SUPER CYBER KIDS

Super cyber kids reference framework for the integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13) - Guidelines for schools (head teachers and teachers)

SuperCyberKids
Deliverable no. D3.1

Call: ERASMUS-EDU-2022-PI-FORWARD
Type of Action: ERASMUS-LS
Project No. 101087250

Co-funded by the
Erasmus+ Programme
of the European Union

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project ref. number	101087250
Project title	SCK - SuperCyberKids
Document title	Super cyber kids reference framework for the integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13) - Guidelines for schools (head teachers and teachers) (M10)
Document Type	Deliverable
Document version	1.0.1
Previous version(s)	
Planned date of delivery	2023-10-31
Language	English
Dissemination level	Public
Number of pages	6464
Partner(s) responsible	TLU (WP3 Leader; Task 3.1 Leader).
Participating partner(s)	CNR-ITD; UMA; ECSO; CGI.
Author(s)	Peadar Callaghan, TLU; Flavio Manganello, CNR.
With contributions by	Manuel Gentile, CNR; Chiara Fante, CNR; Jeffrey Earp, CNR; Salvatore Perna, CNR; Giuseppe Città, CNR; Catlyn Kirna, CGI, Giorgia Bassi, CNR; Stefania Fabbri, CNR; Ilaria Matteucci, CNR; Anna Vaccarelli, CNR; Arnaud de Vibraye, ECSO; Nicolai Plintz, UMA.
Abstract	This document presents the preparatory phase of the European Project SuperCyberKids, with particular focus on Work Package 3 (WP3). WP3 serves as a cornerstone for achieving the overarching project objective, Ob.1.b, which focuses on delineating an EU reference framework for the seamless incorporation of a game-based learning ecosystem centred on cybersecurity into the curriculum for schoolchildren aged between 8 and 13 years. Situated in conjunction with WP2 in the preparatory phase of the project, WP3 embarks upon the meticulous task of shaping the second step of a comprehensive Learning Programme on cybersecurity for the targeted age group.
Keywords	SuperCyberKids, Learning Framework, ...
DOI	

How to cite	

List of Figures

List of Tables

1 Introduction

This document is the second scientific deliverable of SuperCyberKids (SCK), a project funded by the European Union under Erasmus+ Programme (ERASMUS), Work Programme Part: ERASMUS-2022, Call: Partnerships for Innovation - Forward Looking Projects (ERASMUS-EDU-2022-PI-FORWARD), Action type: ERASMUS-LS ERASMUS Lump Sum Grants; TOPIC ID: ERASMUS-EDU-2022-PI-FORWARD-LOT1, Project n.: 101087250.

The SuperCyberKids project aims to design, create and test an educational ecosystem to provide children aged 8 to 13 and their teachers with learning content on cybersecurity, using a game-based approach to increase motivation and engagement. The educational content will be delivered through a gamification platform, including two games on cybersecurity. The overall project approach is based on the delivery of the two main project results, the educational ecosystem and the related guidelines for implementing it.

To test the results, the project will then carry out four pilots in four different settings (Europe-wide in English, and in local languages in Italy, Estonia, Germany). This will lead to develop a Handbook of good practices on Cybersecurity Education in schools for children aged 8-13, including recommendations for researchers, school heads and teachers, parents, game and instructional designers, as well as Recommendations targeting relevant policy makers, regulatory bodies and institutions in Cybersecurity Education.

Within the project, the above-mentioned activities are structured in Work Packages (WPs), namely:

- WP1. Project management and coordination.
- WP2. Definition of the SuperCyberKids Learning Framework (SCKLF).
- WP3. Integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13).
- WP4: Definition of game-based high-quality educational content for Cybersecurity Education.
- WP5. Creation of toolkit and content to enact Cybersecurity Education in classrooms.
- WP6. Implementation of pilot use cases in schools.
- WP7. Evaluation and Quality Assurance.
- WP8. Dissemination, Exploitation, Scaling-up and Sustainability of project results.

1.1 WP3 - Integration of the game-based learning ecosystem on cybersecurity into curriculum for schoolchildren (aged 8-13)

This technical report presents the preparatory phase of the European Project SuperCyberKids, with particular focus on Work Package 3 (WP3). WP3 serves as a cornerstone for achieving the overarching project objective, Ob.1.b, which focuses on delineating an EU reference framework for the seamless incorporation of a game-based learning ecosystem centred on cybersecurity into the curriculum for schoolchildren aged between 8 and 13 years. Situated in conjunction with WP2 in the preparatory phase of the project, WP3 embarks upon the meticulous task of shaping the second step of a comprehensive Learning Programme on cybersecurity for the targeted age group.

1.1.1 Objectives and Scope

Commencing with a rigorous analysis of educational objectives, content variables, assessment metrics (indicators), and requisites for the assimilation of existing content, WP3 aspires to construct an EU-level reference framework. The EU Reference Framework is a comprehensive, multi-dimensional structure designed to standardize, guide, and enhance the quality of Cybersecurity Education across EU member states, specifically targeting schoolchildren aged 8-13. This framework aims to navigate the incorporation of game-based educational content on cybersecurity into formal educational curricula. It aims to create a coherent and effective educational approach that is pedagogically sound, ethically responsible, and legally compliant. The SCK Learning Framework (SCKLF) formulated within WP2 serves as a pivotal reference for demarcating both learning objectives and assessment criteria.

