



Deliverable D5.2
Enactment package for pilot use cases
SuperCyberKids
Call: ERASMUS-EDU-2022-PI-FORWARD
Type of Action: ERASMUS-LS
Project No. 101087250



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Project ref. number	101087250
Project title	SCK - SuperCyberKids
Document title	Realisation of the enactment toolkit for piloting use cases
Document Type	Internal Report /Deliverable /Other [accompanying document]
Document version	<v1, 30/10/2024>
Previous version(s)	
Planned date of delivery	31/10/2024
Language	English
Dissemination level	Public
Number of pages	87
Partner responsible	European Cyber Security Organisation (ECSO)
Author(s)	Arnaud de Vibraye (ECSO)
With contributions by:	Roberta Memeo (GRIFO)
Revised by:	Manuel Gentile, (CNR-ITD)
Abstract	The aim of this deliverable is to create clear guidelines to support the use of SuperCyberKids platform in schools during pilots to be conducted early 2025 in WP6. The document is divided into the three target audiences that will be involved in the implementation of pilots and in schools in general. The document gathers the elements for three enactment packages for these three audiences, to be used separately.
Keywords	Schoolheads, teachers, pupils, parents, enactment package, guidelines, education, classroom, implementation, piloting
DOI	https://doi.org/10.17471/54031
How to cite	de Vibraye, A. (2024). Enactment package for pilot uses cases. Deliverable 5.2 - SuperCyberKids project (ERASMUS-EDU-2022-PI-FORWARD - ERASMUS-LS - Project No. 101087250). DOI: https://doi.org/10.17471/54031

Internal project peer review process

Reviewed by	Role (Organisation)	Date
<i>Luca Laszlo</i>	Consultant (ESHA)	<20/09/24>
<i>Jeffrey Earp</i>	Research Assistant (CNR-ITD)	<28/10/24>
<i>Roberta Memeo</i>	Project Manager (Grifomultimedia)	<18/10/24>
<i>Erica Melloni</i>	Senior Advisor (Avanzi)	<30/09/24>

Approved by		
Manuel Gentile	Project Coordinator (CNR-ITD)	<31/10/24>
Flavio Manganello	Project Manager (CNR-ITD)	<31/10/24>

Table of contents

1	Setting the scene: cybersecurity for kids, why should we care?	6
1.1	The aim of Work Package (WP)	5.....6
2	Using the Guidelines in the education and training system	8
2.1	Who are these guidelines made for?8
3	Implementation package for school heads and task leaders	9
3.1	Introduction9
3.2	Understanding the SuperCyberKids platform9
3.2.1	What are the threats facing children?9
3.2.2	Your role as a school head or as a task leader10
3.3	Introducing SuperCyberKids to parents10
3.3.1	What is SuperCyberKids?10
3.3.2	Talking to parents: why is the SuperCyberKids platform also important for them?11
3.3.3	The Key Benefits of the SuperCyberKids platform:11
3.4	Introduce SuperCyberKids to the education staff at school11
3.4.1	Talking to the educational staff: why is this important for teachers and professional educators?11
3.5	General recommendations for school heads12
4	Implementation package for teachers and professional educators: train the trainer	14
4.1	Introduction14
4.2	Objectives14
4.2.1	The purposes of the platform14
4.2.2	Support the teaching of skills in cybersecurity in the classroom15
4.3	Everything you need to know before the activity in the classroom15
4.3.1	General recommendations for teachers15
4.3.2	The steps for a smooth integration of the SuperCyberKids Platform in the classroom17
4.4	Navigate in Super Cyber Kids ecosystem17
4.4.1	Homepage with map of the SCK modules17
4.4.2	Community Items18
4.4.3	Search function20
4.4.4	Launching a module21
4.4.5	Everything you need to know about the knowledge tests22
4.5	Select the right skills/modules24
4.6	The games included in the SuperCyberkids ecosystem25
4.6.1	Spoofy25
4.6.2	“Nabbovaldo and the Cyber Blackmail”26
4.7	Implementation steps: how to use SuperCyberKids in the classroom26
4.8	Monitoring and evaluation: sustainability and continuous improvement28
4.9	Recommendations for designing a lesson on Cybersecurity28
4.10	Assessment29
4.10.1	Assessment for students29
4.10.2	Assessment for teachers30

4.11	Conclusion	30
5	Implementation package for parents and students	31
5.1	Introduction	31
5.2	Objectives	31
5.3	General tips	32
5.4	Where to start: onboarding the SuperCyberKids platform	32
5.5	Navigate in Super Cyber Kids ecosystem.....	32
5.6	Stay up to date: SuperCyberKids online open-source repository for education.....	39
6	Appendix	40
6.1	Appendix 1: Feedback form.....	40
6.2	Appendix 2: Open-source repository of initiatives relevant for School leaders	42
6.3	Appendix 3: Spoofy lesson plans.....	60
	Online Behaviour	60
	Basic of Cyber Security	64
	Lesson plan:	64
6.4	Appendix 4: Spoofy instructions for educators.....	66
6.5	Appendix 5: How to use Nabbovaldo in class?	82
	Nabbovaldo lesson plans	83
6.6	Appendix 6: SuperCyberKids lesson plan template	86

1 Setting the scene: cybersecurity for kids, why should we care?

We live in a computer-centric world, even more so because during the COVID-19 lockdowns major aspects of life from work to socialization moved online. With younger and younger populations getting increasing access to technology and the Internet, there are also increasing concerns about the associated risks to the health and safety of children in Europe and globally. Cybersecurity is no longer the responsibility of a few technical individuals but the responsibility of society, with an important focus on school and educational systems. Cyberspace represents the greatest human shared common space ever, and it is the responsibility of educators, from teachers to parents, to help look after it.

The movement of so many aspects of human life online has led to the prevalence of cybercrime and cyber criminals. Estimates vary widely as to the cost of cybercrime, with one estimate placing the value of cybercrime as equivalent to the GDP of Spain. Cyber criminals have the potential to cause havoc with their attacks, affecting critical infrastructure like hospitals, power supply systems and banking. These high-profile attacks are not primarily aimed at children, but they will still suffer from the effects of them, nonetheless. Low-profile attacks aimed at children can have a life changing impact as well. Cyberbullying and cyber aggression have a great impact on the mental health of children, while parents and schools often don't have the tools to step in adequately.

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). Therefore, initiatives to raise awareness and increase the skills of kids in cybersecurity are crucial for their future as adults but also as citizens, adding another lifelong learning dimension to education. SuperCyberKids aims to fill the skills and awareness gap among kids aged from 8 to 13 years. To support the implementation of the platform and its responsiveness to teachers' pedagogical goals, the consortium of the SuperCyberKids project has developed an enactment package for school communities: school heads, teachers and parents.

1.1 The aim of Work Package (WP) 5

Within the Work package (WP) 5, the project aims to develop and adapt high-quality educational content for digital education in cybersecurity. The SuperCyberKids platform is aimed at children aged 8 to 13 years as final beneficiaries, but it is intended to be used in schools and at home under the guidance of teachers and parents, to find content and stand-alone educational games on cybersecurity. To ensure that the platform is accessible and user friendly to all members of the target group a package is needed to accompany a diversity of users.

Therefore, to support the implementation and facilitate the use of the SuperCyberKids ecosystem of educational resources, Task 5.3 includes the development of a design and enactment package for the three target audiences to promote optimal experience and use of the SuperCyberKids platform. Based on the previous work and materials developed in other WPs, including the work done in Task 3.2.1 “First version of the guidelines for the localization of the EU reference framework “ and the integration of the Skills framework presented in Deliverable 2.1 “SuperCyberKids Learning Framework” and the Deliverable 3.1, “Definition of the EU reference framework for the integration of the ecosystem into curriculum”, the guidelines provided in this document will support the integration of SuperCyberKids in the curriculum of schools, in the

pedagogical activities of teachers and as a source of information for parents to use the platform at home with young learners. Finally, the following guidelines are designed to support the best use of the platform and the games SPOOFY and NABBOVALDO in existing educational ecosystems.

To build up to the development of the enactment package, we first conducted a mapping of educational initiatives in cybersecurity across Europe. We used the mapping of initiative (see appendix) to provide SCK users with access to a community of educators and providers across Europe. We also identified the modules to provide teachers and educators with a comprehensible and clear tool to set their pedagogical objectives in the classroom based on crucial skills that students will develop during the learning activities. Subsequently, we defined a feedback form to create a review mechanism to ensure the relevance and usefulness of the platform, its evolution, based on the share of best practices, suggestions and feedback of professionals in education.

The enactment package that we are presenting in this document is a compendium and distillation of all the previous results described above. The goal is to provide a clear and comprehensive package containing tips, best practices adapted to a diversity of users and a ready-to-use platform to boost the education of kids in cybersecurity.

Disclaimer: *The document may sometimes include repetitions. This is done on purpose, as the content covers three different but complementary audiences. This allows the three toolkits and guidelines to be used separately.*

2 Using the Guidelines in the education and training system

2.1 Who are these guidelines made for?

The three target audiences of the guidelines are the three most important stakeholders of the education of young people between 8 and 13 years old. The targeted guidelines should clarify how to use the SuperCyberKids platform, but also how to explain its functionalities, its content and its purposes to audiences who are not professionals of cybersecurity, and eager to learn more about the platform and the challenges of cybersecurity education.

Therefore, the guidelines are divided into three audiences:

- AUDIENCE 1: School heads and task leaders¹
- AUDIENCE 2: Teachers and educators
- AUDIENCE 3: Parents and students²

These Guidelines offer concrete, hands-on guidance for the three target audiences, based on their different roles and expectations in the educational system or in the private sphere. They do not offer prescriptions or axioms, but rather aim to provide practical support for informing non-technical audiences, teaching in classrooms and in similar educational settings and for using the platform at home.

¹ By “Task Leader”, the consortium refers to all the professionals with the special role of supervising/leading the cybersecurity efforts of the school or the SCK project involvement of the school.

² In this case, “students” refers to children from 8 to 13, as indicated SCK technical specifications,.

3 Implementation package for school heads and task leaders

3.1 Introduction

Today, cybersecurity is a crucial topic for education of the population, especially the youngest, and a global healthcare matter in our societies. Therefore, school heads must play a central role to ensure that students, school staff and school infrastructure are well equipped to navigate online. The following set of guidelines is designed to assist task leaders and school heads in using a gamification platform in their schools to educate students about cyber risks through engaging games and educational resources. This document should serve as a working document to exchange with teachers, define educational objectives and bring a new dimension of studies and awareness in educational institutions. By integrating these tools into different school systems across Europe, school heads are the cornerstone of a new and needed response from schools to face the increasing exposure of kids to malicious activities. By mobilising their team, professional educators, such as teachers and pedagogical assistants and librarians, they can foster a proactive approach to cyber safety, empowering pupils to recognise and respond to online threats, protect their personal information, and develop responsible digital behaviours. A complete mobilisation of school staff is necessary to raise awareness on the threats online and complete the parental education on this topic. Moreover, these guidelines aim to provide school heads with the strategies and resources needed to foster a secure and informed digital learning environment, preparing students for the challenges of the digital age.

3.2 Understanding the SuperCyberKids platform

SuperCyberKids aims to respond to this need by providing children aged 8 to 13 and their teachers with an educational platform with learning content on cybersecurity, using a game-based approach. The approach aims at stimulating motivation and engagement of pupils, by using educational games to teach specific concepts related to cybersecurity and by linking the performance of activities to the acquisition of points or badges to move up in the rankings. The content is delivered through a gamification platform, including two games on cybersecurity developed by the SuperCyberKids partners, but potentially open to include other games, provided they respond to certain minimal requirements [see D5.1 “Gamification platform and back-end tools” for more information]. The main purpose of the implementation of the SuperCyberKids platform is to foster a common vision of high-quality, inclusive and accessible digital education in Europe, and aims to support the adaptation of schools to the increasing digitalisation of our society.

3.2.1 What are the threats facing children?

Children aged 8 to 13 face several cybersecurity threats. Here are some of the most common ones:

- **Privacy Issues:** This should be the first security issue for young people, but also people in general. Kids can share too much personal information online (home address, school name, or daily routines). This information is exploited by malicious actors.
- **Cyberbullying:** Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted. (UNICEF definition)

- **Online Predators:** Predators often use social media, chat rooms, and online games to target children. They manage to build trust and manipulate children into revealing personal information or arranging face-to-face meetings.
- **Inappropriate Content:** Children can accidentally or intentionally access content that is not suitable for their age. It can be violent or explicit online material.
- **Scams and Phishing:** Beyond online predators, scammers can try to trick children into giving away personal information or clicking on malicious links. This can lead to identity theft or malware infections.

In order to educate and sensitise children around these issues, it is important that school curricula include elements that inform about basic cyber hygiene, threats online, and the appropriate behaviour to adopt online. Schools and educators, whether they are professionals or parents should also have the means to mitigate the risks in a context where threats are increasing and are getting more sophisticated, targeting more the most vulnerable populations like children.

To help protect children from these threats, it is important to educate them about safe online behaviour, monitor their internet usage, mitigate the risks and use parental controls where necessary, but also discuss with them about their understanding of the context, the threat and grab a bit of the complexity of a fast pace changing world.

3.2.2 Your role as a school head or as a task leader

Education systems throughout Europe vary a lot, but the role of the school leadership team and task leader remains essential. The enthusiasm and commitment of the school head will motivate the teaching personnel and ensure the availability of the necessary infrastructure and time allocated for cybersecurity education. General awareness of the current level of threats and available resources, knowledge and policy environment are the responsibility of the leaders of the school. The SuperCyberKids project is aiming to support the school leadership team in this crucial role with evidence-based resources.

Therefore, in addition to understanding the issues involved in educating children aged 8 to 13, school heads should know the threats facing the young and vulnerable public, need to explain them to parents, their teaching staff and, where appropriate, at other meetings between schools, for example. In addition, school heads need to be able to explain the benefits of using this platform to their teachers and parents. Thanks to the action taken by school heads, this could lead to an awareness of the threats and the need to adapt the education of children to challenges of today, particularly by equipping them with tools such as those provided by SuperCyberKids.

3.3 Introducing SuperCyberKids to parents

3.3.1 What is SuperCyberKids?

SuperCyberKids is a free educational platform that merges gamification with cybersecurity education, developed by experts of education and cybersecurity in the scope of a European Union funded project. It features interactive games that teach children essential cybersecurity principles. The platform includes two main games: Nabbovaldo and Spoofy. These games are designed to enhance motivation and engagement, making learning about cybersecurity both enjoyable and effective. The platform is designed to include also other educational resources on cybersecurity developed and shared by teachers, including links to other educational games on cybersecurity.

3.3.2 Talking to parents: why is the SuperCyberKids platform also important for them?

With the increasing use of digital devices and of the internet, and the confrontation with online threats on a daily basis, it is crucial for children and for parents to be aware of the risks and know the best practices on how to protect themselves online. SuperCyberKids provides a safe and controlled environment where they can learn these important skills.

As a school head, you can encourage parents to discuss with their children about what they learn on the platform or play it together with them. For example, ask them about the games they play and the lessons they learn. Your involvement and constructive interaction to encourage them to reformulate will reinforce the importance of cybersecurity and help them apply these lessons in their daily online activities.

3.3.3 The Key Benefits of the SuperCyberKids platform:

Interactive Way of Learning: The platform uses game elements like missions, scores, levels, and badges to make learning about cybersecurity exciting and interactive.

Search function for clear and comprehensive content on cybersecurity for children aged 8 to 13, including games and guidance on how to use them.

Availability of Lesson Plans: the Lesson Plans are a key element to help teachers plan their activities in the classroom and use the SuperCyberKids ecosystem of content on cybersecurity in the best way, specifically tailored to their needs.

Age-Appropriate Content: The games are tailored to be suitable for children aged 8 to 13, ensuring that the content is catching their attention and provides an innovative way to learn, while promoting the "learning-by-doing approach", necessary in a constantly evolving domain such as cybersecurity.

Skills Development: Through these games and based with the SuperCyberKids Learning Framework and tailored modules, children will learn how to recognise and avoid online threats and develop safe online habits. Parents can rely on the content in the platform to support their children learn more about cybersecurity.

3.4 Introduce SuperCyberKids to the education staff at school

3.4.1 Talking to the educational staff: why is this important for teachers and professional educators?

With the increasing use of digital devices and the internet, it is crucial for students and teachers themselves to be aware of the potential risks and how to protect themselves online. SuperCyberKids provides a safe and controlled environment where they can learn these important skills and the following part aims at proving school heads and task leaders with indications and language elements to be able to talk about the key features of the SuperCyberKids platform to a public of professional educators.

- **The role of teachers.** Teachers have an important role to play as educators and caregivers to impart the needed knowledge and engage in thoughtful discussions with children about the potential dangers of the internet and how they should navigate the online world. School

heads can play their part by empowering teachers and equipping them with the necessary tools to be successful in that role.

- **Pedagogical support.** In order to protect children's privacy and avoid use and storage of any sensitive data related to them, the SCK platform is designed to be used by *adults*, i.e. School Heads, Teachers and Parents. Children aged from 8 to 13 are indeed the final target users of this ecosystem on cybersecurity, but their access to the platform must take place always under the supervision of the teacher in the classroom, or parents at home, and using the login details of a registered adult.
- **Gamification:** The program uses game-like elements such as missions, scores, and badges to make learning about cybersecurity more engaging for pupils.
- **Flexibility:** The resources provided can be adapted to meet the specific needs of the pupils. The holistic approach of the platform is central for the integration to educational systems, fostering complete autonomy of the educators and educational innovation. This document provides the educators with lessons plans where educators can take inspiration and information from.
- **Comprehensive tool and guidance:** Both teachers and students will benefit from this program, as it includes training materials, tests, lesson plans and guidelines to help us integrate cybersecurity education into the classroom.

How to support as a school head?

- **Integration into Curriculum:** We can integrate the platform into the existing curriculum, using it as a supplementary tool to reinforce cybersecurity lessons.
- **Classroom Activities:** Teachers can use the games as part of classroom activities, encouraging students to discuss what they learn and apply these lessons in their daily online activities.
- **Parental Involvement:** We can encourage parents to engage with their children about what they learn on the platform, reinforcing the importance of cybersecurity at home.

3.5 General recommendations for school heads

- **Integration with Existing Curriculum:** Ensure that the game-based learning modules align with the current cybersecurity curriculum, fulfilling the educational functions outlined in the framework.
- **Legal and Ethical Compliance:** Prioritize games that adhere to ethical norms and legal standards, particularly those related to the age group of 8–13 years.
- **Resource Allocation:** Allocate necessary technological resources and support. Ensure teachers are trained to facilitate game-based learning and can adapt to various interaction patterns.

- **Assessment Strategy:** Develop a comprehensive assessment strategy that includes both formative and summative assessments. Make sure the assessments are in line with the pedagogical objectives outlined in the SCK EU framework.
- **Monitoring and Feedback:** Implement mechanisms to track the effectiveness of the game-based approach in meeting the objectives of the SCK EU framework.

4 Implementation package for teachers and professional educators: train the trainer

4.1 Introduction

Children are more exposed to the online world than in the past, making them vulnerable to malicious activities. The generalisation of tools, and easy access to the Internet makes it essential for educators to equip their pupils with sufficient knowledge and skills to navigate cyberspace safely. Teachers play a central role in guiding students through the complexities of cyber risks and helping them develop responsible online behaviors. Gamification in education involves integrating game elements such as points, badges, and a set of educational objectives and sufficiently defined skills into the learning process to enhance pupils’ engagement and motivation. This package will guide teachers and professionals of education through the steps to implement the SuperCyberKids gamification platform in the classroom.

