiming to encourage a more aware and safer use of the Internet among young people. Since 2011, the staff of Ludoteca has met more than 16,000 students, all over Italy and beyond. All the educational activities of the project combine play with learning and all contents provided are certified and assessed by CNR-IIT researchers.

The Cybersecurity labs were launched in 2018 in order to spread a safer use of the Internet and a knowledge of the main cyber threats, technical countermeasures and best practices. This educational mission was carried out through edutainment tools such as comics, quizzes, puzzles, group games. Even the field of cybersecurity education can therefore benefit from the use of techniques and resources based on edutainment, declined in various forms depending on the category of the learner.

Moreover, games create an active learning opportunity that favors awareness processes, as opposed to more traditional passive learning techniques.

2. Nabbovaldo and blackmail from cyberspace

Games and videogames are engaging for children, teens, and adults as well and therefore, they are easily welcome as a learning tool in schools. Nowadays, edutainment mostly uses games promoting players' "problem solving" or "collaborative" skills to face the challenges posed by the game. The choice to develop a videogame entirely dedicated to cybersecurity, represents also an opportunity of adopting innovative teaching methods. In fact, "learning by playing" is becoming an increasingly widespread method in the school environment, useful to make learning more engaging and to promote 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 four chapters. The main character is Nabbovaldo, a young inhabitant of Internetopoli, the city of the Internet, passionate about the online world but naive and not aware of the possible risks. 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, however, develops in four main chapters, plus an epilogue. The player moves within five main sections: 1) Environments: external and internal scenarios of the Internet city; 2) Map: the set of various environments on which Nabbovaldo can be geolocated; 3) Mini-games: games of reflection and intuition on cybersecurity issues; 4) Nabbopedia: a small dictionary in which the definitions of technical terms are collected.

2.1 Nabbovaldo at school

The labs based on Nabbovaldo videogame took place in the 2021/22 and 2022/23 school years, involving 15 middle school classes for each year, for a total of 40 hours of activity. The training activity was designed by adopting educational models typical of the "flipped classroom", a method which aims to increase student engagement and learning by making them independently learn the educational contents at home and discussing topics later, during the hours of lessons.
In the case of the videogame, the students were able to play independently at home and then review and deepen cybersecurity topics in class, with the support of the teacher.
While this model is particularly suitable for young people, also considering their familiarity with videogames, it was necessary to plan training activities for teachers. For this purpose, the staff of the Ludoteca del Registro .it supported the teachers for the entire duration of the project, with the aim of passing on all the knowledge relating to the game and its contents, but above all the teaching methods for proposing and sharing it in the classroom.
Furthermore, the classroom activity was facilitated by means of two Guides offered by the Ludoteca, one for students, another for teachers.

2.2 The evaluation

The project evaluation, in the sense of effectiveness in cognitive and educational objectives, was carried out thanks to the collaboration with the University of Florence (Department of Education, Languages, Interculture, Literature and Psychology). The evaluation, which took place through an ex-ante and ex-post questionnaire proposed to students, highlighted a general positive change in terms of knowledge related to IT security and a more aware attitude towards possible risks online. The knowledge that improves the most concerns technical aspects of the Net, such as: "I know what spyware is", "I know what ransomware is", "I know what a denial-of-service attack is". The video game was rated by the kids as user-friendly, with an easy-to-understand game mechanism and operation, and with original graphics. Playing was interesting, as well as delving into the themes presented in the game paths, and the mini-games were fun results.

3. Cyber Park

The last edition of the Internet Festival (October 6-9, 2022) was the occasion to launch the "Cyber Park" initiative, conceived as a playful and educational space in which to bring together all the resources and pre-arranged contents used during Ludoteca labs to introduce children to good cybersecurity practices. The activities, carried out with the support of volunteer educators, previously trained by the staff of the Ludoteca, were designed with the aim of stimulating children's awareness on the main online threats and protection measures, especially in terms of good practices.
Both primary and middle school classes took part in the initiative, for a total of 200 children.

This initiative required careful planning of the activities: each class was divided into smaller groups and each group, entrusted to an educator, did the various activities in rotation. In this way it was easier monitor the participation of students, encouraging interaction and debate. Below is the description of the proposed activities:
Caesar cipher: inspired by the cipher method used by the famous Roman leader to send secret messages. The game involves the use of an artifact built as a double wheel on which the alphabet is shown and on which it is possible to implement the monoalphabetic substitution mechanism. Each class was divided into groups of 5 and each group was given a cipher and a phrase to decipher. The game represents a valid tool for introducing the concept of data "confidentiality" and for explaining encryption techniques;
Memory: online game in which participants have to memorize passwords by trying to match identical cards. The game, followed by the classes via a touch monitor, stimulates reflection on the importance of managing passwords carefully;
Crossword puzzle: the classic crossword puzzle in an online version and via a touch monitor, based on definitions of some basic cybersecurity and IT notions;
Cyber Quiz: group game based on comic strips in which an online risk situation and three possible endings are presented but only one of these represents the correct behavior from a cybersecurity perspective;
Think first, then share: a game based on the use of cards that bear various types of personal information on one side (for example: home address, credit card number, favorite band, favorite color) and, on the other, the arguments for which whether or not it is appropriate to share them online.
Cybersecurity poster: an online handbook on cybersecurity with recommendations to prevent and counter the main cyber threats.

4. Future Developments

In the 2023-2024 school year the activities of Ludoteca will still be focused on cybersecurity education. The video game will also be at the center of the “Super Cyber Kids”, an Erasmus+ programme project in which the IIT-CNR participates. The aim of the project is to create teaching tools and methodologies for cybersecurity education at schools designing and implementing an educational ecosystem on cybersecurity-related skills. This ecosystem will include a wide range of materials in various digital format to anchor the topic of cybersecurity in the classroom, and will be addressed both to the kids in the age bracket 10 to 13 and to their teachers.

References

[1] Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online, doi: 10.21953/lse.47fdeqj01ofo, 2020
[2] 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, doi: 10.1177/1046878120933312, 2020, 51(5), 586–611.
[3] 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, doi: 10.1016/j.compedu.2012.03.004, 2012, 59(2), 661–686
[4] Ranieri, M. Linee di ricerca emergenti nell’educational technology. Form@ re-Open Journal per la formazione in rete, 2015, 15(3), 67-83.
[5] Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. Youth Internet Safety Education: Aligning Programs with the Evidence Base. Trauma, Violence, & Abuse, doi: https://doi.org/10.1177/1524838020916257, 2012, 22(5), 1233–1247.