1.1.2 Methodology and Implementation

WP3 is structured into three distinct but interrelated tasks, each targeting a different facet of curriculum integration:

1.1.2.1 T3.1: Definition of the EU Reference Framework

Spanning from Month 5 to Month 10, Task T3.1 directs its attention towards the development of an EU reference framework that integrates multiple educational dimensions, namely objectives, content, and assessment metrics. Special attention is devoted to the identification of efficacious methods for incorporating the game-based learning ecosystem into formal curricular activities. This task culminates in the delivery of a specific deliverable, designated D3.1, in Month 10, which serves as an initial version of the guidelines for the integration process. **D3.1 is this document.**

1.1.2.2 T3.2: Tools and Guides for Localization

Operating between Month 8 and Month 12, Task T3.2 concentrates on the provision of methodologies and tools to facilitate the localization of the reference framework into national curricula, accentuating the deployment of high-quality game-based educational content. An internal report, noted as R3.2.1, encapsulates the initial guidelines for this localization process and marks the conclusion of the preparatory phase in Month 12.

1.1.2.3 T3.3: Localized Design for Pilot Cases

Occupying the time frame from Month 13 to Month 16, Task T3.3 focuses on the design of localized pilot use cases that instantiate the principles of the reference framework in specific national contexts. This task results in an internal report denoted as R3.3.1, to be released in Month 16.

1.2 Monitoring and Evaluation

WP3 activities will be scrutinized in the E2-WP3 meeting, scheduled in Month 13, to validate the activities conducted in the preparatory phase and to inaugurate the implementation phase, specifically targeting WP4, WP5, and WP6. This meeting is planned to be face-to-face in Estonia.

In summary, WP3 functions not only as a scaffold for the construction of an EU reference framework but also as a linchpin that connects preparatory work with actual implementation, thereby ensuring a cohesive and effective approach to Cybersecurity Education for schoolchildren across Europe.

2 EU Reference Framework for Game-Based Cybersecurity Education: Rationale and Definition

2.1 The necessity of a unified EU Reference Framework for the integration of Game-Based Learning on Cybersecurity into school curricula

The advent of digital technology has permeated various aspects of society, making cybersecurity an imperative area of concern. This significance extends to the education sector, where the integration of cybersecurity awareness and skills is increasingly vital. However, the introduction of Cybersecurity Education for schoolchildren aged 8-13 presents a complex challenge, warranting the development of a standardized European Union (EU) reference framework. The SCK framework aims to integrate a game-based learning ecosystem on cybersecurity into the existing curricula, coupled with explicit Guidelines for schools, including head teachers and teachers.

The necessity for such a framework is manifold:

- **Consistency Across Member States**. A unified EU framework ensures a consistent approach towards Cybersecurity Education across member states. This consistency is paramount for safeguarding the digital infrastructure at both national and continental levels.
- **Pedagogical Efficacy**. The inclusion of game-based learning methods, substantiated by research in educational technologies, holds the promise of increased engagement and effective skill transfer. However, the implementation must be pedagogically sound, making Guidelines indispensable for educators.
- **Self-regulated Learning**. A framework that integrates self-regulated learning strategies allows students to gain not just knowledge but also the skills to manage their own learning journey. This facet is crucial given the ever-evolving nature of cybersecurity threats.
- **Ethical and Legal Considerations**. Given the sensitive nature of cybersecurity, ethical and legal considerations are paramount. A standardized framework will delineate the boundaries of what can be ethically taught and practiced, safeguarding against potential misuse of information.
- **Quality Assurance**. A framework with accompanying guidelines provides a mechanism for quality assurance, ensuring that the intended learning outcomes align with the set educational objectives and standards.
- **Facilitation of Teacher Training**. The provision of Guidelines for schools' aids in the professional development of teachers and head teachers, equipping them with the requisite tools to effectively teach and integrate cybersecurity into the curriculum.

2.1.1 Consistency across Member States

The notion of a unified European Union (EU) framework for Cybersecurity Education addresses a critical need for standardization and consistency across member states. Such uniformity ensures that the approaches, curricula, and competencies developed are congruent, thereby facilitating a cohesive cybersecurity strategy at both national and continental scales. This consistency is not merely a matter of administrative convenience; it is vital for the robust safeguarding of digital infrastructure.

From an educational perspective, a harmonized approach allows for the sharing of best practices, streamlining of resources, and development of common benchmarks for student and professional assessments in cybersecurity. It mitigates the risks associated with fragmented educational systems, where gaps in one member state's cybersecurity preparation could potentially be exploited as a point of vulnerability for the entire EU digital network.

Additionally, given the interconnectedness of digital infrastructures, a singular lapse in cybersecurity readiness in one member state could propagate rapidly across borders, affecting both national and continental security postures. Hence, consistency in educational frameworks could act as a first line of defence, equipping future professionals uniformly with the essential skills and knowledge.

However, while standardization offers numerous advantages, it is important to recognize its limitations. It might stifle innovation or fail to account for unique national contexts and requirements. Therefore, any unified framework should be designed with enough flexibility to allow member states to tailor their Cybersecurity Education programs to meet specific domestic needs, without compromising the overall integrity and effectiveness of the continental approach.

In conclusion, the establishment of a unified EU framework for Cybersecurity Education serves as an invaluable mechanism for ensuring that member states adopt a consistent approach. Such an approach is instrumental in safeguarding digital infrastructure at multiple levels of governance, although it must be implemented with a consideration for the unique needs and circumstances of individual member states.