This set of guidelines is designed to assist professionals in utilising a dedicated platform to educate kids about cyber safety through engaging games, educational materials, and interactive resources. By integrating these tools into the classroom, teachers can create a dynamic and interactive learning environment that not only informs but also empowers your pupils to protect themselves online. The following enactment packages will provide education professionals with practical strategies and best practices to teach cyber safety, ensuring that your pupils are well-equipped to face the digital challenges of the modern world.

By following these guidelines, teachers can effectively integrate a gamification platform into the classroom.

4.2 Objectives

4.2.1 The purposes of the platform

The main objective of these guidelines is to empower teachers with the tools and strategies needed to effectively educate students about cyber risks. By leveraging a dedicated platform, teachers can create an engaging and interactive learning environment. The use of games, educational materials, and resources to teach students about online safety make more attractive the topic of cybersecurity that is sometimes too far away from the learning objectives in class, knowing the already large number of disciplines to teach and the limited time available. Therefore, these guidelines aim to help trainers and teachers, gain time in the implementation of SuperCyberKids and help students recognise and respond to cyber threats, understand the importance of protecting personal information, and develop responsible online behaviours. The objectives are the following:

1. Teachers will be able to use the SCK digital platform to easily decide which games they can use in the classroom as supporting tools for the curricula on cybersecurity. The SCK platform acts as a searchable commented database of games on cybersecurity.
2. Teachers will be able to upload their own resources on cybersecurity in addition to those already present in the SCK platform, that thus will act as a repository of learning and teaching resources on cybersecurity. The content available on the platform can be collected

by teachers in personalised lists (or playlists), or they can use off-the-shelf lists of content recommended by SCK.

3. Teachers will be able leave comments and recommendations on the games (rating system), thus enriching the database of resources on cybersecurity.
4. Among the teaching resources the platform will include also lesson plans, guidelines for formative assessment (discussion aids, protocols) and summative assessment (quizzes, tests, assignments). To see examples of lesson plan, see 4.7 “Implementation steps: how to use SuperCyberKids in the classroom”.

4.2.2 Support the teaching of skills in cybersecurity in the classroom

SuperCyberKids proposes teaching toolkits with tailored lesson plans to help teachers, particularly those who lack experience or are not experts of the topic, to make their pupils aware of the importance of being safe online. The toolkit also lets them assess the progression of their pupils with ready tests at the end of the sequence or period of learning. This package will help teachers to get some help with concrete and dynamic activities for their classes such as:

- **Interdisciplinary Learning:** SuperCyberKids promotes interdisciplinary learning by combining disciplines. This holistic approach can help students make connections between different subjects and understand the broader context of their learning³.
- **Prepare children for evolution in technology and the coming challenges from a technical point of view:** As technology continues to evolve, understanding cybersecurity is becoming increasingly important. By integrating cybersecurity education into math classes, teachers can help prepare students for future challenges and opportunities in the digital age⁴.

The toolkit should allow teachers to develop their lessons in a simple, easy and fast manner to teach their pupils in a didactic way. Nothing should be too complicated, and the activities must be highly recreational. The pupils should understand the platform easily and they should be encouraged to progress and be assessed always in a positive and reaffirming way.

The contents in the platform are linked to the skills in the SuperCyberKids EU reference framework identified in WP2⁵.

4.3 Everything you need to know before the activity in the classroom

Knowing where to start is not always easy at the beginning. A good starting point is to gain insight on the functionalities of the platform and understand the purposes in order to align it with your pedagogical objectives. You will see below the proposed steps in order to engage your class on SuperCyberKids.

4.3.1 General recommendations for teachers

Content Variables:

³ [Frontiers | Shaping the foundation of the SuperCyberKids Learning Framework: a comprehensive analysis of cybersecurity education initiatives \(frontiersin.org\)](https://www.frontiersin.org/articles/10.3389/fpsyg.2020.00000/full)

⁴ [SuperCyberKids - SCK - CNR-ITD](#)

⁵ cf Annex

- Consider the age group when selecting the depth and breadth of the content.
- Consider the classroom setting and available resources.
- Decide whether the game will be used for homework, in-class individual play, or group play.
- Be aware of pre-existing knowledge and skills among the students to avoid redundancy or excessive complexity.
- Opt for content that allows for multiple educational functions, like demonstration, training, and motivation, to be fulfilled.

Educational Objectives/Learning Outcomes:

- Clearly define what the students should know (knowledge), be able to do (skills), and understand (attitudes) after the lesson.
- Use the SCK EU framework as a guide to set these objectives, ensuring alignment with one or more modules, like Malicious Code & Cyber Attacks, Data Privacy & Privacy Awareness, Frauds, Preventing Technologies, Abusive Contents and Safety.

Safety Measures:

- Integrate the safety measures and preventive techniques from the SCK EU framework into the game-based learning environment.

Lesson Activities:

- Use interactive methods like game-based learning to enhance engagement.
- Ensure that the activities are designed to meet the educational objectives set out at the beginning.

Assimilation of Existing Content:

- If using existing content like the Spoofy game, make sure to thoroughly understand its educational objectives, capabilities, and limitations.
- Integrate such content smoothly into the lesson plan, ensuring it serves as a complementary tool rather than a disjointed add-on.

Student Engagement:

- Adapt the interaction pattern (Teacher Monitored Use, Group Play, etc.) to maximize student engagement and learning, ensuring alignment with the framework’s objectives.

Feedback and Adaptation:

- Continuously monitor student progress and adapt the teaching strategy as needed. This should include formative assessments and could be facilitated by in-game analytics.

Assessment and Metrics (Indicators):

- Formative Indicators: Classroom engagement, discussion participation, and on-the-spot feedback during activities like the Spoofy game. Summative Indicators: Scores on quizzes, quality of written assignments, and demonstrated ability to apply learned concepts in practical scenarios.

- Utilize in-game and out-of-game assessments to measure learning outcomes. Be aware of the limitations and benefits of each assessment type as discussed in the guidelines.

Review and Adaptation:

- Post-lesson, analyse the success of the lesson against the set objectives and indicators.
- Make necessary adjustments for future lessons based on this analysis and feedback from students.

4.3.2 The steps for a smooth integration of the SuperCyberKids Platform in the classroom

STEP 1: accessing the platform: Registration and Login

After filling in the Registration form, the system sends an automated email to the registered address with login details (Username and Password). Users can change their password upon first login.

STEP 2: pre-test to define learning needs of the class

Purpose: identifying the core competences to be addressed in (the design of) the learning path that students are to follow. For more information, please refer to the section 4.4.5: "Everything you need to know about the knowledge tests".

STEP 3: Search the database for resources by competencies and other criteria

For more information, please refer to the section 4.4.3: "Search function".

STEP 4: View «cards» containing resources (documents, links to games, video clips)

For more information, please refer to the section 4.4.2: "Community Items".

STEP 5: Create a «playlist» of resources

For more information, please refer to the section 4.4.2: "Community Items".

STEP 5: Classroom activities

For more information about the implementation of the platform in the classroom activities, please refer to part 4.7: "Implementation steps: how to use SuperCyberKids in the classroom".

4.4 Navigate in Super Cyber Kids ecosystem

4.4.1 Homepage with map of the SCK modules

The home page is viewed when the users enter the platform. It contains the **map of the 18 modules that have been prepared and approved by the SCK project**. They make up the SCK education eco-system on cybersecurity. Through a set of buttons and menus, this page gives also access to all the functionalities of the platform.

The map of the modules has been designed to look like a computer motherboard. It is divided into three areas, each of different colour:

- Technical Skill (green)

- Social Skills (blue)
- Integrated Skills (red).

The colour of the three areas grows lighter when nearing the outermost part of the circle; in the centre the colour is deeper, indicating that those modules are at the core of the SCK recommended curriculum.

Figure 1 - home page or map of SCK approved modules

The top menu contains the following buttons:

SCK items: access to this page, where users can select one of the 18 modules available. By clicking on this button on the top menu in other pages of the platform the users go back to this page.

Community items: access to resources suggested by users to be used by the SCK community at large (see section 4.4.2 below).

My Playlists: access to a selection of specific resources by the user currently logged in to the platform.

Profile: access to the Profile page with information about the user currently logged in.

Buttons provided in the top menu enable to change the language of the user interface (English, Italian and Estonian).

In the top right-hand corner there are two buttons:

- Search
- Knowledge test

That give access respectively to the Search function (see section 4.4.3) and to the Knowledge test for assessing initial or final knowledge (see section 4.4.5).

4.4.2 Community Items

This page can be accessed by clicking on the “Community items” button on the top of the navigation page. This area of the platform is a common repository of all resources suggested or uploaded by users (teachers). It contains all the items suggested, uploaded and catalogued by users and is visible to all users registered in the platform.

PLEASE NOTE: all items shown in this mock-up are fictitious, they DO NOT refer to real items and are shown only for demonstration purposes.

The items are shown as cards. Each card contains a short descriptive text, and the list of competencies associated to that item (viewed by clicking on the drop-down menu Competencies). At the bottom there is also the username of the

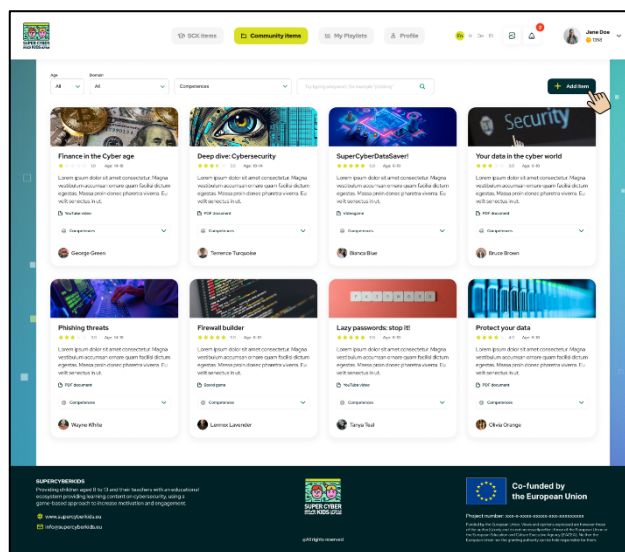


Figure 2 - Community items desktop

user who uploaded that learning resource. The cards for Community items also contain an indication of the type of resources (videogame, PDF document, YouTube video).

How to add an item to the Community items repository

To suggest or upload a new learning resource or item to the repository (“Community items”), user can click on the button ADD ITEM in the top right-hand corner (see figure 5 above). A window pops up with several fields where users can select all the appropriate metadata to associate to the item they are suggesting for inclusion in the SuperCyberKids Community items repository. The fields are the following:

Figure 3 - add an item to the common repository

- Title* (open field)
- Description (open field)
- Age*
- Language*
- Competency Domain and related competencies*
- Item type* (Game, Lesson plan, Video, Document)
- Lesson Style [game-based learning, traditional classroom, other]
- Intended Learning Outcomes (open field, only for lesson plans)
- Image associated to that item.

Fields and menus indicated with * are mandatory.

How to add an item to a personal playlist

After a user has uploaded an item with all the appropriate metadata, they can select that item (or others in the Community items area of the platform) to create their own playlist.

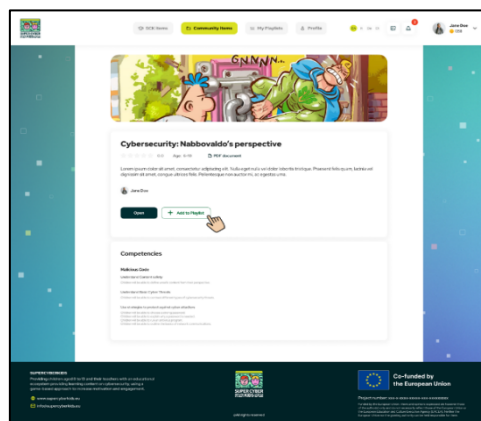


Figure 4 - add an item to the playlist

4.4.3 Search function

The Search function can be used to retrieve learning resources in both areas of the platform, the SCK approved modules and the Community items uploaded by users. After clicking on the button RESOURCE SEARCH in the home page (see figure 4), users can access the Search page (see figure 8), where they can type one or more keywords, and select options from three drop-down menus:

- Age
- Language
- Domain (referring to the six domains of cybersecurity identified in the project, Malicious Code, Frauds, Preventing Technologies, Abusive Content, Data Privacy & Data Awareness, and Safety)
- Competencies [please note that when a domain is selected, the drop-down menu Competencies shows only the competencies pertaining to that domain]
- Type of resource [possible options: lesson plan, game, document, video].

PLEASE NOTE: all items shown in this mock-up are fictitious, they DO NOT refer to real items and are shown only for demonstration purposes.

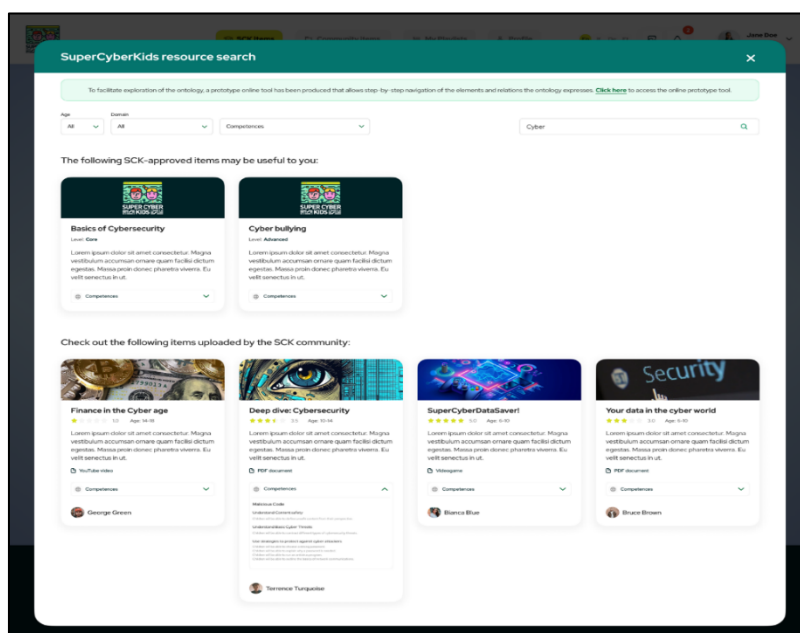


Figure 5 - Search page with results

The page that shows the results of the Search is divided into two areas:

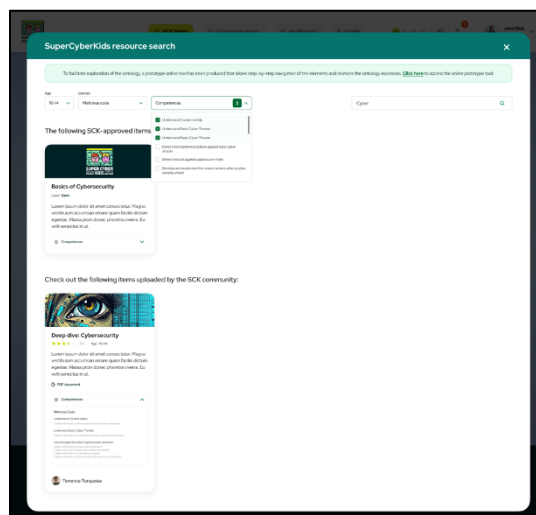


Figure 6 - search using specific competencies

the top area shows the items matching the search retrieved in the ***SCK approved items*** area of the platform, that contains the 18 modules set up by the SCK project;

the bottom area shows the items matching the search retrieved in the ***Community items*** area of the platform, a common repository of all resources suggested by users.

Results are shown in form of card. Each card refers to an item, and contains a short descriptive text, and the list of competencies associated to that item (see in the example above: item “Deep dive: Cybersecurity”). At the bottom of the card there is also the username of the user who uploaded that learning resource.

The cards for Community items also contain an indication of the type of resources (i.e., videogame, PDF document, YouTube video, lesson plan). The stars shown on the card are connected to the rating system: an average of the stars given by users to this resource is shown, 1 star being the lowest appreciation and 5 stars the highest.

By clicking on the card, users can launch the related item (open a lesson plan or a document, launch a video, play a game if embedded in the platform), or select it to be added to their personal playlist.

4.4.4 Launching a module

This figure shows what happens when a user clicks on one of the 18 modules in the navigation page (see section 4.4 above). All modules are open, i.e. there is no fixed sequence to follow. In the example shown, the user has selected the module “Firewalls and browsers”.

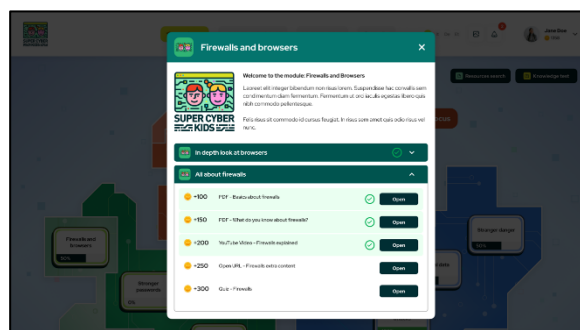


Figure 7 - Opening a module

The window contains a list of all the items that make up the module: they can be a lesson plan, a document to download, a quiz to test the knowledge, or ***a link to a game***. Opening each item the user gains points that make up the final score.

When all the items in the module have been opened, and, in case of a quiz, the quiz has been passed, the user is shown this window with the final score for that module.

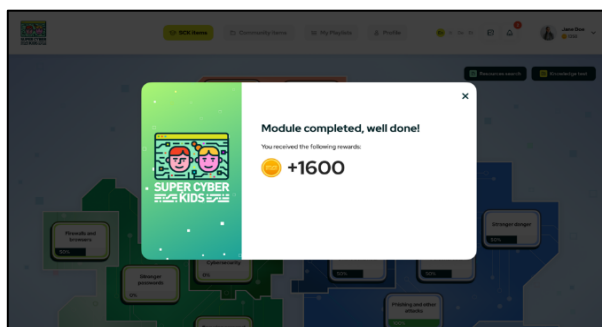


Figure 8 - module completed

4.4.5 Everything you need to know about the knowledge tests

The platform is intended to offer users the opportunity to take a knowledge test, whereby they initially select the language (German, Italian, English, Estonian) and the test type (pre-test or post-test). Regardless of the choice of test type, the same questions are asked, which are presented in a fixed order. For the post-test, the user receives immediate feedback after each question has been answered. This feedback indicates whether the answer was correct and, if not, what the correct answer would have been.

The Knowledge test can be accessed by the button in the top right-hand corner of the Home page. It contains the initial and final assessment divided into the six domains of cybersecurity: *Malicious Code, Frauds, Preventing Technologies, Abusive Content, Data Privacy & Data Awareness*, and *Safety*. Users can select the domain and start answering the test.

It is designed to be used by teachers in the classroom, asking questions to their pupils to test their knowledge of the topics in each domain.

