Game Based Learning for Cybersecurity Education

Giorgia Bassi[1], Ilaria Matteucci[2]

Institute of Informatics and Telematics of CNR, Italy[1, 2]

Abstract

This paper presents the videogame "Nabbovaldo and the Cyber Blackmail" (hereafter referred as Nabbovaldo), which was designed, developed and promoted by the Ludoteca del Registro it, the educational branch of Registro.it.
Nabbovaldo is a serious game created for children aged 11–13 with the aim of enhancing their understanding of responsible and informed use of digital resources and tools, while promoting the adoption of good cybersecurity practices. In this paper, not only describe the videogames objectives and content, but also outline methods and strategies for using it effectively in a educational settings. We show how "Nabbovaldo" has been successfully integrated into the Erasmus+ project "SuperCyberKids", which aims to develop a game-based ecosystem to support teachers in delivering cybersecurity education.

Keywords: *cybersecurity, cybersecurity education, game-based learning, digital education,*

1. The Importance of Cybersecurity Education (CE)

Cybersecurity for children is an increasingly important and fast-growing area of concern, driven by the widespread availability of the Internet and the growing presence of children in digital spaces. As young users spend more time online to do several activities, including learning, gaming, and social interaction, they become more exposed to a wide range of risks, including cyberbullying, identity theft, privacy violations, and exposure to inappropriate content.
This highlights the urgent need for tailored educational initiatives, tools, and strategies that empower children to navigate the online world safely and responsibly being aware of all possible risks.
To support this perspective, we present key statistical data from the global context that highlights the growing prevalence of Internet use among children and teenagers, emphasizing the urgency of addressing cybersecurity at an educational level. In 2023 in the EU, 97% of young people used the internet daily, compared with 86% of all individuals (EUROSTAT). In addition, according to a report of the Global Cybersecurity Forum, 72% of children globally have experienced at least one type of cyber threat online (EUROSTAT). Moreover, between 2021 and 2022, 73% of minors aged 6 to 17 reported going online daily, and 65.9% said they used a mobile phone every day. Nearly 60% of children between 11 and 15 months old spend time in front of a screen (television, computer, tablet, or mobile phone). These findings come from the 14th Atlas of Childhood (at Risk) – Digital Times (2023), produced by Save the Children and focused on analysing the impact of technological and digital changes on children and adolescents.
In this scenario, it becomes evident that cybersecurity can no longer be viewed solely as the responsibility of technical experts. Cybersecurity has become a shared responsibility across all levels of society. In particular, schools and educational systems play a crucial role in fostering digital awareness and safe online behavior among younger generations. Integrating cybersecurity education into school curricula is essential to equip children and adolescents with the knowledge and skills needed to protect themselves in an increasingly connected world.
Therefore, it is essential to inform and update new generations about the major threats posed by new technologies as well as about the appropriate individual and collective behaviour to take to reduce risks. The need to address the skills challenges linked to cybersecurity is also recognised in the recommendations that have led to the adoption of the EU Digital Education Action Plan 2021-2027 Furthermore, if, as underlined by the European Commission ,'there is a need to create a cybersecurity education program for primary and secondary schoolchildren' (EIT Digital Academy, 2020), then it becomes also fundamental to provide teachers with proper training in cybersecurity skills so that they can transfer them in the classroom.
To address this challenge, we introduce the video game *"Nabbovaldo and the Cyber Blackmail"*, a serious gamespecifically designed to raise cybersecurity awareness among children through a gamification-based learning approach. The game engages young learners aged 11–13 in interactive

storytelling and problem-solving scenarios that reflect real-world online threats, helping them build digital resilience in a fun and accessibile way. In addition, we detail how *Nabbovaldo* has been further developed and integrated within the Erasmus+ project “SuperCyberKids”. This initiative aims to embed cybersecurity education into formal school curricula by providing teachers with a dedicated platform and pedagogical tools. The enhanced version of the game serves as a core component of this educational framework, supporting instructors in effectively teaching digital safety and online ethics to students across Europe.