2.1.2 Pedagogical efficacy

The integration of game-based learning methods into educational contexts has garnered increasing attention, primarily due to its potential for enhancing student engagement and facilitating effective skill transfer. Research in the field of educational technologies corroborates the efficacy of these methods, positing that well-designed game-based learning experiences can lead to superior educational outcomes compared to traditional instructional approaches.

Nonetheless, the effectiveness of game-based learning is contingent upon pedagogically sound implementation. This notion emphasizes that the introduction of game elements into an educational setting should not be arbitrary, but instead be grounded in solid pedagogical frameworks and principles. This necessitates the development of comprehensive guidelines for educators, which can serve as an essential tool in the planning, execution, and assessment stages of game-based educational interventions.

Such guidelines could encompass a range of considerations, from alignment with curricular objectives to the integration of scaffolding techniques and formative assessments. They may also provide insights into balancing the elements of play and educational content to ensure that the game serves its primary pedagogical function, rather than diverting focus towards solely entertainment-oriented goals. These guidelines should be both specific enough to provide actionable advice and flexible enough to accommodate variations in educational settings, student populations, and subject matter.

However, it is crucial to acknowledge that while guidelines can significantly aid the process, they are not a panacea. Educators should exercise their professional judgment in adapting these recommendations to their unique teaching contexts. Moreover, ongoing assessment and revision of the guidelines themselves are imperative, given the rapidly evolving landscape of educational technologies and pedagogical research.

In summary, the promise of game-based learning methods in enhancing engagement and skill transfer is supported by extant research in educational technologies. However, the crux of its success lies in its pedagogically sound implementation, making the formulation of robust guidelines indispensable for educators. These guidelines should be considered as dynamic tools, subject to ongoing refinement to meet the demands of an ever-changing educational landscape.

2.1.3 Self-regulated Learning

The integration of self-regulated learning strategies into educational frameworks, particularly in the context of cybersecurity, offers dual advantages: not only does it facilitate the acquisition of domain-specific knowledge, but it also equips students with the metacognitive skills required to manage their own learning trajectories. Given the dynamic and ever-evolving landscape of cybersecurity threats, this latter aspect is of paramount importance for long-term professional efficacy.

A framework that incorporates self-regulated learning encourages students to engage in planning, monitoring, and evaluating their learning processes. These metacognitive activities empower students to adapt their learning strategies in real-time, optimizing for performance and efficiency. This adaptability is particularly vital in Cybersecurity Education, where static knowledge is often rendered obsolete by the rapid advancements in technology and the changing tactics of malicious actors.

Furthermore, the practice of self-regulated learning aligns well with the inherent challenges posed by cybersecurity, a domain characterized by its complex, problem-solving nature. As individuals encounter novel scenarios that require immediate, effective solutions, the ability to self-regulate learning becomes an invaluable asset. It allows for quick integration of new information, reflection on its applicability, and adjustment of tactics to effectively mitigate threats.

However, while the advantages of integrating self-regulated learning into Cybersecurity Education are compelling, it is important to consider potential challenges. The effectiveness of such a framework may vary based on students' prior experience with self-regulation, requiring educators to offer varying levels of scaffolding and support. Moreover, the success of this approach hinges on its thoughtful implementation, necessitating that educators receive adequate training in both self-regulated learning methodologies and the nuances of cybersecurity.

In conclusion, a framework that merges self-regulated learning strategies with Cybersecurity Education offers a robust model for preparing students to navigate the complex, ever-changing landscape of cybersecurity threats. While the approach presents several advantages, including adaptability and long-term professional efficacy, its implementation requires careful planning and ongoing support to address its inherent challenges. Therefore, its adoption should be considered a nuanced strategy rather than a straightforward solution.

2.1.4 Ethical and legal considerations

In the realm of Cybersecurity Education, ethical and legal considerations take on a heightened significance owing to the sensitive nature of the subject matter. Cybersecurity skills possess a dual-use character; they can be employed for both defensive and offensive purposes. Therefore, a standardized framework that clearly delineates the ethical and legal boundaries of what can be taught and practiced becomes imperative for mitigating the risk of misuse of acquired skills and information.

A well-defined framework would offer a standardized set of guidelines and norms, ensuring that educational institutions, instructors, and learners are aligned in their understanding and approach towards ethical conduct. For instance, it could specify the types of penetration testing or intrusion techniques that can be ethically demonstrated or practiced within an academic context. This framework could also outline the requirements for informed consent when engaging in any form of cybersecurity research or practice that involves third-party data or systems.

Moreover, such a framework could incorporate existing legal statutes, such as data protection laws, into the curriculum, thus ensuring that students are not merely technically proficient but also ethically informed and legally compliant. This can enhance the credibility and trustworthiness of cybersecurity professionals, which is of crucial importance given their role in safeguarding sensitive data and critical infrastructure.

However, it is important to recognize that a standardized framework is not without its challenges. Given the dynamic and transnational nature of cybersecurity threats, ethical and legal norms may differ between jurisdictions, potentially complicating the applicability of a standardized framework. Moreover, the framework will need to be agile to adapt to emerging ethical quandaries presented by new technologies and tactics.

In summary, the incorporation of ethical and legal considerations into a standardized Cybersecurity Education framework is not only advisable but paramount. Such a framework serves as a bulwark against the potential misuse of highly specialized knowledge and skills, while also instilling a sense of ethical responsibility and legal compliance among future cybersecurity professionals. Despite its challenges, the benefits conferred by this integrative approach outweigh the complexities involved, making it an indispensable component of comprehensive Cybersecurity Education.