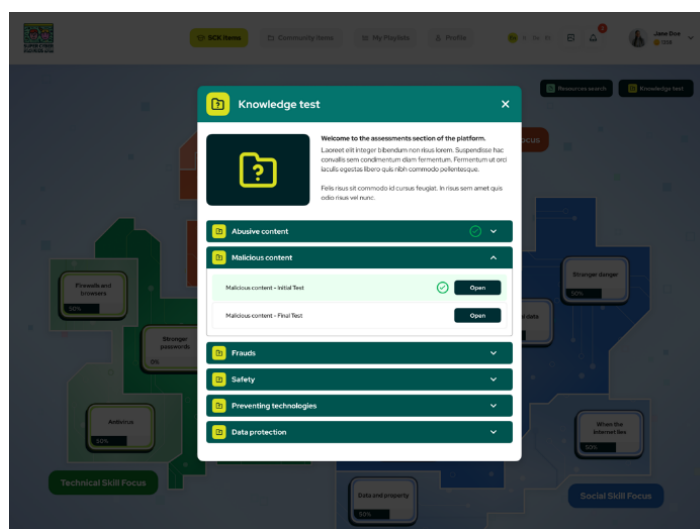


Figure 9 - Knowledge test

Once the user has selected the domain they want to test the knowledge of the classroom about, they are shown two buttons: Initial test and Final test. The Final test can be opened only after the Initial test has been completed.

Both tests can be repeated as many times as wished.

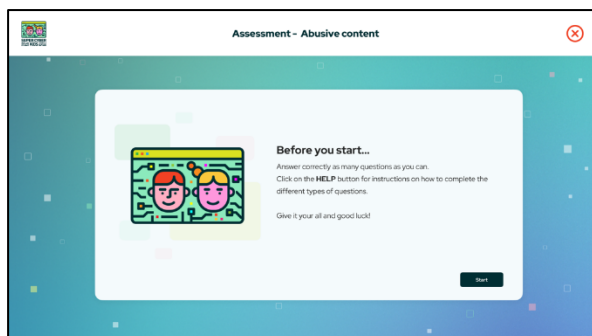


Figure 11 - Start page of the test

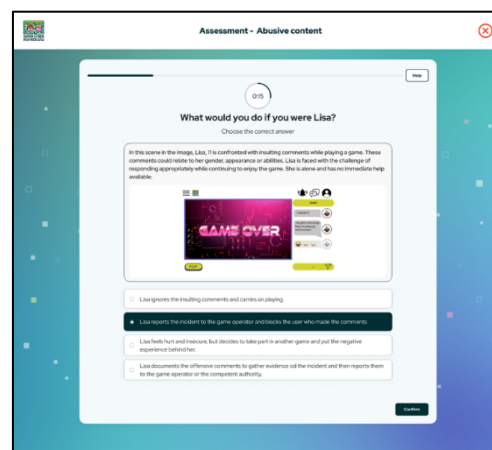


Figure 10 - example of a question in the test

After the users have answered all the questions related to one domain, they are shown a window with the total number of correct answers out of the total number of questions.

The Initial test only shows the points achieved at the end, and no feedback on whether an answer is correct, so that when users do the Final test, they give answers based on what they have learned, not on what they remember from the Initial test. Once a module (consisting of 5 to 13 questions) has been completed, the user receives feedback on how many questions they have answered correctly. At the end of each module, the number of correctly answered questions is displayed. The user can then view the results and compare them with the Initial test at a later point.

User profile

By clicking on the username in the top right-hand corner of the homepage users can access their profile page. In this page it is possible to edit the profile, for example uploading a picture or changing the username and password. The platform can provide evidence of competence, such as a badge.

Badges can be tied to points for completing activities, opening links, downloading documents, successfully responding to quizzes and to performing activities in the platform (e.g. uploading content, post ratings).

All the badges that the user has acquired by performing activities in the platform are shown in the Profile page. In the example shown in the figure above, this user has acquired the following badges

4.5 Select the right skills/modules

By clearly identifying the modules and skills needed to reach pedagogical objectives, teachers can create a more focused, engaging, and effective learning environment that supports student success. For us, it is crucial that teachers have all the information and tools to help them to find their way across the SuperCyberKids ecosystem.

Understand the curriculum map

The map below gives an overview of the modules and skills that should be developed in the classroom or at home by the students. Here are some key elements to understand the map and integrate the modules and skills in teachers’ curriculum and pedagogical objectives.

- **The fundamental skills in cyber for kids from 8 to 13** were identified and clustered at the center (in light grey) of the following figure. These three core modules cover the essential concepts, methodologies and best practices necessary to engage with modules further out in the diagram. This structured approach allows for skills to be reinforced throughout the curriculum and ensures that students have a fundamental understanding before progressing.
- **The curriculum map is presented in multiple layers.** The second and third layer in the curriculum map (in blue and dark grey) are made up of more advanced topics and concepts. Allowing teachers and school administrators to select the materials that are at the appropriate cognitive level for their context. This structured approach allows for skills to be reinforced throughout the curriculum and ensures that students have a fundamental understanding before progressing.
- **Each of the modules has been thematically categorised into three super domains** based on the skills that the student will be engaging with to demonstrate their mastery of the content. This allows teachers and administrators to select the materials that best fit with the context of their specific teaching environment.

Note: These measures promote teacher and administrative autonomy by allowing them to select the appropriate modules for their school or class contexts, while still presenting a framework for them to make informed choices as to the order in which the material is being presented to the students.

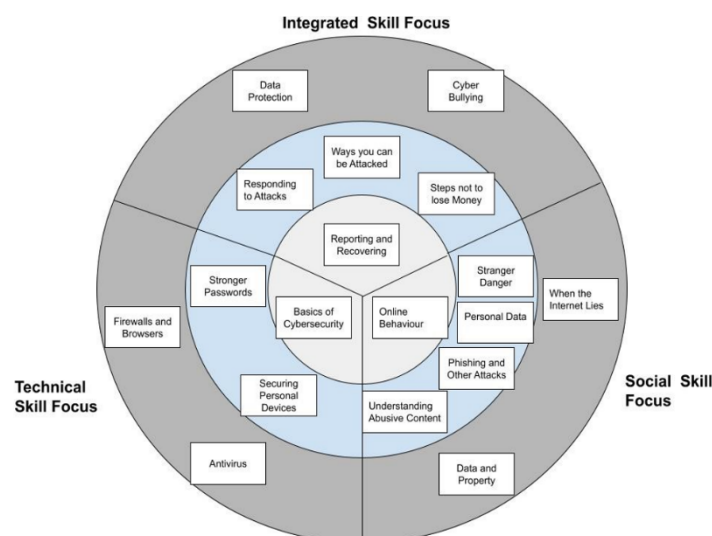


Figure 12 - The SuperCyberKids curriculum map

4.6 The games included in the SuperCyberkids ecosystem

4.6.1 Spoofy

Spoofy teaches children about the dangers of the internet, behaving online and other topics related to smart devices. Engaging, educational and free to play!

Spoofy is a cybersecurity game with the goal to teach children about cybersecurity threats, behaving online and other issues related to smart devices. The game presents different scenarios, the player can collect cyberpets and do other fun things. The target group for the game are younger school aged children, and with an adult, even preschoolers. The originally open worlds are playable separately and do not need a specific order. The school and birthday worlds are shorter and deal with only topics related to kids. The park and grandma’s place are more complicated. Once all four worlds are completed, the cyber machine has been put together and smaller children can play all the worlds again or finish playing. After the four worlds have been completed, a new fifth world opens up: this one is more complicated and is meant for older children, as it requires the player to definitely be able to read. All of the worlds are playable by all ages when playing with an adult.



General rules for playing and moving around

The player can play five different worlds and move between the spaceship and each of the worlds. The first four worlds open up right away; the fifth opens later on. In the game, the player can play in four different worlds and move between the world and the spaceship. Each world has its own individual assignments: solving cyber problems or collecting items. Solving assignments gives the player “experience,” which turns into energy stars. Once the player has accumulated three stars, they can free a pet. The player can then put glasses and hats on the pets.

While walking around, the player can collect different items. They can be on the ground, on the table or given by characters in the game. Some items can be picked up only after certain

assignments have been done. Items go into storage and are divided into two: necessary items and wearable items. Wearable items are marked with a top hat, other items should be kept until they are asked for. The player can wear the wearable items themselves or give them to other characters or pets. They can be removed later. Some wearable items turn up later, the game should be played multiple times. Once the cyber machine is assembled, all assignments are reset and can be done again. Each time the assignments are done, the world reset

How to implement Spoofy in class?

For more details about the implementation of Spoofy with pupils, please see the Appendix 2 and 2 on “Recommendation for educators” and “Spoofy cyber lessons ‘Online Behaviour’”. You will find information on the learning objectives and the lesson plans to help you to integrate the game into your curriculum.

4.6.2 “Nabbovaldo and the Cyber Blackmail”



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.

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.

In this videogame, Nabbovaldo faces the IT threats of Internetopoli; to advance in this challenge and win the game, he will have to perform a series of actions and go through several minigames. The videogame also features new characters who help Nabbovaldo in his quest and have a functional role in the game.

How to use Nabovaldo in class?

For more details about the implementation of Nabbovaldo in class, please see the Appendix 5 and the information on the gameplay and steps to integrate the game into your curriculum.

4.7 Implementation steps: how to use SuperCyberKids in the classroom

For the implementation of SuperCyberKids and its integration in the curriculum in the classroom, we recommend teachers to select for the first learning session the following module: “basics of

cybersecurity". The following teaching and learning approaches are well established and can serve as an inspiration for your work.

Module: Basics of Cybersecurity

Week 1: Introduction to Cybersecurity Threats and Unsafe Content

- **Objective 1:** Students will be able to define unsafe content from their perspective.
- **Objective 2:** Students will be able to contrast different types of cybersecurity threats.
- **Activities:**
 - Discussions on what constitutes unsafe content online.
 - Introduction to various threats such as malware, phishing, and social engineering.
 - Comparison and analysis of different cybersecurity threats through examples and case studies.

Week 2: Password Security

- **Objective 1:** Students will be able to choose a strong password.
- **Objective 2:** Students will be able to explain why a password is needed.
- **Activities:**
 - Guidelines for creating strong passwords.
 - Practical exercises on password strength.
 - Discussions on the importance of password protection.
 - Real-world examples of data breaches to illustrate the need for strong passwords.

Week 3: Antivirus Programmes

- **Objective:** Students will be able to run an antivirus programme
- **Activities:**
 - Introduction to antivirus software.
 - Hands-on practice in scanning and identifying potential threats.
 - Discussion on the role of antivirus programmes in maintaining cybersecurity.

Week 4: Basics of Network Communications

- **Objective:** Students will be able to outline the basics of network communications.
- **Activities:**
 - Understanding how data travels across networks.
 - Fundamentals of protocols and communication channels.
 - Practical exercises on tracing data paths and understanding network components.

4.8 Monitoring and evaluation: sustainability and continuous improvement

Feedback from your pupils: Gather feedback from students on their experience with the platform. Make necessary adjustments to improve the effectiveness of gamified activities.

Your feedback as a professional count! You also have access to a feedback form where you can comment on the platform, send remarks, questions and suggestions. Your operational experience and expertise are important for us to develop the platform and ensure it is aligned with your needs.

Parental Involvement. Keep parents informed about the topics being covered and the resources being used. Home Activities: Suggest activities that parents can do with their children to reinforce learning at home.

Regularly update and diversify gamified activities to keep students engaged. Professional Development: Stay informed about new features and best practices in gamification through ongoing professional development.

Use the SyperCyberKids platform’s “Add a new item” feature to suggest or upload content that you may have developed or have come across that is relevant for cybersecurity. You can add links to other games you know of, or to videos or documents that explain concepts of cybersecurity. The platform provides a range of descriptive tags to help you describe the material you are uploading and sharing with the wider community of other European teachers. You can also rate the contents uploaded or suggested by your colleagues. Thus, the platform can act as a living repository of the best material for teachers for learning activities about cybersecurity in the classroom.

Feedback and Adaptation:

Continuously monitor student progress and adapt the teaching strategy as needed. This should include formative assessments and could be facilitated by in-game analytics.

Assessment and Metrics (Indicators):

- Formative Indicators: Classroom engagement, discussion participation, and on-the-spot feedback during activities like the Spoofy and Nabbovaldo games.
- Summative Indicators: Scores on quizzes (automatically stored in the platform), quality of written assignments, and demonstrated ability to apply learned concepts in practical scenarios.
- Utilise in-game and out-of-game assessments to measure learning outcomes. Be aware of the limitations and benefits of each assessment type as discussed in the guidelines.

4.9 Recommendations for designing a lesson on Cybersecurity

About the content:

- Consider the age group when selecting the depth and breadth of the content.
- Consider the classroom setting and available resources.
- Decide whether the game will be used for homework, in-class individual play, or group play.

- Be aware of pre-existing knowledge and skills among the students to avoid redundancy or excessive complexity.
- Opt for content that allows for multiple educational functions, like demonstration, training, and motivation, to be fulfilled.

Educational Objectives/Learning Outcomes:

- Clearly define what the students should know (knowledge), be able to do (skills), and understand (attitudes) after the lesson.
- Use the SuperCyberKids EU framework as a guide to set these objectives, ensuring alignment with one or more modules like Malicious Code & Cyber Attacks, Data Privacy & Privacy Awareness, Frauds, Preventing Technologies, Abusive Contents and Safety.

Safety Measures:

- Integrate the safety measures and preventive techniques from the SuperCyberKids Learning Framework into the game-based learning environment.

Lesson Activities:

- Use interactive methods like game-based learning to enhance engagement.
- Ensure that the activities are designed to meet the educational objectives set out at the beginning.

Assimilation of Existing Content:

- If using existing content like the Spooify game, make sure to thoroughly understand its educational objectives, capabilities, and limitations.
- Integrate such content smoothly into the lesson plan, ensuring it serves as a complementary tool rather than a disjointed add-on.

Student Engagement:

- Adapt the interaction pattern (Teacher Monitored Use, Group Play, etc.) to maximise student engagement and learning, ensuring alignment with the framework’s objectives.

4.10 Assessment

In class assessment takes the form of teacher observation of activities that are being completed and the student engagement with the materials. This can take the form of continuous assessment of key performance indicators of learning such as time on task, or answering questions posed to the class.

4.10.1 Assessment for students

1. pre-test and post-test:

First, the pretest and post-test created in Section 5.1 can be used as a paper-pencil test (similar to an assessment booklet). This test should be collected by the teacher after completion and sent to the consortium partners.

Note: The consent of the parents is important. Therefore, a corresponding consent form should be requested from the responsible office. It must also be possible to assign the tests anonymously so that children or parents have the option of withdrawing their consent. For this reason, the consortium partners recommend this test as optional.

2. splash board as an in-class assessment:

Alternatively, it is recommended to primarily use a splash board, which is photographed by the teacher at the end of the lesson and sent to the consortium partners.

A board splash is where the teacher gets students to either prepare an artistic representation of what they have learned directly on the board or separately and then they are placed together. This can take many forms such as post its with suggestions for rules to make and remember passwords, or drawings of what to do when a student experiences cyber bullying. The teacher gathers this work and the whole class makes a collage which the teacher can then photograph to store the data and use it later.

4.10.2 Assessment for teachers

To assess the platform, two methods can be used by teachers.

A **feedback form** (Appendix 1) for each of the target audiences of the SuperCyberKids platform with specific questions based on their different tasks and responsibilities (School heads, teachers, students and parents). The form will be available via a link integrated and sent via the platform. The collection and analysis of results will be performed by the relevant consortium partners.

A **focus group** aimed at teachers and head-teacher will be carried out with the goal of gathering and discussing observations and viewpoints on the use of the SCK platform and its possible future adoption, also collecting insights derived from direct experience with children. A focus group is a research method used to gather in-depth insights and diverse perspectives from a targeted group of participants. Through guided discussions, it enables the collection of qualitative data on attitudes, opinions, and experiences related to a specific topic or product. The interactive nature of a focus group fosters dynamic exchanges, allowing researchers to observe participant reactions, uncover underlying motivations, and identify areas for improvement or innovation.

4.11 Conclusion

Implementing a gamification platform can transform your classroom into an interactive and motivating learning environment. By following this package, you can effectively integrate gamification into your teaching practice and enhance student learning outcomes. Feel free to customise this package to better fit your specific classroom needs and goals.

5 Implementation package for parents and students

5.1 Introduction

As our children grow up in an increasingly digital world, it is crucial for parents to be proactive in educating them about the risks they may encounter online. This set of guidelines is designed to help parents use a dedicated platform to teach their kids about cyber safety through engaging games, educational materials, and interactive resources. Children can also use the based accompanied by an adult or play the game autonomously. By leveraging these tools, parents can create a supportive and informative environment at home, where children can learn to recognise and respond to cyber threats, understand the importance of protecting their personal information, and develop responsible online behaviours. These guidelines aim to empower parents with practical strategies and resources to ensure their children are well-prepared to navigate the digital landscape safely. Together, we can foster a safer online experience for our children, equipping them with the knowledge and skills they need to thrive in the digital age. Let's work together to build a secure and informed online community for our kids.

A "take home" kit with general tips for children and parents, and online games are included in the SuperCyberKids game-based learning. One effective way for parents and caregivers to support their children in navigating the digital world is to stay informed about the various online issues and challenges. Check out some key points below, or explore the site for additional information

5.2 Objectives

The primary objective of these guidelines is to equip parents with the knowledge and tools necessary to educate their children about cyber risks effectively. By utilising a dedicated platform, parents can create an engaging and interactive learning environment at home, using games, educational materials, and resources to teach their kids about online safety, helping children recognise and respond to cyber threats, understand the importance of safeguarding personal information, and develop responsible online behaviours. Ultimately, the goal is to foster a safer digital experience for children, ensuring they are well-prepared to navigate the online world with confidence and security.

SuperCyberKids: toolkit for future citizens

From 8 to 13, children are getting able to think logically and in a more abstract way. They have become critical thinkers able to distinguish reality from fantasy more easily. At this stage, the 8–13-year-old kid can manage to participate in more complex and sophisticated conversations and starts seeing the world from his or her own point of view as they are more interested in facts and knowledge. As a matter of facts, at this stage, the child and later on, the pre-teen, will tend to become more interested in others and is ready to adopt a more social 'world view'.

SuperCyberKids can become a toolkit for them to comprehend and confront the world on the internet in a more secure way. SuperCyberKids should be included in the pedagogical and educational project of the school highlighting the fact that being safe online has become significant and essential for the development and the autonomy of the pupils as future responsible citizens.

5.3 General tips

Familiarisation with the platform. To effectively use SuperCyberKids, parents should start by familiarising themselves with the platform’s features and resources.

Engage with your child by exploring interactive games and educational materials together, making learning about cyber safety a fun and collaborative experience. Use the Search function in the platform to look for specific resources appropriate for the age and interests of your child. Encourage open communication, allowing your child to ask questions and share their online experiences. Set clear guidelines and expectations for online behaviour and use the platform’s tools to monitor your child’s progress and understanding. Additionally, reinforce the lessons learned on the platform with real-life examples and discussions about current cyber threats. By staying involved and informed, parents can create a supportive environment that empowers children to navigate the digital world safely and responsibly.

5.4 Where to start: onboarding the SuperCyberKids platform

Landing page

In this page users will find very general information about the SuperCyberKids project and the platform.

The LOGIN button allows registered users to enter the platform.

The SIGN-UP button allows new users to register.

Accessing the platform: Registration and Login

After filling in the Registration form, the system sends an automated email to the registered address with login details (Username and Password). Users can change their password upon first login.

5.5 Navigate in Super Cyber Kids ecosystem

Homepage with map of the SCK modules

This page is viewed when the users enter the platform. It contains the **map of the 18 modules that have been prepared and approved by the SCK project**. They make up the SCK education eco-system on cybersecurity. Through a set of buttons and menus, this page gives also access to all the functionalities of the platform.

The map of the modules has been designed to look like a computer motherboard. It is divided into three areas, each of different colour:

- Technical Skill (green)
- Social Skills (blue)
- Integrated Skills (red).