The rest of the paper is structured as follows: next section briefly present key notions about the game-based approach in eductaion. Section 3 presents the videogame *“Nabbovaldo and the Cyber Blackmail”* showing also the behind the scene of its development. Section 4 describes the Erasmus+ porject SuperCyberKids and the prohect platform into which Nabbovaldo has been integrated. Section 5 draws the conclusion of the paper.

2. Game Based Learning, Serious Games and CE

Game based learning is an educational approach that uses games or game like elements, such as points, levels, and interactive storytelling, to teach specific knowledge or skills . It involves the integration of educational content into a game format, where learners engage in gameplay with the goal of achieving learning outcomes. This method is useful to boost student engagement by enhancing participation, knowledge retention, and information absorption [1,2,3].
The concept of *serious games* is, on the other hand, more specific: these are games designed for a particular purpose other than entertainment. It can be used to train, inform, stimulate reasoning, or influence behaviour, often with the goal of enhancing learning. As a simulation, a serious game creates a virtual environment that closely replicates real-world scenarios. In the context of cybersecurity, it can immerse the user in situations involving cyber threats, requiring them to apply appropriate countermeasures and defence strategies through a problem-solving approach.
As examples, below are reported some of the most famous serious games developed in the field of cybersecurity: *Info Sentinel* and *Agent Surefire* by MAVI Interactive, aimed at raising cybersecurity awareness among the general public; *CyberCIEGE [4] developed by* The Naval Postgraduate School, which teaches students security-related knowledge including encryption, patching, access control, and more and finally *Cybercity Chronicles* commissioned by the Department of Security Intelligence.

Several works and research activities have demonstrated the effectiveness of the game-based learning methods. The main reasons why these methods work are the following:

- *Improved engagement and retention*: Gamified training enhances engagement by ~48–60% and can increase retention by up to 50–75%, surpassing traditional methods that see steep drop-offs over weeks
- *Immediate Feedback:* Real-time reactions to players’ choices help reinforce correct behaviors and correct misunderstandings quickly.
- *Immersive, Safe Simulations:* Learners can experiment with cyber-attack and defense scenarios without real-world consequences, fostering risk-free exploration and learning.
- *Soft Skill Development:* Multiplayer or collaborative game formats encourage communication, teamwork, and strategic thinking—skills valuable beyond technical cybersecurity roles

Certainly, less widespread are serious games about online safety aimed at children and teenagers and mainly they deal with social risks, including cyberbullying.
In general, therefore, game based learning and serious games represent new educational instruments that can enhance cybersecurity education by offering an engaging and enjoyable environment where players can learn and apply skills and concepts through gameplay.

3. “Nabbovaldo and the Cyber Blackmail” Videogame and Other Resources for CE

In 2021, the educational offer was strengthened with the release of the video game "*Nabbovaldo and the Cyber Blackmail*", designed for middle schools and certainly more effective in terms of engagement.

3.1. Ludoteca del Registro .it: Digital Education and Cybersecurity Labs

The project and its contents were edited by the Ludoteca staff, while the development was handled by an external agency experienced in gamification.
Ludoteca is the educational section of Registro .it, the registry of Italian domains, that works within the CNR Institute for Informatics and Telematics (CNR-IIT).
This project, with the patronage of the Italian Authority for Children and Adolescents, promotes the internet culture across schools and aims to encourage a more aware and safer use of the Internet among young people.
Starting from 2019 the Ludoteca launched the project of labs on cybersecueity and aimed at primary (last two years) and middle school classes, maintaining the educational playful approach already experimented for more general themes of knowledge and use of the Internet and digital technology. The variety of educational materials adopted (comics, crosswords, comic strips, playing cards) allowed to adapt the educational offer according to the school grade, managing to engage students through teaching methods based on games.
Specifically, the project aims to enhance knowledge, attitudes, and behaviours in the usage of the Internet and cybersecurity practices. The goal is for children and young people to acquire a vertical curriculum dedicated to cybersecurity, focusing on the following skills: protecting devices; safeguarding personal data and privacy; recognizing and combating the risks of the "cyberspace", such as being aware of the interaction of people, software, and services through technologies, devices, and networks connected to it. The specific educational topics are related to the definition of what cybersecurity is, confidentiality, integrity, and availability of data, malware and attacks, technical countermeasures and good cyber hygiene practices.
Over the years, the educational proposal on cybersecurity has been expanded in both content and tools (see website section: https://www.ludotecaregistro.it/per-le-scuole/cybersecurity/), focusing on the use of learning methods with a high level of engagement in the learner.
In addition to the Nabbovaldo videogame, described below, the Ludoteca project also offers the following game-based learning activities on cybersecurity:

- **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 before sharing**: 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, the name of my dog etc..) and, on the other, the arguments for which whether or not it is appropriate to share them online.

3.2. The Videogame "Nabbovaldo"

The videogame "Nabbovaldo and the Cyber Blackmail" (in Italian: "Nabbovaldo e il ricatto dal cyberspazio") is aimed at children aged 11-14 to improve their knowledge related to the use of digital resources and encourage the adoption of good practice. It is a single-player game that can be used both in the classroom, as reinforcement for the teacher's lectures, and by kids on their own as a self-consistent game.

Fig. 1. Nabbovaldo home page

The game has a hybrid structure: players can either follow a fixed path, or move freely along the map, talk to characters and play the mini-games in any order. The setting is Internetopoli, a city in which landscapes and characters feature the complexity of the Internet world.
The main character is Nabbovaldo, a young inhabitant of Internetopoli, the city of the Internet, passionate about the online world but naive (as the name “Nabbo” or “newbie” in English tells) and not very aware of the possible risks.
For what concerns cybersecurity contents, the main topics are *malware, phishing, online scams, types of hackers, cyberattacks, dark web, troll, fake news.*
The main character Nabbovaldo faces the IT threats of Internetopoli, the Internet city; in particular, as the title tells, the reference is to a specific cyber-attack, that is ransomware. To advance in this challenge and win the game, he will have to perform a series of actions and go through several minigames.

In agreement to the game based learning methodology, the videogame includes a scoring system based on the completion of quizzes, dialogues, and mini games, with the aim of maintaining the learner’s interest and engagement.

Fig. 2. Nabbovaldo Minigame

4. SuperCyberKids Project

SuperCyberKids is an Erasmus+ project aimed to provide children aged 8 to 13 and their teachers with an educational ecosystem providing learning content on cybersecurity, using a game-based approach to increase motivation and engagement. Eight partners from 5 countries are involved, including the umbrella organisations dealing at EU level with cybersecurity (ECSO), and school heads (ESHA), who collect through their membership actors from all Europe
The content will be delivered through a gamification platform, including educational resources and games on cybersecurity. The video game Nabbovaldo and other related resources have been included in this educational ecosystem
The overall project approach is based on the delivery of the two main project results, the educational web platform and the related guidelines for implementing it. Currently, the project is in the pilot phase in four different settings (Europe-wide in English, and in local languages in Italy, Estonia, Germany) to test the results. This will lead to develop a Handbook of good practices on cybersecurity education in schools for children aged 8-13, including recommendations for researchers, school heads and

teachers, parents, game and instructional designers, as well as Recommendations targeting relevant policy makers, regulatory bodies and institutions in cybersecurity education.

4.1. The SuperCyberKids Platform

One of the outcomes of the project is the SuperCyberKids Platform (Fig. 3) that has been designed and developed for teachers. The platform includes all games and materials produced into the project lifetime organized by contents categorized in three macro areas related to different acquired skills: 1) Integrated Skill (in orange), 2) Social Skills (in blue) and 3) Technical Skills (in green).
Each macro-area is divided in three layers, from base notions (in dark) to more advanced skill (in light color).