2.1.5 Quality Assurance

The establishment of a framework complemented by guidelines serves as a pivotal mechanism for quality assurance in educational contexts. This approach ensures that the intended learning outcomes are not only clearly articulated but also systematically aligned with predefined educational objectives and standards. Such alignment is indispensable for fostering a cohesive and effective learning environment, wherein the educational efforts are intentionally directed towards achieving specific competencies and skills.

In practical terms, a framework with accompanying guidelines provides educators with a roadmap for curriculum design, instructional methods, and assessment strategies. By adhering to this framework, educators can be more confident that their instructional practices are in line with the set objectives, thereby maximizing the likelihood of achieving the intended learning outcomes. Additionally, it offers a baseline for external evaluations, such as accreditation processes, ensuring that the educational program meets or exceeds the standards required by authoritative bodies.

Quality assurance, facilitated by a comprehensive framework, also benefits learners. It assures them that the education they are receiving is grounded in best practices and is geared towards meeting explicit objectives that have been vetted for their relevance and applicability. This assurance can enhance student motivation and engagement, as they can more clearly see the value and purpose of their educational journey.

However, it is crucial to acknowledge that while a framework provides a structure for quality assurance, its effectiveness is contingent on its implementation fidelity. Thus, continuous monitoring and evaluation are required to ensure that the guidelines are being adhered to and that they remain relevant in light of emerging educational research and industry demands. Furthermore, a balance must be struck to ensure that the framework allows for enough flexibility to accommodate unique educational contexts and learner needs.

In summary, the integration of a framework with guidelines is an essential strategy for ensuring quality assurance in education. It serves to align the intended learning outcomes with set educational objectives and standards, providing a reliable mechanism for both internal and external evaluations of educational quality. While the framework is a powerful tool for achieving these ends, its success ultimately depends on its faithful implementation and ongoing adaptation to meet evolving standards and needs.

2.1.6 Facilitation of Teacher Training

The provision of guidelines for educational institutions serves a dual function in the professional development of teachers and head teachers, particularly in the specialized area of Cybersecurity Education. Firstly, these guidelines act as a scaffold upon which educators can build their teaching strategies, ensuring that their instructional practices are grounded in validated pedagogical approaches and domain-specific best practices. Secondly, the guidelines facilitate the systematic integration of cybersecurity topics into the existing curriculum, thereby aligning educational efforts with the evolving demands of the field.

From a teacher training perspective, guidelines offer a structured pathway for continuous professional development. They can be incorporated into training modules that focus on a variety of aspects, ranging from pedagogical approaches suitable for Cybersecurity Education to ethical considerations and legal compliances. This enables educators to acquire not just the technical acumen required to teach cybersecurity concepts, but also the pedagogical skills to deliver this content in an effective and engaging manner.

For head teachers or educational leaders, these guidelines provide a blueprint for curriculum development and resource allocation. They assist in identifying key areas where investment is needed—be it in the form of specialized software, hardware, or additional teaching staff with expertise in cybersecurity. Such informed decision-making is instrumental in ensuring the efficacy and relevance of the educational program.

However, it is important to acknowledge that while guidelines are a valuable resource, they are not a one-size-fits-all solution. Educational institutions differ in their capacities, student demographics, and existing curricular structures. Consequently, the successful implementation of guidelines requires their contextualization to the specific needs and constraints of each institution. Additionally, for guidelines to remain effective, they should be subject to periodic review and updates to reflect advances in cybersecurity practices and pedagogical research.

In conclusion, the provision of guidelines for schools significantly aids in the professional development of teachers and head teachers, particularly in the nuanced field of Cybersecurity Education. These guidelines serve as foundational tools for the effective teaching and seamless integration of cybersecurity into the curriculum. However, their successful application necessitates both contextual adaptation and ongoing revision to meet the evolving requirements of the field and the educational landscape.

2.2 Defining the EU Reference Framework for Integrating Game-Based Learning on Cybersecurity into School Curricula: Scope and Objectives

In the scope of this project, the term "EU Reference Framework" signifies a standardized set of guidelines, protocols, and benchmarks established at the European Union level for the integration of game-based learning ecosystems focused on cybersecurity into the curricula for schoolchildren aged 8-13. This framework serves multiple key functions:

2.2.1 Normative guidelines

The EU Reference Framework offers a normative outline that stipulates the essential elements and quality standards that educational institutions across member states should adhere to. This ensures a harmonized approach to Cybersecurity Education. More specifically, the concept of a "normative outline" within the EU Reference Framework refers to a prescriptive set of guidelines and parameters designed to govern the integration of game-based learning on cybersecurity in educational settings. These guidelines are not mere suggestions; rather, they function as authoritative directives that educational institutions are expected to comply with.

The framework identifies the core components integral to Cybersecurity Education. These may include key topics like data protection, network security, and ethical hacking, among others. The aim is to establish a foundational body of knowledge that is deemed essential for schoolchildren aged 8-13.

Beyond the content, the framework also sets quality standards to ensure the educational experience is both effective and equitable. These standards could be related to teacher qualifications, pedagogical approaches, and assessment methods. For instance, the framework may specify that educators involved in this program must undergo specialized training in both cybersecurity and game-based learning methodologies.

One of the principal objectives of having such a framework at the EU level is to create a unified educational strategy across member states. This is particularly important in the context of the digital single market and the transnational nature of cybersecurity threats. A harmonized approach ensures that all students, regardless of their country of residence within the EU, receive a comparable and high-quality education in cybersecurity.