The colour of the three areas grows lighter when nearing the outermost part of the circle; in the centre the colour is deeper, indicating that those modules are at the core of the SCK recommended curriculum, as explained in R3.1.1 “Guidelines for schools (head teachers and teachers) - initial version”.



Figure 13 - home page or map of SCK approved modules

The top menu contains the following buttons:

SCK items: access to this page, where users can select one of the 18 modules available. By clicking on this button on the top menu in other pages of the platform the users go back to this page.

Community items: access to resources suggested or uploaded by users to be used by the SCK community at large (see section 4.5 below).

My Playlists: access to a selection of specific resources by the user currently logged in to the platform.

Profile: access to the Profile page with information about the user currently logged in (section 4.9).

Buttons provided in the top menu enable to change the language of the user interface (English, Italian and Estonian).

In the top right-hand corner there two buttons:

- Search
- Knowledge test

That give access respectively to the Search function (see section 4.4.3) and to the Knowledge test for assessing initial or final knowledge (see section 4.4.5).

Community Items

This page can be accessed by clicking on the “Community items” button on top of the navigation page. This area of the platform is a common repository of all resources uploaded by users (teachers). It contains all the items uploaded and catalogued by users and is visible to all users registered in the platform.

PLEASE NOTE: all items shown in this mock-up are fictitious, they DO not refer to real items and are shown only for demonstration purposes.

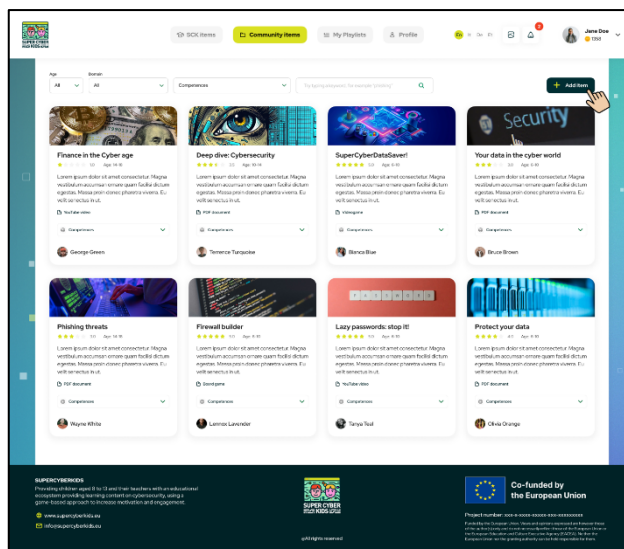


Figure 14 - Community items desktop

The items are shown as cards. Each card contains a short descriptive text, and the list of competencies associated to that item (viewed by clicking on the drop-down menu Competencies). At the bottom there is also the username of the user who uploaded that learning resource.

The cards for Community items also contain an indication of the type of resources (videogame, PDF document, YouTube video).

How to add an item to the Community items repository

To suggest or upload a new learning resource or item to the repository (“Community items”), user can click on the button ADD ITEM in the top right-hand corner (see figure 6 above). They are shown a window where they can select all the appropriate metadata to associate to the file they are uploading:

- Title* (open field)
- Description (open field)
- Age*
- Language*
- Competency Domain and related competencies*
- Item type* (Game, Lesson plan, Video, Document)
- Lesson Style [game-based learning, traditional classroom, other]
- Intended Learning Outcomes (open field, only for lesson plans)
- Image associated to that item.

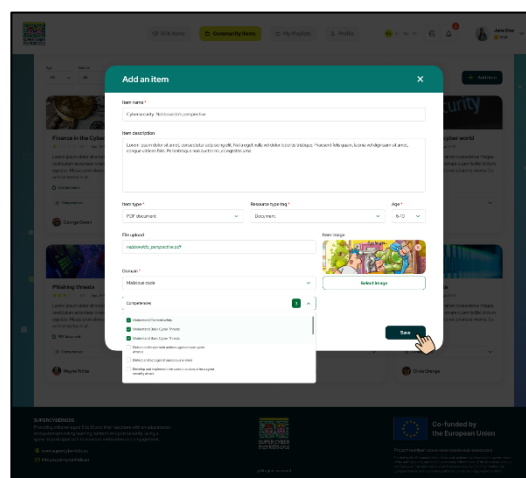


Figure 15 - add an item to the common repository

How to add an item to a personal playlist

After a user has uploaded an item with all the appropriate metadata, they can select that item (or others in the Community items area of the platform) to create their own playlist.

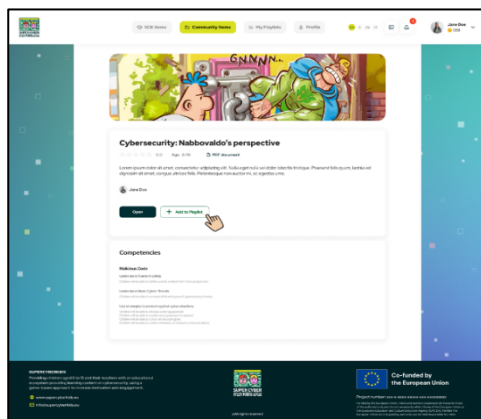


Figure 16 - add an item to the playlist

Search function

The Search function can be used to retrieve learning resources in both areas of the platform, the SCK approved modules and the Community items uploaded by users. After clicking on the button RESOURCE SEARCH in the home page (see figure 5), users can access the Search page (see figure 9), where they can type one or more keywords, and select options from three drop-down menus:

Age

Domain (referring to the six domains of cybersecurity identified in the project, Malicious Code, Frauds, Preventing Technologies, Abusive Content, Data Privacy & Data Awareness, and Safety)

Competencies [please note that when a domain is selected, the drop-down menu Competencies shows only the competencies pertaining to that domain].

The figure below shows the result of a search with the keyword “Cyber”.

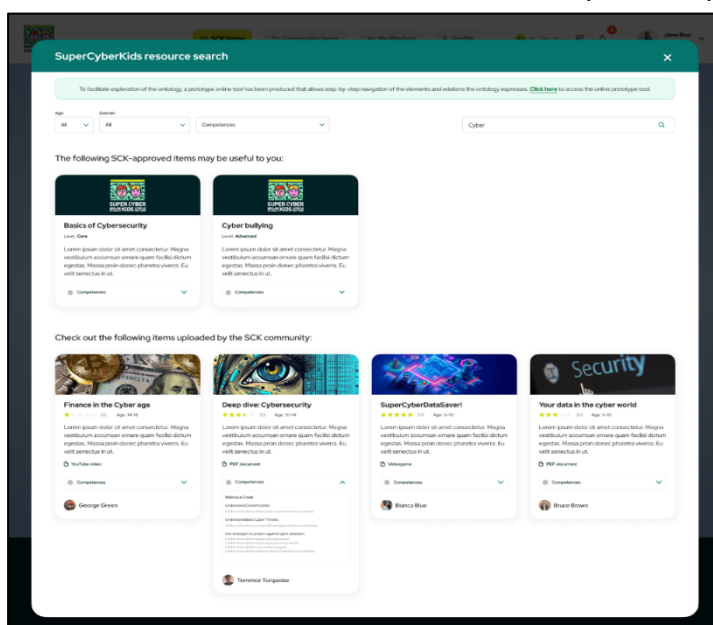


Figure 17 - Search page with results

PLEASE NOTE: all items shown in this mock-up are fictitious, they DO not refer to real items and are shown only for demonstration purposes.

The page that shows the results of the Search is divided into two areas:

the top area shows the items matching the search retrieved in the ***SCK approved items*** area of the platform, that contains the 18 modules set up by the SCK project;

the bottom area shows the items matching the search retrieved in the ***Community items*** area of the platform, a common repository of all resources uploaded by users.

Results are shown in form of card. Each card refers to an item, and contains a short descriptive text, and the list of competencies associated to that item (see in the example above: item “Deep dive: Cybersecurity”). At the bottom of the card there is also the username of the user who uploaded that learning resource.

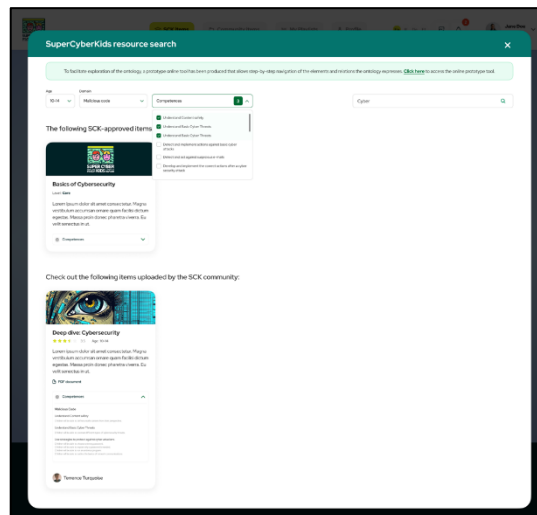


Figure 18 - search using specific competencies

The cards related to Community items also contain an indication of the type of resources (videogame, PDF document, YouTube video).

Below there is an example of a specific search using the fields provided: age: 10-14, domain “Malicious Code”. The user can select the competencies related to that domain in the drop-down menu by checking the boxes.

In the top of the page (green background) there is a link to the Ontology Domain Explorer tool developed by CNR, as additional (external) tool to explore the ontology.

Launching a module

This figure shows what happens when a user clicks on one of the 18 modules in the navigation page (see section 4.4 above). All modules are open, i.e. there is no fixed sequence to follow. In the example shown, the user has selected the module “Firewalls and browsers”.

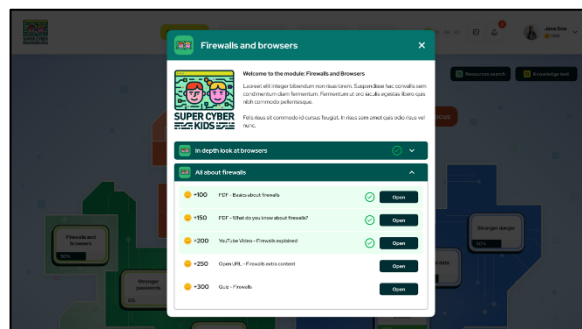


Figure 19 - Opening a module

The window contains a list of all the items that make up the module: they can be a lesson plan, a document to download, a quiz to test the knowledge, or ***a link to a game***. Opening each item the user gains points that make up the final score.

When all the items in the module have been opened, and, in case of a quiz, the quiz has been passed, the user is shown this window with the final score for that module.

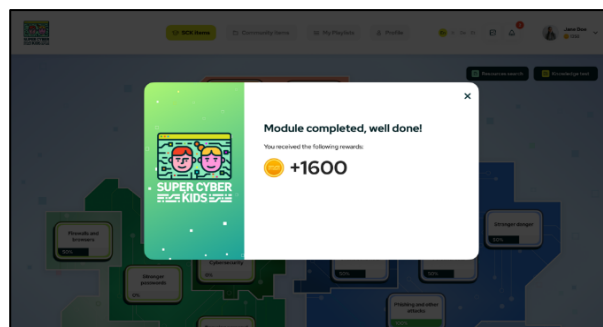


Figure 20 - module completed

Everything you need to know about the knowledge tests

The Knowledge test can be accessed by the button in the top right-hand corner of the Home page (see section 4.4.). It contains the initial and final assessment divided into the six domains of cybersecurity: *Malicious Code*, *Frauds*, *Preventing Technologies*, *Abusive Content*, *Data Privacy & Data Awareness*, and *Safety*. Users can select the domain and start answering the test.

It is designed to be used by teachers in the classroom, asking questions to their pupils to test their knowledge of the topics in each domain. See Report 5.1.1. “Implementation of the tools for measurement and assessment of educational intervention” developed by UMA: “One possible implementation scenario could be the teacher going through the tool together with the class in the classroom”.

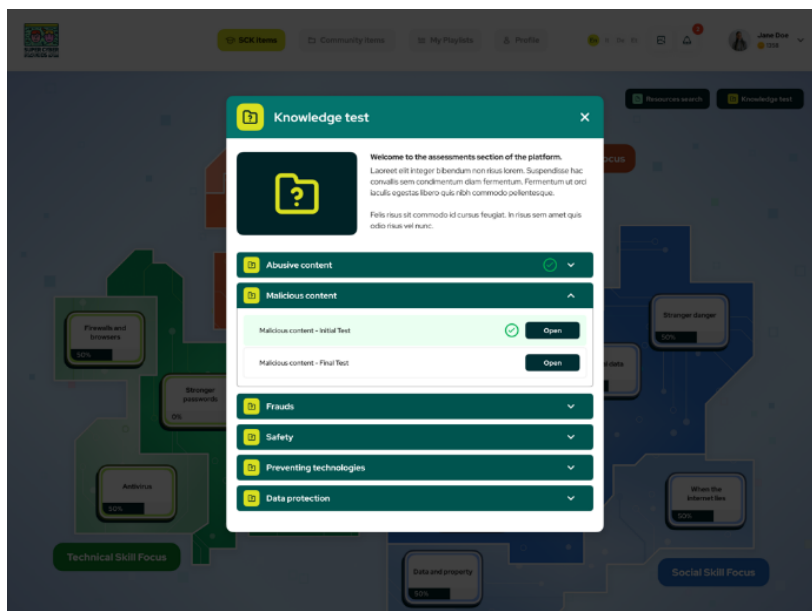


Figure 21 - Knowledge test

Once the user has selected the domain they want to test the knowledge of the classroom about, they are shown two buttons: Initial test and Final test. The Final test can be opened only after the Initial test has been completed.

Both tests can be repeated as many times as wished.

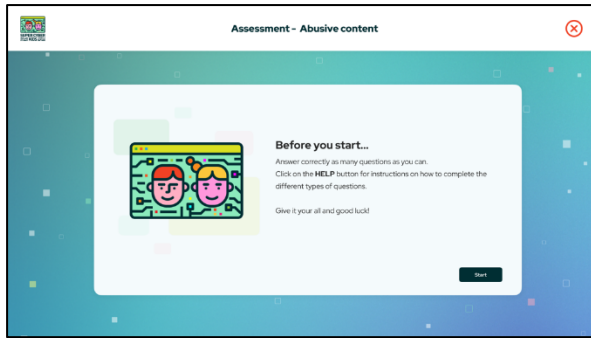


Figure 23 - Start page of the test

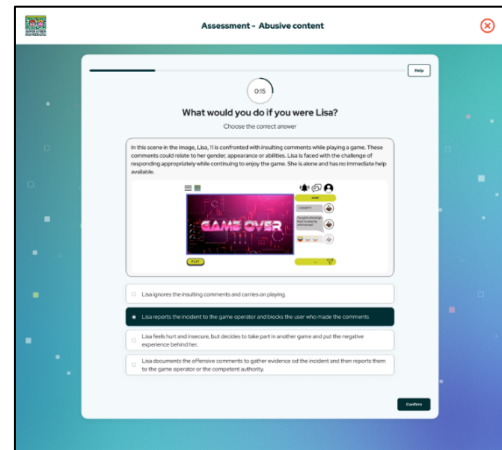


Figure 22 - example of a question in the test

We can set up a countdown for each question (optional), shown on the top of the window. After the users have answered all the questions related to one domain, they are shown a window with the total number of correct answers out of the total number of questions.

The Initial test only shows the points achieved at the end, and no feedback on whether an answer is correct, so that when users do the Final test, they give answers based on what they have learned, not on what they remember from the Initial test. Once a module (consisting of 5 to 13 questions) has been completed, the user receives feedback on how many questions they have answered correctly. At the end of each module, the number of correctly answered questions is displayed. The user can then view the results and compare them with the Initial test at a later point.

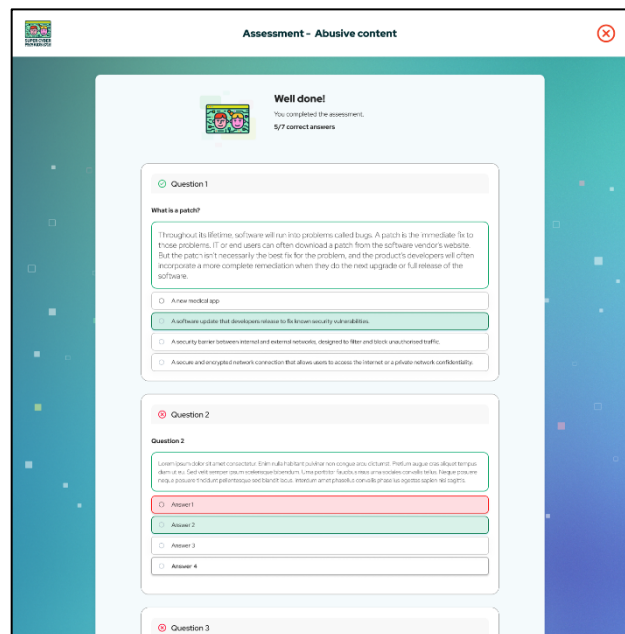


Figure 24 - Results page at the end of the Final test

User profile

By clicking on the username in the top right-hand corner of the homepage users can access their profile page.

In this page it is possible to edit the profile, for example uploading a picture or changing the username and password.

The platform can provide evidence of competence, such as a badge.

Badges can be tied to points for completing activities, opening links, downloading documents, successfully responding to quizzes and to performing activities in the platform (e.g. uploading content, post ratings).

All the badges that the user has acquired by performing activities in the platform are shown in the Profile page. In the example shown in the figure above, this user has acquired the following badges

Profile page. In the example shown in the figure above, this user has acquired the following badges

5.6 Stay up to date: SuperCyberKids online open-source repository for education

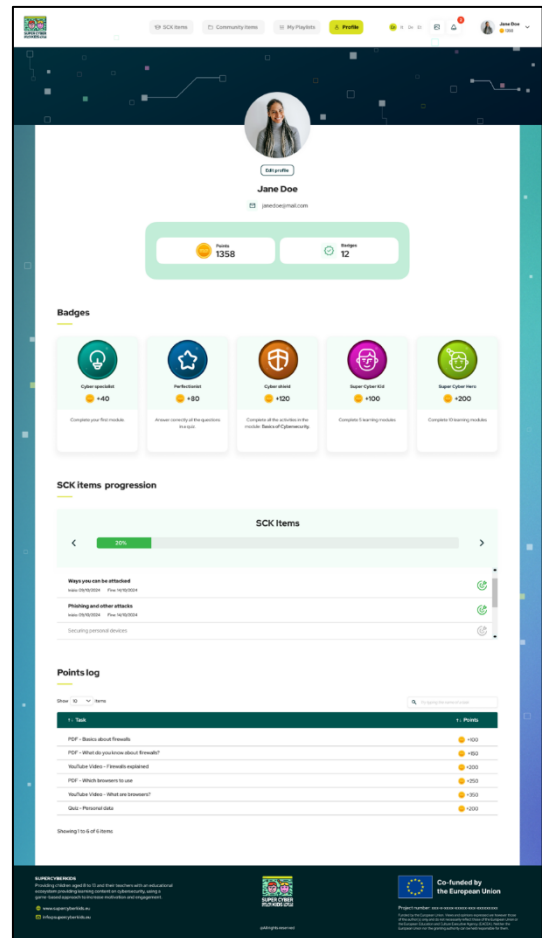


Figure 25 - User Profile page

SuperCyberKids gives you access to a wide range of online teaching resources, linked to the map of modules and skills in the appendix. SuperCyberKids is the European gateway to all the initiatives where your child can acquire skills and learn in a fun way, and where you too can enrich your knowledge of the challenges of cyber security and its place in children's education.