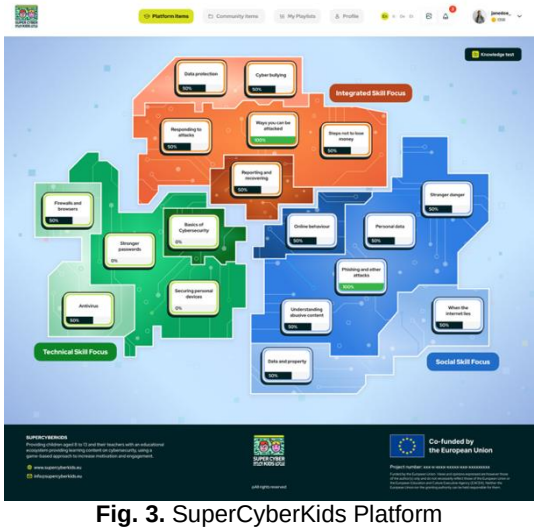

Fig. 3. SuperCyberKids Platform

4.2. Nabbovaldo in SuperCyberKids

As outlined in Section 3, the initial version of *Nabbovaldo* was developed in Italian, as it was originally conceived for use in cybersecurity education labs within Italian schools. As part of the SuperCyberKids project, the game has since undergone significant enhancements to support its integration into the curricula of schools across Europe.
To this end, *Nabbovaldo* has been fully translated into English and its structure has been redesigned to align with the pedagogical framework of the SuperCyberKids platform. In the current version, the game's content is organized by specific cybersecurity topics, allowing educators to select learning modules relevant to their lesson plans.
Moreover, a color-coded legend has been introduced to guide teachers through the game's content, ensuring alignment with the platform's recommended instructional scheme. This redesign offers greater flexibility and adaptability, enabling the game to be implemented in a variety of classroom settings, regardless of national curricula or teaching styles. As a result, *Nabbovaldo* serves not only as an engaging educational tool but also as a scalable resource for cybersecurity education across diverse European learning environments.

5. Conclusion

In this paper, we presented the serious game *Nabbovaldo and the Cyber Blackmail*, a videogame specifically developed for children aged 11 to 14 to raise awareness about the cybersecurity risks they may encounter while navigating the Internet. Through a gamified, narrative-driven experience, *Nabbovaldo* introduces key cybersecurity concepts in an accessible and engaging way, empowering young users to recognize threats and adopt safer online behaviors.

The game has been developed as part of the European Erasmus+ project "SuperCyberKids", which aims to foster a culture of cybersecurity education within European schools. *Nabbovaldo* serves as a concrete example of how serious games can be effectively integrated into classroom settings

to enhance student engagement, support teachers in delivering complex topics, and promote digital resilience from an early age.

By aligning its structure with educational frameworks and offering multilingual support, the game demonstrates the potential of serious games as flexible, scalable tools for enriching cybersecurity curricula across different cultural and national contexts.

REFERENCES

[1] Valdemar Švábenský, Jan Vykopal, Milan Cermak, and Martin Laštovička. 2018. Enhancing cybersecurity skills by creating serious games. In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018). Association for Computing Machinery, New York, NY, USA, 194–199. https://doi.org/10.1145/3197091.3197123
[2] Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T. & Boyle, J. M. (2012) A systematic literature review of empirical evidence on computer games and serious games. Computers & Education, 59(2), 661–686. doi: 10.1016/j.compedu.2012.03.004
[3] 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. Simul. Gaming. 51(5), 586–611 (2020). https://doi.org/10.1177/1046878120933312
[4] CyberCIEGE definition. https://en.wikipedia.org/wiki/CyberCIEGE?utm_source=chatgpt.com. Last access, 11 June 2025.
[5] Flavio Manganello, Peadar Callaghan, Giuseppe Città, Paola Denaro, Jeffrey Earp, Chiara Fante, Dirk Ifenthaler, Catlyn Kirna, Luca Janka Laszlo, Ilaria Matteucci, Salvatore Perna, Nicolai Plintz, Anna Vaccarelli, Manuel Gentile: SuperCyberKids: Enhancing Cybersecurity Education in K-12 Through Digital Game-Based Learning. HELMeTO2023: 323-334