The normative outline carries policy implications, mandating changes at institutional and possibly legislative levels to accommodate the framework's guidelines. This could mean the revision of current curricula, investment in teacher training programs, and the establishment of oversight bodies to ensure compliance and quality assurance.

In summary, the normative outline in the EU Reference Framework serves as a regulatory blueprint, aiming to ensure uniformity, high quality, and comprehensive coverage in the teaching of cybersecurity across EU educational institutions. The intent is to elevate Cybersecurity Education to a standard that is both rigorous and universally applicable within the EU.

2.2.2 Curriculum integration

The framework provides directives for integrating cybersecurity topics into existing curricula. It delineates the scope, sequence, and depth of content that should be imparted at various educational levels, particularly focusing on the 8-13 age group. The integration of cybersecurity topics into existing school curricula is a nuanced endeavour that requires careful planning and strategic implementation. Within this context, the EU Reference Framework serves as a guiding document that provides specific directives for this integration.

The framework outlines the range of topics that are deemed critical for Cybersecurity Education. These may encompass areas such as data privacy, malware threats, password security, and ethical considerations. By providing a well-defined scope, the framework ensures that essential facets of cybersecurity are covered, thereby fostering a comprehensive educational experience.

The framework offers a logically sequenced roadmap for the introduction and development of these topics. It stipulates the order in which topics should be introduced, building from foundational to more complex concepts. This sequencing is designed to align with the cognitive and developmental stages of schoolchildren in the 8-13 age group, ensuring that the content is age-appropriate and progressively challenging.

In addition to the scope and sequence, the framework also defines the depth to which each topic should be explored. Depth here refers to the complexity and granularity of the subject matter. For instance, while younger students might learn about the importance of secure passwords, older students may delve into the specifics of encryption techniques.

While the framework is designed to be universally applicable across the EU, it acknowledges the importance of adaptability to various educational contexts and levels. The focus on the 8-13 age group implies a specialized approach, recognizing that this age bracket has unique educational needs. The guidelines would specify how the content can be adapted for children at different stages within this range, with a balance of theoretical knowledge and practical application.

Furthermore, the framework is constructed to synergize with existing educational curricula, allowing for seamless integration rather than imposing an additional, isolated subject. It may suggest interdisciplinary approaches where cybersecurity concepts are integrated into subjects like social studies, science, or mathematics, thereby enhancing the contextual relevance of Cybersecurity Education.

In summary, the framework's directives on the integration of cybersecurity topics into existing curricula are meticulously designed to be comprehensive yet adaptable. They aim to ensure that students within the EU, particularly those aged 8-13, receive a thorough, age-appropriate, and sequentially organized education in cybersecurity.

2.2.3 Pedagogical approaches

While focusing on game-based learning ecosystems, the framework also offers a pedagogical model that aligns with contemporary educational theories. It advocates for methods that not only engage but also effectively facilitate the transfer of cybersecurity skills and awareness. The EU Reference Framework goes beyond merely endorsing game-based learning as a delivery mechanism for Cybersecurity Education; it also aligns this approach with a pedagogical model informed by contemporary educational theories. This alignment serves to substantiate the efficacy of the game-based learning ecosystems within a broader educational context.

The framework draws on well-established educational theories such as constructivism, situated learning, and cognitive load theory. It recognizes that learning is most effective when students are actively engaged in the process, constructing knowledge through interaction and problem-solving. Game-based learning serves as an ideal platform for such active learning, as it naturally incorporates elements of challenge, competition, and reward.

Game-based learning ecosystems are designed to engage students on multiple levels—cognitive, emotional, and social. The framework's pedagogical model ensures that these elements of engagement are not only present but also balanced to maximize learning outcomes. For example, the emotional engagement achieved through game mechanics like scoring and levelling up is leveraged to heighten cognitive engagement with cybersecurity concepts.

One of the critical aspects addressed by the framework's pedagogical model is the effective transfer of skills and awareness from the game-based environment to real-world contexts. It employs methods such as scaffolding and contextualization to ensure that the skills acquired within the game are not isolated instances of knowledge but can be applied in practical, real-world cybersecurity scenarios.

The framework also incorporates formative assessment methods that align with its pedagogical model. These could involve in-game analytics to track performance and identify areas for improvement or the use of post-game debriefing sessions to facilitate reflection and metacognition.

While the focus is on student-centred, game-based learning, the framework also outlines the role of teachers as facilitators in this learning ecosystem. This role is crucial for ensuring that the game-based activities are aligned with the educational objectives and for providing additional context or clarification when needed.

In essence, the EU Reference Framework's emphasis on a pedagogically sound model seeks to ensure that the game-based learning ecosystems are not merely engaging but are also academically rigorous and effective in transferring cybersecurity skills and awareness. The framework thus serves as a nexus between innovative educational technology and time-honoured educational theory.

2.2.4 Assessment metrics

It incorporates evaluation metrics to gauge the efficacy of the teaching and learning processes. These metrics are designed to assess both the acquisition of knowledge and the development of relevant skills in the field of cybersecurity. Evaluation is a critical component in the educational landscape, serving as the basis for measuring the success of teaching and learning endeavours. Within the context of the EU Reference Framework, the inclusion of evaluation metrics adds a layer of accountability and empirical rigor, specifically tailored to assess the nuances of Cybersecurity Education delivered through game-based learning ecosystems.