6 Appendix

- **Appendix 1:** Feedback form
- **Appendix 2:** Open-source repository (cf in the Teams)
- **Appendix 3:** Spoofy lesson plan: Oline Behaviour
- **Appendix 4:** Spoofy instructions for educators
- **Appendix 5:** How to use Nabbovaldo in class?
- **Appendix 6:** SuperCyberKids lesson plan template

6.1 Appendix 1: Feedback form

Feedback form for School heads

Question	Topic of the question	Categories of information	Question type	Expected information
What is the name of your school?	Name of school	General information	Open question	Information on users
What is the age of your students using SuperCyberKids?	Age	General information	Multiple choice question	Information on users
What are the reasons why you started to use the SuperCyberKids platform ?	Use of the platform	User motivation	Open question?	Information on awareness/dissemination?
What domains or modules are more interesting for you now?	Modules	User motivation	Multiple choice question	Better identify and target the needs in the market
Would you recommend SuperCyberKids to your colleagues?	Future recommendation	User experience	Multiple choice question	Identify functionalities to improve and align SCK with the needs of users
How did you learn about SuperCyberKids?	Promotion	General information	Multiple choice question*	Information on awareness/dissemination ?
What would you improve on the platform	Future recommendation	User experience	Multiple choice question**	Identify functionalities to improve and align SCK with the needs of users
How do you integrate SCK in the general objectives of your school?	Learning objectives	User Experience	Open-ended question	Better define of SCK is integrated in the learning objectives and curriculum of schools

Feedback form for teachers

Question	Topic of the question	Categories of information	Question type	Expected information
What is the name of your school?	Name of school	General information	Open question	Information on users
What is the age of your students?	Age	General information	Multiple choice question	Information on users
How did you learn about SuperCyberKids	Promotion	General information	Multiple choice question	Information on advertisement
Would you recommend SuperCyberKids to your colleagues?	Future recommendation	User Experience	Open-ended question	Information on advertisement
On what topic(s) do you find SCK useful in class?	General use	User Experience	Open-ended question	Identify the needs of teachers

Feedback form for parents

Question	Topic	Categories	Question type
How did you learn about SuperCyberKids?	Promotion	General information	Multiple choice question
Would you recommend SuperCyberKids to others?	Future recommendation	User Experience	Open-ended question
How do you rate the usability of SCK?	General use	Platform features	Open-ended question
How would you describe your overall experience using SuperCyberKids?	General use	User Experience	Rating (scale from 1 to 10)
Functionalities to be improved	Future recommendation	User Support	Open question

6.2 Appendix 2: Open-source repository of initiatives relevant for School leaders

Name of the CE initiative/project	Language	Type	Mapped to modules	Description
Dark Fairytales	English	Awareness raising	Online Behaviour	Surfshark's Dark Fairytales Cybersecurity Books for Children is an initiative designed to teach kids about online safety and cybersecurity through modernized versions of classic fairytales. These books take familiar stories and adapt them to highlight various online threats, such as phishing, malware, and privacy issues, making complex cybersecurity concepts accessible and engaging for young readers. The stories are complemented by interactive elements and illustrations to keep children interested and help them understand the importance of safe online practices. The goal is to instill good cybersecurity habits in children from an early age, combining entertainment with education to make learning about internet safety both enjoyable and effective.
Madebykids	English	Awareness raising	Basics of cyber security	Youth Hackathon is an initiative created by MadeByKids in collaboration with various educational and corporate partners, aiming to provide free access to coding, game design, and app development for students, especially girls, in Austria. The project involves hands-on, game-based learning experiences that promote technical skills, creativity, and teamwork. The main goals of Youth Hackathon are to enhance digital literacy, foster interest in STEM fields, and equip young people with essential skills for the digital age. The initiative seeks to prepare students for future job markets by developing their computational thinking, problem-solving abilities, and innovative potential.
Safer Internet Day	English	Awareness raising	Online Behaviour	Safer Internet Day 2021, celebrated on February 9th, aimed to promote safe and positive use of the internet. Specifically, the initiative sought to: -Raise awareness among young people about responsible social media use. -Educate parents and teachers on protecting children online. -Engage authorities and policymakers to implement effective online safety policies. -Encourage collaboration among various

				organizations to create a better and safer internet.
Better internet for kids (BIK+)	English	EU Policy initiative	Cyber Bulling	<p>The Better Internet for Kids (BIK+) Strategy, launched by the European Commission in May 2022, aims to improve digital services for children, ensuring their protection, empowerment, and respect online. The strategy is based on three main pillars:</p> <ul style="list-style-type: none"> Safe digital experiences: protecting children from harmful and illegal online content, behavior, and risks, while enhancing their digital well-being. Digital empowerment: providing children with the skills needed to make informed decisions and express themselves safely and responsibly online. Active participation: giving children a voice in the digital world, promoting child-led activities for innovative and safe digital experiences. <p>The strategy is supported by extensive consultations with children, parents, teachers, member states, the ICT industry, civil society, and international organizations. A child-friendly version of the strategy was developed with input from young ambassadors to make it accessible to all age groups.</p>
DigComp 2.2	English	EU Policy initiative	Basics of cyber security	<p>DigComp 2.2 aims to enhance digital competence across Europe by providing a detailed framework for the knowledge, skills, and attitudes needed in the digital age. The objectives are:</p> <ul style="list-style-type: none"> -Promote digital literacy: equip citizens with the ability to understand and engage with digital technologies. -Support lifelong learning: encourage continuous development of digital skills to adapt to evolving technologies. -Enhance employment opportunities: provide a basis for developing digital skills relevant to the job market. -Improve online safety: educate on safe and responsible use of digital technologies. <p>Foster creativity and innovation: encourage the creation and sharing of digital content.</p>

European Education Area	English	EU Policy initiative	Basics of cyber security	The Digital Education Action Plan (2021-2027) is an initiative by the European Union to enhance digital education across Europe. It focuses on fostering a high-performing digital education ecosystem and enhancing digital skills and competencies for the digital transformation. The plan includes actions to support digital literacy, tackle disinformation, and improve access to digital tools and resources. It aims to ensure that education and training systems are fit for the digital age and resilient to future challenges.
The Danish National Strategy for Cyber and Information Security	English	National Programme	Basics of cyber security	The Danish National Strategy for Cyber and Information Security 2022-2024 aims to enhance Denmark's resilience against cyber threats. The main focus areas include: -Protection of vital societal functions: strengthening the security of critical government ICT systems, supporting SMEs, and enhancing police capabilities against cybercrime. -Improving skills and management: promoting digital literacy and security awareness among public and private sector leaders. -Public-private cooperation: encouraging collaboration between the government and businesses and establishing a national cybersecurity hotline. -International participation: increasing involvement in international collaborations with the EU, UN, and NATO to counter cyber threats. The government has allocated DKK 270 million for 34 key initiatives.
The national cybersecurity strategy	English	National Programme	Basics of cyber security	National Cybersecurity Strategy (NCSS) is a plan of action designed to enhance the security and resilience of national infrastructures and services against cyber threats. It is a high-level, top-down approach that sets out a range of national objectives and priorities to be achieved within a specified timeframe. The key objectives of an NCSS include: -Cybersecurity governance and standards: establishing robust governance frameworks and adhering to high cybersecurity standards. -Capacity building and awareness: improving skills and raising awareness about cybersecurity among citizens, businesses, and government entities.

				<p>-Legal and regulatory measures: implementing effective laws and regulations to protect against cyber threats and ensure compliance.</p> <p>-Public-private cooperation: promoting collaboration between public institutions and private companies to share knowledge and resources.</p> <p>International cooperation: engaging in international partnerships to strengthen global cybersecurity efforts.</p>
The national cybersecurity strategy of Czech Republic	English	National Programme	Basics of cyber security	<p>The National Cybersecurity Strategy of the Czech Republic for the period 2021-2025 aims to enhance the security and resilience of national infrastructures and services against cyber threats. The strategy addresses various challenges and sets specific goals to ensure a secure digital environment.</p> <p>Objectives:</p> <p>-Strengthening cyber defense: enhancing capabilities to protect against cyber threats and ensuring a robust defense system, including military operations in cyberspace.</p> <p>Governance and regulatory framework: implementing effective governance structures and regulatory measures to support cybersecurity efforts.</p> <p>Capacity building and awareness: improving skills and raising awareness about cybersecurity among citizens, businesses, and government entities.</p> <p>Public-private cooperation: fostering collaboration between public institutions and private companies to share knowledge and resources.</p> <p>International cooperation: engaging in international partnerships to strengthen global cybersecurity efforts and enhance national security.</p> <p>The strategy is implemented by various bodies, including the National Cyber and Information Security Agency (NÚKIB), which oversees cybersecurity policies and coordinates efforts across different sectors</p>

Cybermarvel / eSafetyeducation	English	National Programme & materials	Online Behaviour	<p>The eSafety webiste is a governative website containing resources helping different stakeholders manage online safety issues. Target stakeholders are young people, educators, kids, and parents. The website provides readers with information and support when dealing with violent or distressing online content.</p> <p>Cybermarvel is an educational project aimed at promoting cybersecurity awareness and skills among students from New South Wales. It contains interactive activities, online challenges, and competitions to deliver cybersecurity knowledge and safe online behavior. The website includes educational resources for teachers and students. Its main goal is to inspire interest in cybersecurity careers and promote a deeper understanding of online safety.</p>
Cyber Security Challenge PT	English	Talent search initiative	Basics of cyber security	The website of the Portuguese National Cybersecurity Centre is dedicated to the "Capture The Flag" event and mainly includes information about this cybersecurity competition. The is infact a structured competition aimed at supporting the development of cybersecurity attitude and skills, providing participants with practical challenges and learning opportunities in a competitive environment.
CyberEnJeux	French	Teaching materials	Basics of cyber security	The website of the French Cybersecurity Agency (ANSSI) provides information about this governmental organization that is responsible for cybersecurity. The site describes aims and responsibilities of the organization and also contains a number of services, including training and certification of cybersecurity products and services.
Cyber Security for Schools	English	Teaching materials	Basics of cyber security	The https://www.ncsc.gov.uk/ is the website of the National Cyber Security Centre. The section dedicated to education contains advice, resources, and opportunities for schools and students, especially involved in higher education, interested in cyber security. The website also provides teachers with professional training and contains content related to CyBok, a project aiming at providing a foundation for the development of the cyber security profession.

Saferinternet.at	German	Teaching materials	Cyber Bulling	SaferInternet.at is a website devoted to the promotion of a safe use of the Internet among different stakeholders (young, parents, teachers, and young workers). It contains educational content related to a number of issues (e.g., cyberbullism, social media, digital games, and problematic content). It also includes several online services to support stakeholders' gathering of information such as newsletter and a brochure service.
Cyber Citizen	English	EU Policy initiative	Basics of cyber security	The Cyber Citizen initiative aims at realizing a learning model for cybersecurity and a learning portal based on that model. Content of the learning portal is designed for the use of all citizens and take into account different target groups. To this aim, a game will be realized as well.
PARTICIPATE	English (and potentially Greek, Finnish, Danish and Irish)	Policy recommendations, teachers and parents guides+ new research	Cyber Bulling	The PARTICIPATE project PARTICIPATE brings together Europe's top experts in anti-cyberbullying to build a research and training network that will: 1. Create world-class Early Stage Researchers (ESRs) with transferable multi-disciplinary and intersectoral skills necessary to work with parents, youth, teachers and other professionals to more effectively prevent and reduce cyberbullying across Europe 2. Introduce a vital new dimension into cyberbullying research by investigating the largest group of parents ever studied 3. Harness the knowledge and perspectives being developed in different countries, academic disciplines, youth organisations and technology companies, uniting them in a powerful, strategic collaboration in the fight against cyberbullying in Europe 4. Develop sufficient expertise on parents to create a state-of-the-art toolkit for teachers and other professionals working with parents to prevent cyberbullying

Repository of initiatives relevant for teachers

Name of the CE	Language	Type of initiative	Mapped to modules	Description
----------------	----------	--------------------	-------------------	-------------

initiative/project				
BEE SECURE	English	Teaching materials	Basics of cybersecurity	BEE SECURE is an initiative by the Luxembourg government that promotes safety and responsibility in the use of information and communication technologies. It offers educational resources, training, and support on topics such as personal data protection, cyberbullying prevention, and online safety for various age groups. The goal is to raise awareness and educate the public on how to navigate the internet safely and responsibly, protecting their privacy and recognizing online risks.
Bulgarian Safer Internet Centre	English	Teaching materials	Basics of cyber security	Bulgarian Safer Internet Centre is dedicated to protecting, supporting, and educating children and young people about the safe use of digital technology. A key program, the Cyberscouts Training Programme, trains children aged 11 to 13 to recognize online risks and act as advisors for their peers, promoting online safety. Other objectives include awareness campaigns, training for teachers and parents, and support through a helpline for online safety-related psychological consultations.
Cyber Explorers	English	Teaching materials	Basics of cyber security	Digital Explorers is a series of cartoons promoted by the European Union to educate young people about the opportunities and challenges of digitalization. It follows characters Helena, Klaus, Kasia, Enzo, and Marion on a journey across Europe to explore topics such as artificial intelligence, supercomputers, blockchain, and online security. The goal is to inform and raise awareness about digital advancements, promote online safety, and illustrate how digital technologies influence Europe's future.
Cyber Guide Famille	English	Teaching materials	Basics of cyber security	Cyber Guide Famille is an initiative by Cybermalveillance.gouv.fr aimed at raising awareness among families about cybersecurity risks. It provides ten practical recommendations to protect families from cyber threats, covering topics such as password management, backups, updates, and phishing prevention. The goal is to educate parents and children about good digital practices and improve their online security through guides and interactive quizzes.
Cyber Safe Kids	English	Teaching materials	Phishing and other attacks	Cyber Safe Kids by Palo Alto Networks is an educational program aimed at raising awareness about cybersecurity among children and families. The initiative offers: -Free workshops: interactive sessions led by experts to teach good online security practices. -Guides and activities: educational materials to help parents and teachers discuss digital safety with children. -Online courses: training modules for different age groups, focusing on common threats like phishing, password protection, and privacy. The goal is to provide tools and knowledge for safe and responsible online navigation.

Cyber Security for Schools	English	Teaching materials	Basics of cyber security	<p>Cyber Security for Schools in the UK aims to develop cybersecurity skills among students through various educational programs. These include:</p> <ul style="list-style-type: none"> -CyberFirst: a series of courses and competitions for young people aged 11 to 17, designed to spark interest in cybersecurity. -Cyber Schools Hub: collaborative programs with schools to enhance cybersecurity education. -Cyber Discovery: a competition for students aged 13 to 18 aimed at discovering and developing talents in cybersecurity. <p>The main goal is to prepare the next generation of cybersecurity professionals, providing the skills needed to tackle future cyber threats.</p>
CyberEnJeuX	French	Teaching materials	Basics of cyber security	<p>CyberEnJeuX promoted by ANSSI, in collaboration with the French Ministry of Education, is an educational program that uses games to teach middle and high school students about cybersecurity. The main objectives include:</p> <ul style="list-style-type: none"> -Awareness: educating students about digital risks and good cybersecurity practices. -Active learning: using game-based activities like hackathons to teach complex cybersecurity concepts. -Skills development: increasing students' interest in careers in the cybersecurity field.
Cyberinformed Citizen Course	Portugues	Teaching materials	Basics of cyber security	<p>Internet Segura is part of the European Safer Internet Plus program and aims to promote safe, conscious, and critical internet use among Portuguese citizens. Its objectives are:</p> <ul style="list-style-type: none"> -Education and awareness: raising awareness of cyberspace threats and encouraging safe and responsible browsing. Protection of minors: ensuring that children and adolescents use the internet safely, educating them about risks and online safety practices. Support and assistance: providing tools and support to protect users from illegal content and dangerous online behaviors. <p>Cyberinformed Citizen Course is part of the e-learning offer available on the NAU platform (within the Internet Segura site). This course is designed to improve citizens' digital skills, covering various aspects of cyber hygiene. Topics include:</p> <ul style="list-style-type: none"> - Main threats in cyberspace. - Best practices for using technologies. - Disinformation and safe online consumption. - Security and privacy on social networks. <p>The courses are accessible for free and aim to make online navigation safer for all participants.</p>

CyberSafeKids	English	Teaching materials	Basics of cyber security	CyberSafeKids is an Irish charity founded in 2015, dedicated to making children stronger, smarter, and safer in the online world. The organization provides innovative educational programs, research, and advocacy to help children, parents, schools, and businesses navigate the digital world safely and responsibly. They collaborate with schools to teach students how to use the internet safely, with parents to raise awareness about their children's online activities, and with businesses to support working parents.
Cybersecurity Lab	Czech	Teaching materials	Anti virus and other security applications	NOVA Cybersecurity Lab by PBS is an educational initiative aimed at teaching participants how to protect their digital lives. Through a series of interactive challenges, users take on the role of a technology manager at a startup and must defend the company from increasingly sophisticated cyberattacks. The main goals of the project are: - Educating about cybersecurity: providing knowledge about digital threats and defense techniques. - Developing coding skills: helping participants learn the basics of programming. - Promoting critical thinking: teaching how to identify and manage online scams. - Raising digital awareness: emphasizing the importance of data protection and online privacy. The project uses educational videos and practical activities to make learning engaging and applicable to real life.
Cyberwise	English	Teaching materials	Phishing and other attacks	CyberWise is an Irish educational initiative aimed at teaching cyber resilience in primary and secondary schools. The main goal is to develop an understanding and management of cybersecurity challenges. Specific objectives include: - Education on cybersecurity: providing in-depth knowledge about digital risks and how to mitigate them. - Promoting female participation: encouraging girls' participation in the cybersecurity field. - Collaboration with schools and institutions: implementing pilot courses and providing educational resources for teachers and students. The project is funded by the Department of the Environment, Climate and Communications (DECC) and supported by various academic and professional institutions.

European CyberSafety Projects	Greek	Teaching materials	Basics of cyber security	<p>European CyberSafety is a collaborative initiative aimed at improving online safety for young people through various educational and awareness activities. The main objectives include:</p> <ul style="list-style-type: none"> -Promoting safe Internet use: educating young people, parents, and educators about online risks and safety measures. -Supporting cyberbullying victims: providing resources and helplines for those affected by cyberbullying. -Creating a European cooperation network: collaborating with other European countries to share best practices and resources.
Festival of Safe Internet	English	Series of educational events	Basics of cyber security	<p>Festival of Safe Internet is an initiative organized by NÚKIB (National Cyber and Information Security Agency) of the Czech Republic, aimed at promoting online safety among young people, educators, and the general public. The main objectives include:</p> <ul style="list-style-type: none"> -Online safety education: offering courses and resources for teachers and students on how to navigate the internet safely. -Awareness: increasing awareness of digital risks and good cybersecurity practices. -Community engagement: organizing events and activities that involve schools and families to promote safe internet use.
KnowBe4	English	Teaching materials	Phishing and other attacks	<p>Cybersecurity Activity Kit by KnowBe4 is an interactive set designed to teach children the fundamental skills of online safety through fun and educational activities. It includes games like "Password Zapper" and "Spot the Phish," a coloring book on safety, a video module on cyberbullying, and other creative tools to promote cybersecurity awareness. The main objectives are:</p> <ul style="list-style-type: none"> -Online safety education: Teaching children the basics of internet safety. -Cyberbullying prevention: Providing resources to recognize and address cyberbullying. -Engagement through play: Using game-based activities to make learning fun and engaging.
Learning Corner (EU)	English	Teaching materials	Basics of cyber security	<p>Learning Corner (EU) is an educational platform for students, teachers, and parents to learn and teach topics related to the EU. It offers teaching resources, educational games, activities, and competitions for different age groups, from primary school children to secondary school students. The main objectives are:</p> <ul style="list-style-type: none"> -Educating about EU values and functioning: providing a deep understanding of the European Union, its history, institutions, and policies. -Supporting teachers: offering ready-to-use teaching materials and networking opportunities with other teachers across the EU.

				-Promoting youth participation: encouraging young people to engage in European activities, such as exchange programs and volunteering.
Ludoteca del Registro	Italian	Teaching materials	Ways you can be attacked	<p>The Ludoteca del Registro is an educational initiative promoted by Registro.it and managed by the Institute of Informatics and Telematics of the CNR. The project was launched in 2011 during the Internet Festival in Pisa and is primarily aimed at children aged 6 to 10 years.</p> <p>Main Objectives</p> <p>Digital Education: Raise awareness among young people about the conscious and safe use of the Internet.</p> <p>Online Safety: Teach correct behaviors to protect privacy and manage digital identity.</p> <p>Technological Understanding: Explain basic concepts such as data transmission, protocols, and binary language through playful activities.</p> <p>Activities and Methodologies</p> <p>Games and Workshops: Interactive activities such as group games and mini workshops.</p> <p>Educational Materials: Resources for teachers and families to facilitate digital education.</p> <p>Web App "Internetopoli": An interactive app that guides children through lessons about the Internet.</p>
Parole O_Stili	Italian	Teaching materials	Basics of cyber security	<p>Parole O_Stili is a social initiative aimed at raising awareness against verbal violence. It promotes respectful and civil communication online and offline through its "Manifesto of Non-Hostile Communication," which outlines ten principles to encourage responsible behavior on the internet.</p> <p>Main Objectives</p> <p>Digital Civility: encourage respectful interactions online.</p> <p>Awareness: educate on the impact of words and how they can unite or harm.</p> <p>Responsibility: promote the understanding that virtual interactions have real-life consequences.</p> <p>Activities and Tools</p> <p>Manifesto: a set of principles for non-hostile communication.</p> <p>Educational Resources: materials for schools, companies, and public administration.</p> <p>Events and Workshops: initiatives to spread awareness and educate various sectors.</p>

Proofpoint	English	Teaching materials	Basics of cyber security	<p>The Cybersecurity Activity Book for Kids by Proofpoint is designed to introduce children to cybersecurity in an engaging and entertaining way. The book includes various activities such as:</p> <p>Coloring Pages: customizing avatars and superhero-themed pages.</p> <p>Word Searches: focused on cybersecurity terms.</p> <p>Mazes: teaching children to avoid phishing.</p> <p>Dos and Don'ts: practical tips for staying safe online.</p> <p>Objectives</p> <p>Education: introduce fundamental cybersecurity concepts to children.</p> <p>Engagement: provide fun activities to make learning about cybersecurity enjoyable.</p> <p>Awareness: teach children safe online behaviors early on.</p>
Safer Internet Centre Italy	Italian	Teaching materials	Online Behaviour	<p>Generazioni Connesse – Safer Internet Centre (SIC) Italia is a project co-financed by the European Commission under the Digital Europe program. Coordinated by the Italian Ministry of Education, it involves several key organizations, including the Police, universities, and child protection agencies like Save the Children and Telefono Azzurro.</p> <p>Main Objectives</p> <p>Safety Education: provide information, advice, and support to children, teens, parents, and educators regarding safe internet use.</p> <p>Illegal Content Reporting: facilitate the reporting of illegal online material.</p> <p>Innovative Services: develop high-quality, innovative services to ensure online safety for young users.</p>
Safer Internet Hungary	Hungarian	Teaching materials	all modules are covered	Website of the International Child Rescue Service. The website contains materials (videos, texts, games) for students, teachers, and educators to promote a safer use of the Internet.
Youth Toolkit	English	Teaching materials	all modules are covered	The Humane Tech website focuses on the impact of technology on the younger generation. This site promotes a more conscious and responsible use of technology among young people, parents, and educators, highlighting how it can affect the mental, emotional, and physical well-being of young people.
Apprendre en jouant	French	Awareness and teaching material	Online Behaviour	See Apprendre en jouant Centre pour la Cybersécurité Belgique (belgium.be), line 30
FarexBene	Italian	Awareness and teaching material	Cyber Bulling	Website of the Italian project Safer Internet Centre – Generazioni Connesse. The Safer Internet Centre (SIC) has been set up to provide information, advice and support to children, young people, parents, teachers, and educators who have experiences, including problematic ones, related to the Internet and to facilitate the reporting of illegal material online.

Betternet.be	English	Awareness raising*	Online Behaviour	Website of the Belgian Safer Internet Centre promoting the development of a better internet for all children in Belgium.. The website offers media literacy initiatives for professionals, a helpline for all e-safety related issues and problems and a hotline for child sexual abuse material.
Schools Capture the Flag	English	Competition/game	Basics of cyber security	Website of the annual Irish Cyber-Schools Security Challenge organised by Zero Days Security aiming at presenting the cyber-security industry as an exciting and accessible career pathway to student of all levels and grades.
Cybersafety	Greek	Platform	Online Behaviour	The CYberSafety project aims to create an awareness platform where stakeholders (e.g., schools, governative institutions)) can find information, resources and use tools, but also share experiences, expertise and good practices. The website contains a specifically designed tool for youth, the Youth Group that allows young people to exchange opinions, knowledge and experiences about the use of digital and online technologies.
E-learning portal	Polish	Platform	Basics of cyber security	The website contains e-learning courses for primary and lower secondary school students and teachers on topics related to Cybersecurity, ICT, artificial intelligence and more
Cybertrials	Italian	training and competition	Basics of cyber security	Website of Cybertrials, third edition of the free gaming and training programme for the digital experts of the future, organised by the Cybersecurity National Lab. Cybertrials is designed for involving girls attending upper secondary school. The website contains training and educational materials for students willing to participate in the game.
OlyCyber	Italian	training and competition	Basics of cyber security	Website of OlyCyber, the Italian Cybersecurity Olympiad, organised by the CINI's Cybersecurity National Lab, a competition programme aimed at fostering and encouraging students' approach to cybersecurity issues. The website also contains training and educational materials for students willing to participate in the competition.
Apprendre en jouant	French	Awareness and teaching material	Reporting and Recovering	Website of the Centre for Cybersecurity of Belgium. The website contains educational materials and information covering cybersecurity issues that can be useful for several stakeholder, such as schools, private, public, and governative institutions.

Targalt Internetis	Estonia	Platform, materials, training	all modules are covered	Website realized as outcome of the project Targalt Internetis. The website contains educational materials to promote a smarter Internet use by children and their parents and the prevention of online distribution of child sexual abuse material. The materials is intended for the use of different targetts: children, youth, parents, and teachers.
Keeping children and young people safe online	Poland	Awareness and teaching material	all modules are covered	The biggest conference in Poland on online threats and safety will take place on 24-27 September 2024. Experts from all over Europe will gather to discuss a wide range of issues related to the safety of children and young people online.
Youth Internet Monitor 2024	Austria	Research	Online Behaviour	The Youth Internet Monitor is an initiative of Saferinternet.at and presents current data on the use of social media by young people in Austria. Which social networks are currently popular among young users in Austria? Which networks are most popular among girls? Which are the favourites with boys?
Roadshow "ZIGZAGA na NET"	Portugal	Awareness and teaching material	Online Behaviour	The book was developed with the aim of promoting children's digital literacy and is based on "ZigZaga na Net. Novas aventuras", in turn inspired by the stories of the second season of the ZigZaga podcast.

Repository of initiatives relevant for parents

Name of the CE initiative/project	Language	Type	Mapped to modules	Description
A smart kid's guide to the online world of wonders	English	Game	Basics of cybersecurity	<p>The guide is designed to help children safely and effectively navigate the internet. It provides foundational knowledge about the internet's workings and emphasizes the importance of safe online behavior. The guide teaches children about privacy, the concept of a digital footprint, and how to protect their personal information. Through interactive activities and relatable examples, it encourages critical thinking and the ability to discern between real and fake information online.</p> <p>The guide also introduces basic programming concepts in a fun, accessible way, aiming to spark interest in technology and digital creativity. The aim is to empower children to use the internet as a positive tool for learning and communication while being mindful of potential risks.</p>

Be Internet Awesome	English	Game	Basics of cybersecurity	<p>Be Internet Awesome is a program that teaches kids online safety that emphasizes five key principles:</p> <p>Be Internet Smart: Share with care and communicate responsibly.</p> <p>Be Internet Alert: Identify and avoid fake information.</p> <p>Be Internet Strong: Secure personal information with strong passwords.</p> <p>Be Internet Kind: Promote kindness and counteract bullying.</p> <p>Be Internet Brave: Encourage open communication with trusted adults about online concerns.</p> <p>The initiative provides educational resources for families and educators, including interactive game to make learning engaging and fun.</p>
Save the children	Italian	Awareness	Basics of cybersecurity	<p>Generazioni Connesse, Italy's Safer Internet Centre, is dedicated to promoting safer internet use among children and teenagers. It is co-financed by the European Commission and offers resources for teachers, parents, and students. The platform provides educational tools, advice on digital safety, and guidance on addressing online risks such as cyberbullying, grooming, and exposure to harmful content. It also features a helpline offering confidential support and advice on internet-related issues. The project aims to foster a positive and safe online environment for young people.</p>
Band Runner	English	Game	Online Behaviour	<p>The CEOP Education website for 8-10-year-olds is designed to teach children about online safety through engaging content. It features characters like Alfie, Ellie, and the Popcorn Wizards to make learning fun and relatable. The site offers videos, safety tips, and interactive activities to help children understand the risks of the internet and how to stay safe. Additionally, there are resources for parents and carers to support their children in navigating the digital world safely.</p>

Cyber Chronix	English	Game	Data and Property	Cyber Chronix is an educational game designed for students aged 12 to 15 and older. It aims to teach about data protection and privacy through interactive storytelling and quizzes. The game helps players understand the importance of online privacy and the risks associated with sharing personal information. It encourages critical thinking and responsible online behavior in a fun and engaging way.
Cyber Defense Quiz	English	Game	Ways you can be attacked	The Carnegie Cyber Academy aims to educate children about internet safety and cybersecurity through interactive games, quizzes, and missions. Its objectives include: Teaching foundational cybersecurity knowledge and skills. Promoting safe online behavior and personal information protection. Raising awareness of common cyber threats. Encouraging responsible digital citizenship. Providing engaging and practical learning experiences. Key features include training missions, cyber defense quizzes, detailed faculty pages on cybersecurity topics, and insights into cadet life, all designed to make learning about cybersecurity fun and effective.
CyberLand	English	Game	Basics of cybersecurity	Cyber Games UK is an educational platform offering a variety of interactive games focused on cybersecurity. The games are designed to enhance users understanding and skills in various cyber-related areas, such as code cracking, malware awareness, password security, and network topologies. Developed in collaboration with the National Crime Agency and Cyber Security Challenge UK, these games provide practical and engaging learning experiences. The primary aim is to educate users about cybersecurity, helping them navigate and secure the digital world effectively.

CyberSprinters	English	Game	Stronger Passwords	<p>The CyberSprinters Practitioner Overview from the NCSC provides a detailed educational toolkit for teaching children aged 7-11 about cybersecurity. It includes a variety of interactive activities and games that cover essential cybersecurity topics such as creating strong passwords, protecting personal information, updating devices, and identifying suspicious messages. The guide emphasizes the growing need for cybersecurity awareness among children due to their increasing use of technology. It also offers practical suggestions for educators on how to use the resources effectively in different educational settings, ensuring alignment with the curriculum across the UK. The activities are designed to be engaging and educational, helping children develop vital cybersecurity skills and knowledge in a fun and interactive manner.</p> <p>Additionally, the guide includes FAQs, curriculum mappings, and additional resources such as crosswords and word searches to reinforce learning. The aim is to equip children with the tools and understanding needed to protect themselves online and recognize potential cyber threats.</p>
Hackchallenges	Dutch	Game	Responding to attacks	<p>Hack Challenges NL is an educational platform dedicated to enhancing cybersecurity skills through interactive challenges. Users can participate in various activities, such as hacking simulated accounts on "Vosboek" and competing in "Capture the Flag" (CTF) events. These hands-on challenges are designed to provide practical experience in cybersecurity, helping users to understand and navigate the complexities of digital security. The primary aim of Hack Challenges NL is to educate and improve users' cybersecurity skills by offering engaging and practical learning experiences. This approach helps users develop the knowledge and abilities needed to protect themselves and their data online.</p>
HackShield	English	game	Responding to attacks	<p>HackShield is an educational game aimed at children aged 8 to 12, designed to raise awareness about cybersecurity. In the game, children become "cyber agents," completing various quests and challenges that teach them how to navigate the internet safely. The goal is to empower kids to recognize and avoid cyber threats while also encouraging them to share their newfound knowledge with older generations. This initiative is</p>

				supported by DNS Belgium and is available for free on both computers and mobile devices.
Interland	English	Game	Online Behaviour	<p>Interland is an interactive educational game from Google's Be Internet Awesome program, designed to teach kids critical online safety skills. The game is divided into four unique lands, each addressing different aspects of digital citizenship:</p> <p>Kind Kingdom: Focuses on promoting kindness and combating cyberbullying. Players learn to foster positive interactions and support others online.</p> <p>Reality River: Teaches players to identify and avoid phishing, scams, and other forms of misinformation by making discerning decisions.</p> <p>Mindful Mountain: Encourages thoughtful sharing by demonstrating the impact of sharing information online and the importance of privacy.</p> <p>Tower of Treasure: Emphasizes the importance of creating strong passwords and protecting personal information to safeguard online accounts.</p> <p>These engaging and educational challenges help reinforce safe and responsible online behavior in a fun, game-based format.</p>
The Case of the Cyber Criminal	English	Game	Data and Property	<p>The Case of the Cyber Criminal is an educational game aimed at teaching children about online safety. Players take on the role of a detective to stop a cybercriminal by engaging in interactive challenges. Through these activities, players learn how to protect personal information, recognize phishing attempts, and understand the importance of cybersecurity. The game uses quizzes and scenarios to reinforce lessons on privacy and responsible online behavior, making it a fun and engaging way for kids to learn about internet safety.</p>
Awareness raising and training	Spanish	Internet Segura for Kids	Reporting and Recovering	<p>The INCIBE (Instituto Nacional de Ciberseguridad) website offers resources for children, educators, and families to promote online safety and cybersecurity awareness. It provides educational materials, guides, interactive activities, and advice on handling cyber incidents. The site also features specific sections for real-life cases, FAQs, cybersecurity courses, and campaigns aimed at fostering a safer digital environment for minors.</p>

6.3 Appendix 3: Spoofy lesson plans

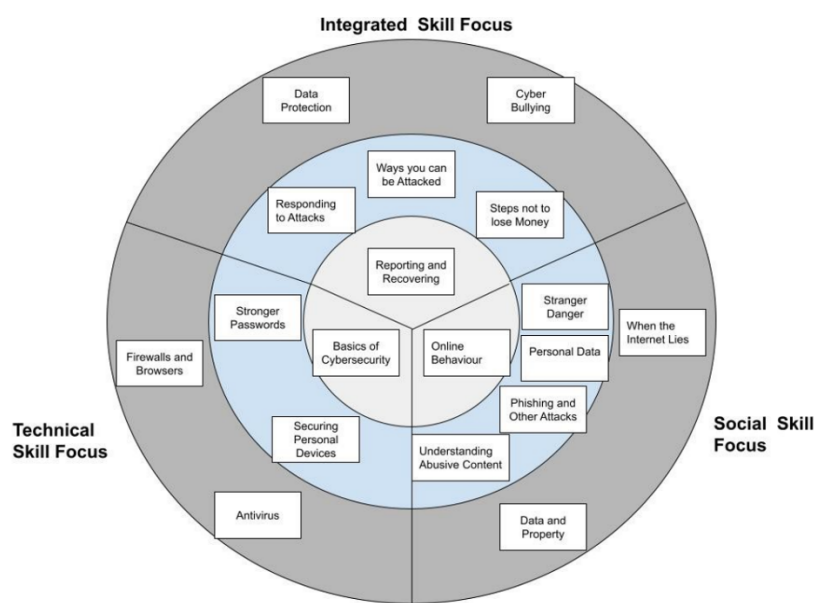
Online Behaviour

Learning Context:

– Ages 8-10

- 10-25 students
- 1 hour
- Location: classroom with projector or screen visible to all students
- Resources:
 - Internet-connected computer for instructor
 - *SPOOFY* game with lesson materials
 - Whiteboard
 - Paper and writing instruments for students

Objectives:








- Social Skill focus
 - o Online behavior
 - Stranger Danger
 - Understanding Abusive Content
- ST - M1:Children will be able to recognise situations where they should contact a trusted adult
- ST - M3:Children will know what action to take in case of cyber-bullying
- ST - M3:Children will know the basics of online bullying;Children should know what action to take in case of cyber-bullying, both for themselves and for others

Lesson plan:

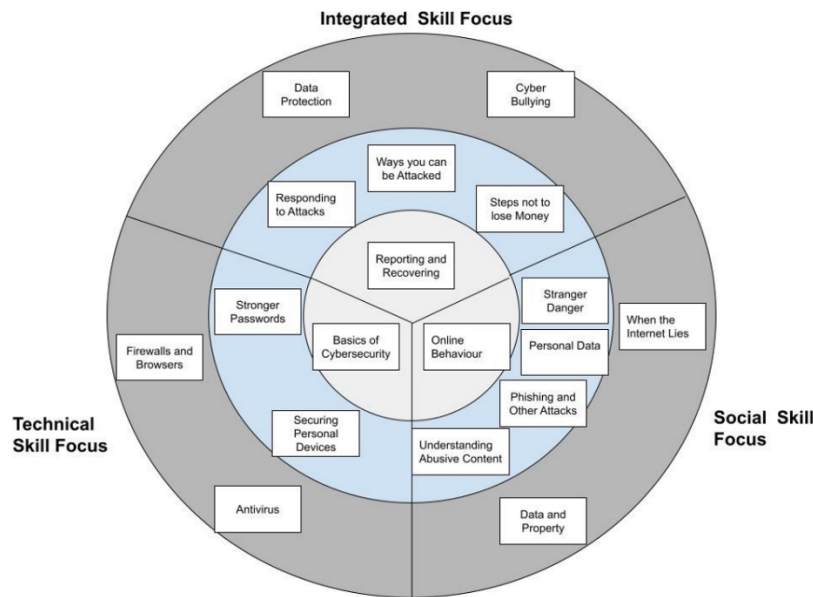
(NB! Many students will be used to watching other people play games online while still feeling like they are a participant. One technique video game streamers often use to include viewers in on-screen activities is to always use the pronoun “we” instead of “I” when making decisions in game. “Where should *we* go next?” is far more inclusive of the audience than asking “Where should *I* go next?” Try using this speech pattern when working through the game together.)