The framework incorporates a variety of metrics that go beyond traditional assessment methods like written tests or quizzes. These may include:

- In-Game Analytics: Metrics such as completion rates, scores, and decision-making patterns within the game provide real-time data on student performance.
- Skill-based Assessments: Practical exercises or simulations that require students to employ cybersecurity skills in controlled but realistic scenarios.
- Metacognitive Assessments: Tools to evaluate students' awareness of their own learning processes, such as self-report surveys on perceived competency or learning strategy effectiveness.

The framework's evaluation metrics are designed to assess two major educational outcomes:

- Knowledge Acquisition: Metrics evaluate the extent to which students have grasped the theoretical underpinnings of cybersecurity, such as understanding key terms, concepts, and principles.
- Skill Development: The metrics also measure the practical skills that students have developed. These skills could range from basic abilities like setting up secure passwords to more advanced tasks like identifying security vulnerabilities in a network.

The framework likely recommends both formative and summative evaluations. Formative evaluations occur during the learning process and are aimed at identifying areas for improvement, thereby informing instructional adjustments. Summative evaluations are conducted at the end of a learning period to gauge overall achievement and effectiveness.

Importantly, the evaluation metrics are aligned with the educational objectives laid out in the framework. This ensures that what is being measured accurately reflects the intended learning outcomes, thereby validating the efficacy of the teaching and learning processes.

The framework may also propose feedback mechanisms that utilize these metrics to refine the game-based learning ecosystems continually. This could involve iterative cycles where evaluation results are analysed to make data-driven enhancements to both content and pedagogy.

In summary, the evaluation metrics within the EU Reference Framework serve as a robust toolset for assessing the multifaceted outcomes of Cybersecurity Education. By focusing on both knowledge acquisition and skill development, these metrics offer a comprehensive view of educational efficacy, thereby providing valuable insights for continuous improvement.

2.2.5 Ethical and legal compliance

The framework establishes ethical and legal guidelines for Cybersecurity Education. This is particularly crucial given the sensitive and potentially dangerous nature of the subject matter. The incorporation of ethical and legal guidelines within the EU Reference Framework serves as a pivotal safeguard, given the dual-use nature of cybersecurity knowledge—that is, its potential for both protective and malicious applications. Such guidelines function as essential boundaries, ensuring that the Cybersecurity Education provided does not inadvertently foster unethical or illegal activities.

The framework outlines a code of ethics that teachers and students are expected to adhere to. This may include guidelines on:

- Responsible Disclosure: Teaching students how to responsibly report security vulnerabilities rather than exploiting them.
- Privacy: Educating students on the ethical implications of privacy invasion and unauthorized data access.
- Integrity: Imparting the importance of honesty in reporting and documenting cybersecurity issues.
- Inclusivity: Ensuring that Cybersecurity Education is accessible to all students, irrespective of their socio-economic or cultural background, to avoid creating a digital divide.

The framework also lays out legal parameters that are aligned with existing EU laws and regulations, such as the General Data Protection Regulation (GDPR). This can include:

- Data Handling: Guidelines on how personal and sensitive data should be treated in educational settings.
- Intellectual Property: Rules concerning the use and distribution of software or digital content in the learning environment.
- Consent: Requirements for obtaining informed consent when conducting cybersecurity exercises that involve student participation or data collection.

Given the potentially sensitive nature of cybersecurity exercises (e.g., penetration testing), the framework may require that schools conduct risk assessments to identify and mitigate ethical and legal risks. Such assessments would ensure that educational activities do not inadvertently harm individuals or systems.

Recognizing that the effective implementation of ethical and legal guidelines is contingent on knowledgeable educators, the framework may include provisions for teacher training in this area. It may also establish mechanisms for accountability, where compliance with ethical and legal guidelines is regularly reviewed and audited.

Adherence to ethical and legal guidelines is not only a matter of compliance but also crucial for building public trust. Parents, guardians, and the broader community need to be assured that the Cybersecurity Education their children are receiving is both safe and responsible.

In summary, the ethical and legal guidelines within the EU Reference Framework serve as a foundational layer, ensuring that Cybersecurity Education is conducted within a framework of social responsibility and legal compliance. The sensitive and potent nature of cybersecurity knowledge makes these guidelines not just advisable but indispensable for the integrity and credibility of educational programs.

2.2.6 Teacher Training and Professional Development

Accompanying the framework are guidelines specifically tailored for head teachers and teachers. These provide a roadmap for the professional development necessary to successfully implement the framework in educational settings.

The inclusion of guidelines specifically designed for head teachers and teachers within the EU Reference Framework acknowledges the pivotal role that educators play in the successful implementation of Cybersecurity Education. These guidelines serve as a roadmap for professional development, offering a structured pathway for educators to acquire the skills and knowledge necessary for effective pedagogy in this specialized field.

The guidelines outline the specific skill sets that educators need to master. These could range from technical skills, such as familiarity with cybersecurity tools and software, to pedagogical skills, like the ability to integrate game-based learning methods into the curriculum effectively.

Given that educators are often at the forefront of curriculum planning and design, the guidelines offer strategies for integrating the framework's objectives into existing educational programs. This could involve lesson plans, project designs, and assessment methods that align with the framework's goals.

Given the sensitive nature of cybersecurity, the guidelines also provide a module on ethical and legal considerations. This training ensures that educators are well-equipped to navigate the complex ethical landscape, from responsible disclosure of vulnerabilities to the legal ramifications of data handling.