Activity	Time	Details	Learning Goal	Extras
Introduction	3-5 min	Indicate to class that the topic for the day is going to be about proper behavior. Elicit one example of bad behavior to the board. Eg listening to music loudly in public. Introduce vocabulary: etiquette, netiquette	Introduction of the lesson focus	:
Think pair share	10 min	Place the students in pairs and ask them to come up with more examples of bad behaviour online and in real life. Stds write the examples in a list. The teacher draws a T chart on the board with etiquette on	Personalization of the learning	

		one side netiquette on the other. Elicit examples to the board and place them in the correct column or in between for both		
Game introduction	5 min	Teacher "so today we are going to play a game together in class. What examples on the board do you think we will find in the game?" If this is your first time playing <i>SPOOFY</i> with this class, you will want to explain the overarching goal of the game: to get the spaceship running again. You may explain this yourself or play through the short tutorial/explainer with the class. Draw S's attention to screen and navigate to the map icon, and then to the school yard level icon to begin the text.	Placing Game based learning within the context of the topic	Map icon:  Level icon: 
Play game First issue	10 min	 Issue 1: Navigate to the teacher to get an overview of your goal in the school: get all students into the classroom. Navigate into the hallway. Upon entering the hallway, draw attention to the unhappy crowd near the next classroom. Elicit reasons for their unhappiness as well as possible fixes. (NB! Headphones to fix issue are in the room in which you started) (Follow guidance from students as much as possible, but also try to steer the class toward working solutions quickly in order to move on from the text in a timely manner.) Once the problem is solved, elicit whether this was an etiquette issue or a netiquette issue. Also draw attention to the fact that both groups are now smiling. If desired, discuss when/where headphones and speakers are appropriate. (+2-3 minutes)	Online Behavior - Basic etiquette	Note that a number of decorative items can be collected during the course of this game. Allow students to choose who should wear these items as the game progresses. This will encourage students to stay more engaged in the game even though they aren't playing themselves.
Play game Second issue	10 min	Issue 2: Navigate back into the hallway to find the crying child  Elicit reasons why he might be crying. Upon approaching, the answer will become more clear. (He appears to be looking for his bunny) Upon reading the issue, elicit what kind of issue this is: etiquette or netiquette. Allowing students to guide exploration at this point will help the class stay more engaged in the process. No clues can be found inside the school building at this time, so allow students to navigate outside once other options have been exhausted. (This free navigation will present clues for later puzzles to the more attentive students.) If time is short, you may guide navigation in a more direct path toward your goals. Once outside, avoid interacting with other characters quite yet (though students may note them down for later interactions),	Primary goal: Online Behavior - Basic etiquette Reinforcement goals: Understanding Abusive Content - ST - Module 1: Children should be able to recognise situations where they should contact a trusted adult	

		<p>and find the bunny rabbit on the left side of the yard. Pick it up and head back inside to return it to the crying student. Child states that "other players are bullying them on the internet" and they "want to say something really mean to them in return."</p> <p>Upon reading the issue, elicit what kind of issue this is: etiquette or netiquette.</p> <p>Pause the game and elicit feedback from the class. Is this an appropriate response?</p> <ul style="list-style-type: none"> Collect a number of possible responses before clicking to continue <p>When the chat appears, discuss the possible answers and elicit the correct answer from the class.</p>  <p>Before selecting the third (correct) option, elicit reasons as to why the other options are incorrect.</p> <p>Select the third option and discuss the ensuing conversation with the class.</p> <p>The teacher should focus the discussion with guiding questions about how the student would feel in that situation.</p>	ST - Module 3: Children should know what action to take in case of cyber-bullying	
Think Pair Share	10 min	<p>Place students into pairs "Have you ever experienced cyber bullying? Have you ever been a cyber bully? Tell your partner about it."</p> <p>Give the students 5 minutes to discuss while monitoring and providing support.</p> <p>Sharing: Elicit examples of cyberbullying students have experienced in their own lives, whether they were on the receiving end or not.</p> <p>Discuss what they did in those situations and if that was the appropriate response.</p> <p>Discuss what they should do next time.</p> <p>Focus on the concept of getting an adult to help. Have the pairs create a list of "trusted adults"</p> <p>Elicit the list to the board.</p> <p>Ask the students to think about who their trusted adults are in their lives to whom they may turn in situations like the one portrayed in the game.</p>	<p>Primary goal: Online Behavior - Basic etiquette Reinforcement goals: Understanding Abusive Content - ST - Module 1: Children should be able to recognise situations where they should contact a trusted adult ST - Module 3: Children should know what action to take in case of cyber-bullying</p>	
Review	5 min	<p>Teacher: "Today we learned about Etiquette and Netiquette, what is the difference?"</p> <p>"Why is it important to behave online?"</p>	Reinforcing the learning objectives	

Basic of Cyber Security







Learning Context:

- Ages 8-13
- 10-25 students
- 1 hour
- Location: classroom with projector or screen visible to all students
- Resources:
 - Internet-connected computer for instructor
 - *SPOOFY* game with lesson materials
 - Whiteboard
 - Paper and writing instruments for students

Lesson plan:

(NB! Many students will be used to watching other people play games online while still feeling like they are a participant. One technique video game streamers often use to include viewers in on-screen activities is to always use the pronoun “we” instead of “I” when making decisions in game. “Where should *we* go next?” is far more inclusive of the audience than asking “Where should *I* go next?” Try using this speech pattern when working through the game together.)

Activity	Time	Details	Learning Goal	Extras
Intro	5 min	<p>If this is your first time playing <i>SPOOFY</i> with this class, you will want to explain the overarching goal of the game: to get the spaceship running again. You may explain this yourself or play through the short tutorial/explainer with the class.</p> <p>Navigate to the main computer, click on the map icon if necessary, and then click on the beach scene level icon.</p>		<p>Map icon:</p>  <p>Level icon:</p> 

Play game Issue	10 min	 <p>Issue 1: Find the man in a wheelchair and click on his speech bubble to reveal that he has found an unlocked device!</p> <p>Ask students if they've ever found an unlocked device before and what they should do if they do find an unlocked device.</p> <p>NB! The device opens to a personal page which allows us to locate the owner, but you should impress on students that there are other ways of ascertaining who the owner is provided the device does not have the owner's home page on display.</p> <p>Elicit from the class who they think owns the device?</p> <p>After discussing with the class, navigate around the scene until you locate the dog pictured on the device and</p>  <p>its owner standing nearby.</p> <p>She says she's lucky an honest person found her device and asks how to better protect it in the future, and then asks what makes a good password.</p>	Basics of Cybersecurity -	
Discussion	5-7 min	<p>What makes a good password?</p> <p>Elicit ideas from the class about what makes a good password.</p> <p>Elicit reasons you would want a good password (why is the girl lucky an "honest person" found her device?).</p>	Basics of Cybersecurity -	
		<p>Younger Students:</p> <ul style="list-style-type: none"> – Ask students if they know any ways to make a password strong – Discuss why it could be bad for someone to get access to your device 	<p>Older Students:</p> <ul style="list-style-type: none"> – Discuss the things that make a password stronger or weaker – Discuss why these measures are effective – Discuss why it could be bad for someone to get access to your device 	
Activity	15 min	<p>Have students write down a number of ideas for passwords they think would be strong. A list of 10 should do for this activity.</p> <p>Groups students in pairs or small groups and have them take turns playing a version of 20 questions regarding the passwords. (e.g. Does your password have your pet's name? Does your password reference your favorite movie? Etc.)</p> <p>For each question a student answers "yes" to, they must cross out the offending password.</p> <p>If the student is forced to cross out all of their</p>	Basics of Cybersecurity	

		<p>passwords before their peer has asked 20 questions, they lose. If they still have passwords un-crossed, they win. Trade sides and play again.</p> <p>If you have time, you can ask students to take what they've learned, write 10 more passwords, and try the game again (possibly after switching groups).</p> <p>Have the students circle any password that weren't guessed and hand the papers back to the teacher.</p>		
Wrap-up 1	4-7 min	<p>If you played the 20 questions password game earlier, bring out the papers with passwords written on them and ask students if they remember the passwords they wrote down.</p> <p>Impress on students the need to have strong passwords that they can also remember. It's no good to have a strong password you have to write down and look up to use every time you want to access a service.</p> <p>Recall what makes a good password</p> <p>Elicit rules for proper netiquette</p>	Basics of Cybersecurity - Stronger Passwords	
Wrap-up 2	2-3 min	<p>If you didn't play the 20 questions game before, ask students to recall what makes a good password.</p> <p>Elicit rules for proper netiquette</p>	Basics of Cybersecurity - Stronger Passwords	

6.4 Appendix 4: Spoofy instructions for educators

These instructions are meant for educators of different kinds. Here you can find information about the game, overviews of the worlds, additional assignments for using the game in class and other additional information.

Overview of the game



Spoofy is a cybersecurity game with the goal to teach children about cybersecurity threats, behaving online and other issues related to smart devices. The game presents different scenarios, the player can collect cyberpets and do other fun things.

The target group for the game are younger school aged children, and with an adult, even pre-schoolers. The originally open worlds are playable separately and do not need a specific order. The school and birthday worlds are shorter and deal with only topics related to kids. The park and grandma's place are more complicated. Once all four worlds are completed, the cyber machine has been put together and smaller children can play all the worlds again or finish playing. After the

four worlds have been completed, a new fifth world opens up: this one is more complicated and is meant for older children, as it requires the player to definitely be able to read. All of the worlds are playable by all ages when playing with an adult.

General rules for playing and moving around

The player can play five different worlds and move between the spaceship and each of the worlds. The first four worlds open up right away; the fifth opens later on. In the game, the player can play in four different worlds and move between the world and the spaceship. Each world has its own individual assignments: solving cyber problems or collecting items. Solving assignments gives the player "experience," which turns into energy stars. Once the player has accumulated three stars, they can free a pet. The player can then put glasses and hats on the pets.

While walking around, the player can collect different items. They can be on the ground, on the table or given by characters in the game. Some items can be picked up only after certain assignments have been done. Items go into storage and are divided into two: necessary items and wearable items. Wearable items are marked with a top hat, other items should be kept until they are asked for. The player can wear the wearable items themselves or give them to other characters or pets. They can be removed later. Some wearable items turn up later, the game should be played multiple times. Once the cyber machine is assembled, all assignments are reset and can be done again. Each time the assignments are done, the world reset.

Focus of the game

Cyber security is an important topic for everyone, including children. Many have smart devices themselves; computer and internet are also taught in schools. Even though many internet websites presume the users are 12 years old, often children go there earlier. Also, many play various online games, use school forums and other media. So, it is important to explain to children at an early age how to behave on the internet and what are the dangers. Therefore, this game focuses on three following important aspects.

The internet is not separate from real life. Social media posts and general behaviour online influences people in real life as well. Money spent on the internet is real money, words said and posted online have an effect on people, and you can do real harm online. It is part of cyber security to make people understand that children understand the consequences of their actions: a friend gets hurt, unpleasant information spreads, or one ends up as a victim of a crime.

Not everyone online is your friend. Children meet different people online, many of them are old or new friend, but it is also important to teach that there might also be bad people who don't seem like that initially. Therefore, it is important to be careful when accepting friend requests, but it is also important to know in general that there are criminals on the internet. Even though children don't have contact with hacking and cybercrime themselves, it would be good to inform them of these topics.

Ask an adult for help. Children don't often know or dare to ask an adult for help. Maybe the parent does not know how to solve this particular cyber issue, but they can look further. Children experience different things online that they cannot yet explain, therefore it is vital to get help from parents.



The first world – the school

In the school world, the cyber hero has to help children and adults in school and around it. The main focus of the world is how to behave on the internet. There are many items to pick up (headphones, a stuffed rabbit, and wearable items), five smaller and one big assignment. The world is short and does not require a lot of planning.

Overview and goals of the assignments in the school world

- The first three assignments are outside and deal with these three topics: do not post photos of other people on the internet, one must communicate politely online, and strange profiles exist. You can get necessary items from outside to go back into the school.
- The next three assignments are about communicating online, and the cyber hero also finds the parts of the fake profile. One of the messages is to always talk to an adult when there is a problem.
- The last assignment is outside again, solving the fake profile. The main goal is to teach that strange friend requests should not be accepted.

Additional class assignments

The main topic of the school world is communicating on the internet so there is room for multiple discussions that focus on kids' own experience and polite communication.

For example, questions:

1. What is the difference between communicating online and face to face?

2. Can children put up a photo of a teacher?
 - a. It is important to stress here that the person taking the photo is also the owner of the rights, but they should still not upload it without the photo subject's permission.
3. What to do when people get bullied online?
4. What could happen if you accept a friend request from someone you don't know?
 - a. The stranger could bully or harass, could share your personal information, or turn out to be a criminal. As communication is also part of some of the other worlds, one can also focus on one of the two other topics: bullying and fake profiles.
5. Idea for an assignment: children cooperate to write down a plan as to what to do if they see someone get bullied online. Could be a group or pair assignment. This is followed by a discussion with the teacher as to how they themselves should behave online and who to ask for help.
6. Assignment: what could be the ways to determine if the friend request is from a real friend?
 - a. Is the photo familiar? Name familiar?
 - b. Is there a possibility to see mutual friends? Ask them if they really know this person.
 - c. Ask an adult for help!

The second world – the park



In the park world the cyber hero has to mostly help adults, and the focus is on cyber security. There are some collectible items as well, but it is also possible to start with assignments right away. The assignments don't repeat themselves, but the theme of cyber security is almost everywhere.

The world is longer than the first and several assignments need for the cyber hero to talk to multiple people and some assignments require previous ones to be completed.

Overview and goals of the assignments in the park world

- In the beginning, three assignments are open, all in the top part of the game. The goals are privacy-related: what information to share on photos, how to secure a device and one assignment about hacking. The goal of that one is to introduce the topic to the children.
- One of the key assignments is money; the goal is to teach that children cannot spend their parents' money without asking for permission
- One two-part assignment deals with photo sharing again – who is allowed what. The assignment looks at sharing photos when you are the author and, on the photos, and when it is someone else's photo.

Additional class assignments

The main topic of the park is safety, so the topics for discussion are a slightly more grown up.

1. What kind of pictures are suitable for the internet?
 - a. The author of the photo and the people on it have to consent to the upload
 - b. All parties should like the photo
2. Why do we need passwords for our devices? What is a good password like?
 - a. The longer the better. A good password is at least 12 characters long
 - b. Being complicated is also good: letters, numbers, different characters
 - c. Do not share your passwords with others
 - d. Different devices and different accounts have to have different passwords. Why?
3. Shopping online – who is paying?
 - a. Buying things
 - b. Spending money in online games
4. What is privacy?
5. What is hacking? Is it good or bad?
6. An idea for an assignment: children list all their accounts and change them into different passwords. Individual assignment.



The third world – at grandma's

Grandma's world focuses on online scams and criminal activities. The assignments are not very long but are more grown up than in the first two worlds. The topics of the world are maybe a bit complicated for pre-schoolers, but it is still worth a play. The activities in the world take longer, the play through is about 15-20 minutes.

Overview and goals of the assignments in grandma's world

- There are two assignments in the beginning, outside the house. One of them is a constant one and starts with a photo uploaded online. The other assignment is about sharing spam mail.
- There are two assignments inside the house: grandma and grandpa. The former deals with friend requests but grandpa's assignment has two options: one can pick correctly right away and buy the simpler and more expensive ladder, or to pick incorrectly and buy the cheaper one. The first moves the game on but the other opens an additional assignment that deals with computer viruses. The virus assignment also has two options: if one clicks correctly, the man gives the cyber hero the hammer but if one clicks incorrectly, the computer gets infected, and the player has to bring antivirus software from the house and only then the man gives the hammer. It would be useful try all options with the kids.
- The main assignment of the world is to look for the missing goose and egg and finding and handing over the criminal to the police. It is not essential to find the goose to finish the world but gives extra experience. One assignment is to take a photo of the criminal. This is where it would be recommended to discuss with the kids that this is different from real life.

Additional class assignments

The focus of this world is very grown up, but several topics are important to children as well. As there are some topics here that are not covered elsewhere in the game, it is important to cover the most important things during discussions.

1. What possible bad things could happen on the internet?
 - a. Scams, criminals, viruses
2. What to do so that you would be safe online?
 - a. Virus protection, not accepting strangers' friend requests, no pictures with personal info, be careful.
 - b. It is important to stress to the kids that bad things could happen to everyone online, but one has to be careful.
3. What to do when something happens?
 - a. Tell an adult: parent, teacher.
 - b. Introduce the web police.
4. Shopping online
 - a. What and when to buy?
 - b. It should be stressed that adults should be consulted but they should also be critical themselves.
5. Assignment in a computer class: how do I know this computer is safe? Look for virus protection etc.
6. Assignment about online shopping: make a list of things to keep in mind when buying something. Working in groups, pairs
 - a. What page is this? How much does it cost? What is seen on the photos etc.



The Fourth world – birthday party

The birthday world repeats several topics covered before: passwords and device safety, sharing photos online, shopping online. The world is not more complicated or difficult than others, it is more suitable for children, similar to the school world. The world is short and suits also the younger children.

Overview and goals of the assignments in the birthday world

- In the beginning, there are several assignments outside that repeat earlier topics. When one takes the hat to the boy at the gate, it starts an assignment that takes the cyber hero indoors.
- Inside has an assignment about online shopping and this time the focus is on free vs paid items. The goal is to warn children that free does is not always the right way to go.

Additional class assignments

The focus of the world is suitable for all children, discussions can match their level.

1. Why do we need passwords for our devices? What is a good password like?
 - a. The longer the better. A good password is at least 12 characters long.
 - b. Being complicated is also good: letters, numbers, different characters.
 - c. Do not share your passwords with others.
 - d. Different devices and different accounts must have different passwords. Why?
2. Shopping online – free or not free?

- a. Why free things are often not good?
- b. What to keep in mind when shopping?
3. Caring for one's devices.
 - a. How to take care of computers, tablets, and phones?
4. Assignment for myself: what should I do to make sure my devices don't break? A group assignment, an individual assignment
 - a. Assignment about online shopping: make a list of things to keep in mind when buying something. Working in groups, pairs. What page is this? How much does it cost?



The fifth world – The street

The street world opens up once all the other worlds have been played. This is not a compulsory part of the game, because it requires the player to be able to read. The main themes of the world are online scams and false information: bad apps, protecting one's accounts with WiFi and passwords, and copying from the internet.

Overview and goals of the assignments in the street world

- This world offers multiple assignments that deal with fraud on the internet: the characters get fake messages and emails, and they also deal with bad apps in the store.
- One of the most important topics is how to protect oneself: choosing the right WiFi and how to protect one's accounts. All these assignments form part of the main sequence of assignments.
- One assignment deals with copying material from the internet: why one shouldn't do this and how using artificial intelligence is also wrong if it is not allowed by instructions.

Additional class assignments

This world deals with multiple topics already discussed, but there are some new questions that can be elaborated on in class.

What to look for when downloading an app from the internet?

- a. Make sure you have the exact name of the app you are looking for.

- b. The apps should be highly rated, with many reviews and regular updates.
- 2. Which Wi-Fi network to use?
 - a. A secured network is better than an unsecured one.
 - b. It is important to know whose network you are using.
 - c. Is it correct behaviour to go to a café and just ask for the WiFi password? This could be a longer conversation.
- 3. How to recognise a phishing email?
 - a. Who is writing to me? How do I find out? Does it match with the sender's address/phone number I had before?
 - b. Does it tell me that I need to act quickly? If so, these kinds of emails are suspicious.
 - c. What information does the seller want/give? Is anything suspicious?
 - d. How can I check the information that has been sent?
- 4. How can I get my homework done faster?
 - a. Copying from the internet is fraud.
 - b. Even a little bit is wrong.
 - c. Information found online could be fake. You always need to check it yourself.
 - d. Using artificial intelligence is not allowed unless so stated.

Additional assignments to elaborate on the topics

- 5. Assignment: Fix all of your passwords and, if possible, add multifactor authentication.
- 6. Research assignment: What is multifactor authentication and where can I use it?



Important themes in the game

The main goal of Spoofy is to get children thinking about cyber hygiene topics and to give them instructions on how to behave in certain complicated situations. There are multiple different kinds of assignments in the game, but there are also ever-present topics that should be discussed with children both at home and at school.