Recognizing that the cybersecurity landscape is continuously evolving, the guidelines emphasize the need for ongoing professional development. This could include recommendations for regular training sessions, workshops, and conferences that educators should attend to stay updated.

The guidelines may also include recommendations for building professional networks, both within and outside the educational institution. Such networks can serve as valuable resources for sharing best practices, troubleshooting challenges, and staying updated on industry trends.

To gauge the efficacy of professional development programs, the guidelines might also include self-assessment tools and feedback mechanisms. These instruments allow educators to evaluate their competencies, identify areas for improvement, and track their progress over time.

Particularly, for head teachers and educational leaders, the guidelines would likely include additional modules on administrative aspects. This could encompass strategies for securing funding, ensuring compliance with educational standards, and overseeing the successful implementation of the framework at an institutional level.

In summary, the educator-specific guidelines accompanying the EU Reference Framework serve as a comprehensive roadmap for professional development. They aim to equip head teachers and teachers with the multifaceted skills and knowledge required to successfully implement Cybersecurity Education, thereby acting as a catalyst for the effective realization of the framework's objectives.

2.2.7 Dynamic evolution

Recognizing the rapidly evolving nature of the cybersecurity landscape, the framework is designed to be dynamic. It allows for periodic reviews and updates to adapt to technological advancements and emerging threats.

The cybersecurity domain is characterized by its rapidly evolving landscape, where new threats and technologies emerge at an accelerated pace. Acknowledging this inherent dynamism, the EU Reference Framework is crafted to be a living document, capable of adaptation and evolution to remain relevant and effective.

The framework includes provisions for scheduled reviews at regular intervals, such as annually or biennially. These reviews involve a comprehensive evaluation of the framework's efficacy, encompassing both educational outcomes and alignment with current cybersecurity threats and technologies.

To ensure that the reviews are holistic and informed, they may involve multiple stakeholders, including educational experts, cybersecurity professionals, and policymakers. This multi-disciplinary approach ensures that the framework remains robust and comprehensive.

One of the keys focuses of these periodic reviews is to adapt the framework to address new and emerging cybersecurity threats. For example, if ransomware attacks become more prevalent, the framework could be updated to include specific modules focused on this type of threat, equipping students with the knowledge and skills to understand and mitigate such risks.

In addition to adapting to threats, the framework is also designed to incorporate technological advancements in the field of cybersecurity and educational technology. This could involve updating the game-based learning ecosystems to utilize new technologies like augmented reality or incorporating new tools and software that become industry standards.

The framework likely includes built-in feedback mechanisms, such as surveys, interviews, and performance analytics, to gather data from educators and students. This data is invaluable for identifying areas for improvement and gauging the overall effectiveness of the educational program.

Given that laws and regulations surrounding cybersecurity and data protection may also evolve, the framework is designed to be updated to maintain compliance with new legislative requirements, such as amendments to the General Data Protection Regulation (GDPR) or new EU directives on cybersecurity.

Each update or revision of the framework would be documented meticulously, providing a changelog that outlines what modifications have been made, the rationale behind them, and the stakeholders involved in the review process. This ensures transparency and allows educational institutions to seamlessly adapt to the new changes.

In summary, the dynamic design of the EU Reference Framework serves as a proactive measure to ensure its sustained relevance and effectiveness. By allowing for periodic reviews and updates, the framework remains agile, responsive, and aligned with the ever-changing landscape of cybersecurity challenges and advancements.

3 Problem Statements. Kids' cybersecurity.

3.1 Problem Statement. Why should we care?

Having children be more cyber aware is an important step in reducing cybercrime and encouraging them to enter the field of cybersecurity in later life. Most education efforts have focused on students in high school or above and have involved a wide variety of approaches. Game based learning has been shown to be a valuable way of engaging with younger students on complex issues. However appropriate sourcing, selection and use of these games in an educational context remains difficult. To overcome these issues the report provides an overview of the different sources for cybersecurity games. It also provides a series of design suggestions for the creation of an online repository for the curation and storage of serious cyber security learning games. Finally, it examines how the classroom usage of these games and how a teacher can select the appropriate game for their class and get the most out of it.

We live in a computer centric world, during the covid lock downs many aspects of life, from work to socialization, moved online. With younger and younger children getting more and more access to technology. This has led to concern about the associated risks to the health and safety of children around the world. Cybersecurity it seems is no longer the sole concern of a few technically savvy individuals but the responsibility of society. Cyberspace represents the greatest human shared common space ever and it is all our responsibilities to look after it.

The necessity for a cyber savvy youth is for two separate but interconnected reasons: the first is to reduce cybercrime, the second is to address the shortfall in cybersecurity workers available.

The movement of so many aspects of human life online has led to a boom in cybercrime and cyber criminals. Estimates vary widely as to the cost of cybercrime from the billions to trillions of dollars globally (depending on how it is calculated) 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 (Chowdhury & Gkioulos, 2021). These high-profile attacks are not primarily aimed at children, but they will still suffer from the effects of them, nonetheless.

There are however low-profile attacks that may be specifically aimed at a younger audience. The ENISA Threat Scanning Landscape for 2023 identified eight key threats of which phishing and social engineering attacks are the most likely to target children directly (European Union Agency for Cybersecurity., 2022). Both threats fit within the Mitre ATT&CK (*MITRE ATT&CK®*, n.d.) and Lockhead Martins cyber kill chain models (*Cyber Kill Chain®*, n.d.) as reconnaissance techniques. Thus, their interruption will thwart many other threats located down the line.