Sharing photos

When taking and sharing photos, it is important that the kids keep in mind:

1. Whom they are taking photos of and does this person know this;
2. Do not post photos of other people, especially if they are embarrassing.
3. Do not post photos with personal information: name, phone number, address etc. Also do not post information that can attract thieves or nudity.

Another topic to discuss with kids would be to never send anyone photos of themselves wearing skimpy outfits or nudity. Also, not to share these kinds of photos of others, children or adults. It is advisable to not share photos of oneself to strangers in general, always discuss with an adult first. Internet is full of suspicious people who collect photos of children or organise "modelling competition" or send photos of themselves in return. Children should also tell an adult when they get photos from someone.

Friend requests

People get many friend requests; children are no different. Therefore, it is important that they can critically evaluate, which are good requests to accept. Adding the wrong people can give them additional information and access. Therefore, it is important to stress that they should know the person in real life or at least in a game or similar. If the photo and name are familiar but the profile seems strange, they should also be careful and ask for additional information because there are many fake accounts going around.

When they meet an internet friend in real life, they should always consult an adult first, especially if the "friend" asks them not to.

Free things

There are many free things, ads and good offers on the web. Many of them are scams.

1. Free things offer come with viruses or other malware. If it should not be free (like a movie, for example) and someone else is charging for it, the free one is suspicious.
2. „Share this and you might win,” is usually a scam. Even if you get the reward right away, the sharing is still not a good idea.

If something seems like too good to be true, it usually is.

Communicating on the internet

Communicating on the internet is no different from the offline world, one must be polite. But one has to think of additional consequences, children should keep in mind the following:

1. When writing something or uploading a photo on the web, there will always be a trace of it.
2. Words said online have the same impact as things said in real life – insulting someone online is not kinder.
3. You cannot keep track of shared information: you must be careful with what you share and with whom, but you must also keep in mind that others might share your information further.

Passwords and multifactor authentication

All devices and accounts should be password protected. You must remember three things:

1. All passwords must be unique, each account has to have a different password.
2. Passwords must be long and complicated.
 - a. At least 12 digits
 - b. Letters, numbers, and other symbols.
 - c. Don't use easily recognisable things like your name, name of a family member etc.
3. Do not share your passwords with anyone, maybe only your parents.
4. One way to protect one's account is using multifactor authentication. This means that you need something else in addition to a password. For example, a message is sent to your phone, or you need something physical (such as your ID card or Smart ID) or something biological (like your fingerprint). With this additional layer, it is much more difficult to hack into your account.

SCAMS on the internet

The number one internet threat right now is scams. This often means phishing emails and messages or the spreading of false information. It is important to be vigilant at any age and to keep in mind the main rules of cyber hygiene.

1. Always be careful when selecting a WiFi network, downloading apps or reacting to messages.
2. Fake messages can come via email or SMS, through instant messengers or even as phone calls.
3. It is important to always double-check the information through a different channel before reacting.
4. Some common signs of scams are:
 - a. a surprising sender;
 - b. the phone number or address is different from the sender's usual one;
 - c. being prompted to react quickly; and/or
 - d. vagueness in details.
5. Never send money based on just one email or message.
6. Children should always discuss any suspicious messages with their parents, especially when money or data are involved.

Hacking

Hacking is any misuse of computer to get access to someone's computer or system. Hackers can have ethical goals but often they are malicious. Hacking usually requires computer skills and knowledge but there are also those who purchase readymade assets on the internet and use them for their goals. Hacking is usually illegal so hackers are often greeted by police at their doors, and hackers are considered criminals.



The game – where and what?

Here is an overview as to where one should go while playing the game and where to click. Answers to all the questions that children might get when playing and getting stuck or lost.

The spaceship

In the beginning of the game, the player learns all the main activities. The robot gives instructions about using the control panel and collecting and wearing the items. The player can use the control panel to choose the cyber hero, choose the world, change the language and volume, and to later buy cyber-pets. The control panel also has the button for resetting the game if that is what the player wants.

The school world

1. The first class has headphones that need to be taken to the boy in the class next door.
2. The next activity is outside, access through the door bottom of the screen.
3. There is a girl on the right with an assignment about photos.
4. There is a caretaker by the street with an assignment about internet communication. The caretaker will give a key that opens a locked classroom.
5. There is a boy by the swing-set who has an assignment that can be solved inside, and he gives a magnifying glass for it.
6. Next to the boy is also a stuffed rabbit that goes to the boy inside the school.
7. The key opens the locked door on the top of the screen, behind it is the principal with a communication assignment. The principal will give the hero a wearable hat.
8. The magnifying glass assignment is in the classroom to the right. The end result is hair that needs to be taken to the boy outside.
9. The cyber machine part is in the first classroom which finishes the world.
10. There are different wearable glasses, hats and a moustache in the world. Some appear later during the game.

The park

1. There is a lady by the ice cream cart who has an assignment about spending money online. The solution has four steps:
 - a. The girl with the teddy bear by the tables. She will give the player clothes and will wait for a bow.

- b. The clothes should be taken to the woman top of the screen who will give the player money.
 - c. The money goes back to the woman by the ice cream cart, she will give flowers in return.
 - d. The bow comes from solving the tablet owner assignment.
2. There is a man in a wheelchair top of the screen, he has a tablet looking for an owner. The owner can be found using the dog photos on the tablet and she is on the right. She will give the player the bow for the little girl and a hat for a future assignment.
3. Top of the screen also has an assignment on internet photos, this will provide the player with chocolate.
4. On the right side there is a bush and in there is a stop sign that needs to be taken to the construction worker in the bottom right who has a hacking related assignment.
5. The girl with the bear will give an ice cream for the bow.
6. The ice cream and the hat go to the women waiting by the photo booth, they have a photo related assignment and once that has been done, keep an eye on the young man who picks up the women's photo. He is the last assignment, and this provides the player with a decoration.
7. The chocolate, flowers and decoration have to be taken to the mayor who is waiting by the big cake and who will give the missing cyber machine part. This will end the world.
8. The world has hats that can be found and worn.

At grandma's

1. The long assignment of the world starts at the empty coop, where the first part is about a photo, but the player must also find the egg and the goose.
2. After the coop, the player should talk to the police officer who is nearby. The police officer gives the hero a camera and instructions. Before proceeding with that, some other assignments have to be done inside the house and in the yard.
3. In bottom left there is a group of kids who have a spam related assignment, and the solution gives the player a flashlight.
4. Near the kids is a bush and there is the missing goose.
5. In the house is grandma who has an assignment related to friend requests and the reward is a key.
6. The key, camera and flashlight are needed to find the thief. Once all items are collected, the player has to go to the shed, outside and bottom left. Inside is the thief and the player has to take a photo of him and take it to the police officer. There is also a rake in the shed and that is needed later.
7. The police officer gives the player the missing egg and this (with the goose) should be returned to the owner. This step is not necessary for completion of the world.

8. Inside the house is also grandpa, he has an assignment about shopping online, it has two different solutions:
 - a. If the player chooses the expensive and boring ladder, the assignment is done, grandpa gives the ladder to the cyber hero, and they can finish the world.
 - b. If the player chooses the cheaper and shinier ladder, it turns out to be broken and now a hammer is needed.
 - c. The hammer assignment is with the man waiting by the shed, there are again two solutions:
 - i. If the player closes the ads, the hero gets the hammer.
 - ii. If the player clicks on the hammer, the computer gets a virus, and the hero has to get the antivirus.
 - iii. Antivirus is inside the house, with grandpa. After taking that to the man, the hero gets the hammer.
 - d. Grandpa will exchange the hammer for the ladder.
9. The ladder and rake are needed by the tree outside, the cyber machine is up in the tree.
10. The world has different headgear and a face scarf; can be found on the ground and as rewards for assignments.

The birthday

1. The first assignments are outside by the presents and the cake. The cake task is about sharing photos and gives the hero some chocolate.
2. The birthday girl has a password assignment that gives the hero a party hat that should be taken to the kid at the gate. He has an assignment about a lost device and safety. The reward is some popcorn.
3. Inside the house is a boy by the computer who has a downloading assignment. Solving it correctly leads to them needing their mom from the kitchen; the mom wants first the popcorn and her handbag in the bedroom. Mom will give the hero tickets and a pamphlet.
4. The tickets, pamphlet and chocolate go to the man waiting by the fishing game outside, he will give the player a fishing rod in return.
5. The fishing rod should be taken left of the house where the missing cyber machine part is.

Now the first four worlds have been completed and younger children can go and play them again. There is also now a new world open, for children aged 10+.

The street

1. The main focus of the world is opening up the safe, which starts with talking to the police officer. The officer sends the player to speak to the electrician and, after that, to the fire fighter. Once both of their assignments have been solved, the police officer gives the safe to the player.

2. The electrician needs a flyer for their assignment: you can get it from the young person standing next to the hardware store, top left.
3. The safe needs to be fixed and opened. In order to fix it, the player must solve the store owner’s assignment (the hardware store, top left), which grants the player a screwdriver. In order to open the safe, the necessary gemstone is provided by the girl standing near the safe. Both assignments are already open when the game starts.
4. There is an older lady inside the store: she has an assignment dealing with scams and hands out a wearable item.
5. There is a young woman at the bottom of the park who has an assignment dealing with plagiarism and artificial intelligence, and she also hands out a wearable item.
6. Once the safe is open, a code card emerges, and the player can take it back to the spaceship.

Now all the worlds have been completed. All of them can be played again, as the assignments will provide new wearable items.

6.5 Appendix 5: How to use Nabbovaldo in class?

Using “Nabbovaldo e il ricatto dal cyberspazio” in a classroom setting can be an engaging way to teach students about cybersecurity while integrating various educational objectives. These guidelines aim at providing you with some steps and ideas on how to effectively use this game in your class:

Introduction to Cybersecurity: Start with a brief introduction to cybersecurity concepts. Explain the importance of online safety and the basic terms they will encounter in the game, such as ransomware, phishing, and malware.

Game Setup: Ensure that all students have access to the game on their devices. The game is available on both Android and iOS platforms. You might want to play a demo version yourself to familiarise yourself with the gameplay and objectives.

Guided Play Sessions: Organise guided play sessions where students can play the game in a structured environment (work in team-setting). You can have them work through different chapters of the game.

Discussion and Reflection: After each play session, hold a class discussion to reflect on what they learned. Ask questions like:

What cybersecurity threats did Nabbovaldo encounter?

How did he solve the problems?

What can we learn from his actions?

Integration with Curriculum: Integrate the game’s content with your existing curriculum. For example, if you’re teaching math, you can create problems based on the game’s scenarios, such as calculating the probability of a cyber-attack or budgeting for cybersecurity measures.

Project-Based Learning: Encourage students to create their own cybersecurity projects based on what they’ve learned. They could design posters, write essays, or even create their own mini-games or simulations.

By incorporating “Nabbovaldo e il ricatto dal cyberspazio” into your classroom activities, you can make learning about cybersecurity interactive and fun, while also reinforcing important educational objectives.

To sum up : use a game in the class

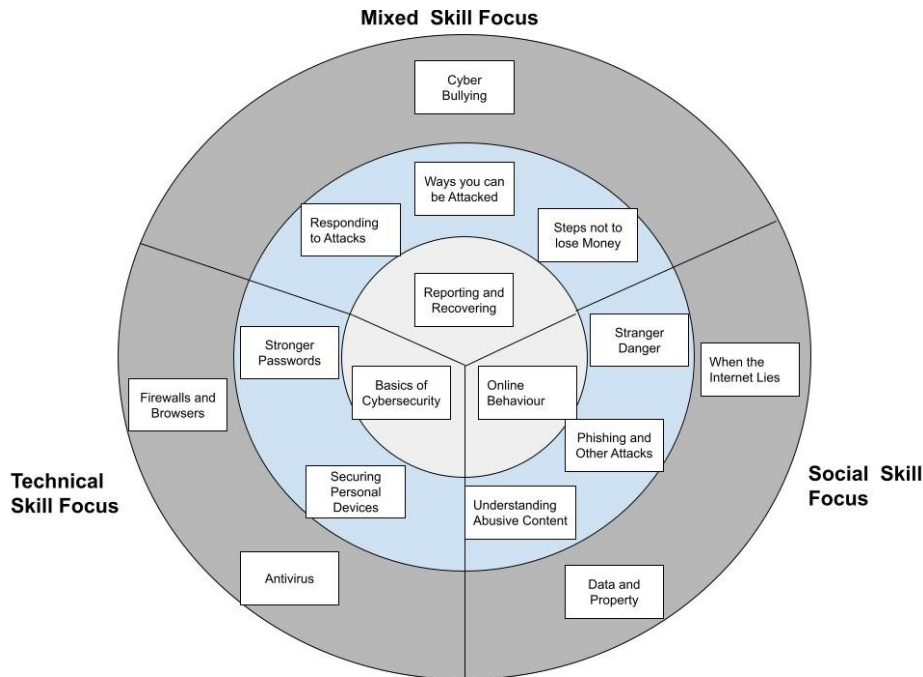
- Do a brief introduction to cybersecurity concepts
- Ensure that all students have access to the game on their devices
- Organise guided play sessions for students
- Discussion and Reflection
- Use SCK curriculum map to help you to integrate the platform to your goals

Nabbovaldo lesson plans

Technical Skill Focus

Securing Personal Devices

Main tool: Video game “Nabbovaldo and the blackmail from cyberspace” and standard group games.



- ☐ Ages 10-13
- ☐ 20-25 students
- ☐ 1 hour
- ☐ Location: classroom with projector or screen visible to all students
- ☐ Resources:
 - Internet-connected computer for instructor
 - *NABBOVALDO* game with lesson materials
 - Whiteboard
 - Paper and writing instruments for students

Objectives:

The game introduces children to strategies for protecting against cyber attackers.

The game introduces children to detecting and implementing actions against basic cyber-attacks.

The game introduces children to understanding basic cyber threats.


The game introduces children to basic prevention technologies.


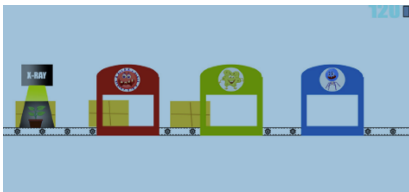
The game introduces children to using software tools to protect digital devices.

The game introduces children to strategies to protect their personal information while surfing the web.

Lesson plan (duration: 60 minutes)

(NB! Many students will be used to watching other people play games online while still feeling like they are a participant. One technique video game streamers often use to include viewers in on-screen activities is to always use the pronoun “we” instead of “I” when making decisions in game. “Where should *we* go next?” is far more inclusive of the audience than asking “Where should *I* go next?” Try using this speech pattern when working through the game together.)

Activity	Time	Details	Learning Goal	Extras
Introduction	3 min	<p>Indicate to class that the topic for the day is going to be about securing personal devices</p> <p>Elicit one example of bad behavior to the board, e.g. a weak pin to access to the own device.</p> <p>Introduce vocabulary: password, credentials, firewall, malware, privacy</p>	Introduction of the lesson focus	
Group game	15 min	<p>Place the students in small groups (4 students) and ask them to come up with a song they like and consider the first letter of the words that compose one sentence of its text in order to create an acronym.</p> <p>The teacher asks each group to share the acronym and the other groups have to guess the song.</p> <p>The teacher explains that each acronym could be the starting point to create a good password (complex but easy to remember).</p>	<ul style="list-style-type: none"> • Password 	
Nabbovaldo - Chapter 2	10 min	<p>Introduce the videogame Nabbovaldo by presenting main characters.</p> <p>Chapter 2 - Social Club Scene (characters: Men in Black). The Teacher introduce the importance of guaranteeing different access to different contents according to the rights of the person that is asking for the target resource. The different rights are presented as different passwords (credentials)</p> 	<ul style="list-style-type: none"> • authentication mechanisms • password 	

Group game	15 min	<p>The teacher introduces basic concepts about cryptography, such as the "Ceaser cipher".</p> <p>Place the students in small groups (4 students) and give them a sentence in plain text that has to be encrypted and then decrypted by using Ceaser cipher (a paper artifact made of two concentric rings).</p> 	<ul style="list-style-type: none"> • Encryption mechanisms 	
Nabbovaldo - Chapter 2	10 min	<p>Meme House: Protection by firewalls/Firewall minigame</p> <p>The mini-game consists of "sterilizing" in the right way a series of packages that proceed along a conveyor belt, some of which contain viruses</p> 	<ul style="list-style-type: none"> • firewall and browsers 	
Review	5 min	<p>Teacher: "Today we learned about Securing Personal Devices, How can we do it?"</p> <p>"Why is it important Securing Personal Devices?"</p> <p>"What can we use in order to protect personal devices?"</p>	<p>Reinforcing the learning objectives</p>	

6.6 Appendix 6: SuperCyberKids lesson plan template

Learning context	<ul style="list-style-type: none"> • Age Group: 10-12 years old • Class Size: 25 students • Duration: 45 minutes • Location: Computer lab with individual workstations for students • Resources: Computers with internet access, projector, educational game software focused on password security (i.e., "Nabbovaldo e il ricatto dal cyberspazio")
Objectives	<ul style="list-style-type: none"> • For School Heads: <ul style="list-style-type: none"> ○ Ensure that the lesson integrates seamlessly into the existing cybersecurity curriculum. ○ Confirm the adequacy of technical resources such as computers and game software. • For Teachers: <ul style="list-style-type: none"> ○ Students should be able to explain safe practices, such as password creation and hashing (Educational Function: Demonstration). ○ Students should be able to create and use strong passwords (Educational Function: Training). ○ Increase motivation and engagement in the subject matter (Educational Function: Motivation).
Topic	<ul style="list-style-type: none"> • Password and Encryption
Lesson Flow	<ul style="list-style-type: none"> • For School Heads <ul style="list-style-type: none"> ○ Preparation: Ensure that the computer lab is available and that the educational game software on password security is installed and functioning on all computers. ○ Support: Provide teachers with a quick guide on how to use the educational game and its features for assessment. ○ Quality Assurance: Schedule a post-lesson review with the teacher to gather feedback on the effectiveness and engagement levels of the lesson. • For Teachers <ul style="list-style-type: none"> ○ Introduction (5 minutes): Briefly introduce the topic and its importance in cybersecurity. Explain the learning objectives. ○ Direct Instruction (10 minutes): Use a presentation to explain the basics of strong passwords, hashing, and encryption. Highlight the dangers of weak passwords. ○ Game-Based Learning Activity (20 minutes): <ul style="list-style-type: none"> ▪ Ask students to log in to their computers and launch the educational game focused on password security. ▪ Students will follow scenarios in the game that require them to create and use strong passwords. ▪ Interaction Pattern: Teacher-Monitored Use. ○ Class Discussion (5 minutes): After the game, facilitate a class discussion about what they learned, what was surprising, and why strong passwords are crucial.

	<ul style="list-style-type: none"> ○ Wrap-up (5 minutes): Summarize key takeaways and inform students that they will be assessed on this topic in a future lesson.
Assessment	<ul style="list-style-type: none"> ● For School Heads: <ul style="list-style-type: none"> ○ Ensure that the game software has built-in analytics to track student progress for formative assessment. ○ Ensure that the teachers have access to external assessment tools like quizzes for summative assessment. ● For Teachers: <ul style="list-style-type: none"> ○ Formative Assessment: Utilize the game’s analytics to monitor which students were able to successfully create strong passwords during the game. ○ Summative Assessment: Administer a quiz in the next class focusing on the concepts taught. Include questions that test the students’ understanding of why strong passwords are essential.