3.1.1 Threat landscape

3.1.1.1 Social engineering

Social engineering attacks are a broad group of attacks in which there is an attempt to manipulate the user. They do not target the computer system directly but instead attempt to manipulate the user into taking an action through four different mechanisms. The first is that they manipulate through the offer of financial rewards, offer of Money (you have just one 1,000 euro click here to collect). The second attempts to play on the Ideology of the user (sign this online petition to stop animal testing). Next, they will attempt to convince the user that they have been compromised (we have already hacked your webcam and recorded you watching things you shouldn't). Finally, the attacks may focus on stroking the Ego of the victim (we would like to recognise your work for charity click the link below). These attacks were categorised by the C.I.A as recruitment tools and are known in the literature as the M.I.C.E model (Burkett, 2013).

3.1.1.1.1 Phishing

A phishing attack is a specific example of a social engineering attack. Normally an email which appears to be sent from a reliable source. The email contains a link that the user is asked to click. If this is done some malware is downloaded onto the machine and access is given to the cyber attacker. Most phishing attacks send out a form letter style email to the recipients attempting to manipulate them using M.I.C.E. As noted in the ENISA threat landscape for 2023 there has been a rise in phishing as a service in the last year. This means that the cybercriminals do not even need to be technologically capable but can pay for the software to do it for them. This should result in increases in phishing attacks with more people being scammed.

Other social engineering attacks that students are particularly vulnerable to.

3.1.1.2 Disinformation and Misinformation

3.1.1.2.1 "Fake news"

One of the leading topics these days is "fake news" aka information that is not correct but is shared as fact. This does not seem like a cyber issue, and it is not usually classified as such when discussing companies etc. Still, it is a topic that is relevant to children online as well. Firstly, they encounter and share a lot of information - TikTok, Instagram posts, YouTube videos etc. They help amplify certain material over other things. Secondly, wrong information can also be a cyber issue. Children are targeted with fake ads for games, with fake apps and scare tactics. A good example of scare tactics meeting spam was in October 2023 when thousands of establishments in Estonia received bomb threats, including schools. There was also additional information shared on Snapchat and TikTok, about how some schools had already been blown up. None of this happened, this was an example of disinformation.

"Fake news" is usually a wide-ranging term that can be narrowed down to either "disinformation" or "misinformation." The former is a clear attempt to share fabricated information, mostly for nefarious purposes. Misinformation is accidentally misleading, unreliable and somewhat wrong information. The goal is to share information, but the end result is the same - wrong information is spreading. It is important to note that this is an issue of media competency above everything but does impact children's cyber security as well.

3.1.2 Why might children be targeted?

The main question is: why attack children? In general, there are two reasons: children are a specific target, and they are a way to access their parents or other adults.

3.1.2.1 Stepping stones

One of the primary reasons why children may be targeted is to be used as an avenue of attack. This can be likened to the child being used as a stepping stone to get to more valuable information. For example, the use of shared family devices can lead to children mistakenly downloading malware or spyware to the device. When coupled with poor cyber hygiene practices on the part of adults, this can be a recipe for disaster. The habit of people to reuse passwords between work and social accounts is one example of this vulnerability. The child unwittingly downloads a keylogger in the form of a game or other media which then captures the passwords of all the users of the shared device. Even if the parent does not use the device for anything work related, a common password used with the work account gives access.

These indirect attacks can best be combated by educating people of all ages about the principles of cyber hygiene.

Children can also give out information about their families or homes. A targeted phishing attack can be useful for collecting information or for blackmailing. Children might also have access to parents' credit cards or personal information that they might share by accident or as a result of an attack.

3.1.2.2 Direct targeting

3.1.2.2.1 Recruitment/manipulation and legal implications

Unfortunately access to the target is sometimes the primary goal of the cybercriminal. This can take many forms, from grooming and exploitation through to the compromising of technology to allow the criminal to spy on children. Recruitment has two aspects: firstly, the technological knowledge. It is easy to target children who might not know how anything works and therefore are ignorant of dangers. But all children are a possible target socially. All children are vulnerable when it comes to not understanding the impact of their actions, legal aspects etc. For example, hacking is a crime, even when you are under age.

There are also significant moral and social implications. Taking photos of classmates, sharing personal information, uploading sensitive videos etc. These issues are partially related to cyber hygiene but are part of a wider social understanding of how the internet and the world work.

3.1.3 Financial attacks

3.1.3.1 Loss of accounts

Certain video games come with purchased items, one can buy things with real life money and then sell or trade these items. Phishing is used to get access to children's accounts and then the items are sold. As the hackers might not know who has the most valuable items, all accounts are in danger, even if there is nothing sellable.

3.1.3.2 Low level ransomware attacks

While high level ransomware attacks make the news regularly (the Colonial pipeline attack (Reeder & Hall, 2021), the Irish Health service attack ("HSE Cyber-Attack," 2021)), it is unlikely for children to be targeted in this manner, mostly because they do not have the financial resources to make it worthwhile. There is one area in which ransomware attacks may be possible for children however, namely in the online game environment. It is possible for accounts in games to be compromised and for the player to have their virtual property stolen or held for ransom. Students should be aware of the risks this entails and encouraged to maintain good cyber hygiene. There is limited data available on this aspect of cybercrime and further research is needed.

3.1.3.3 Loot boxes and gambling targeting children

Children are a target for many online activities that harm them but are not necessarily illegal. A rising trend in online gaming is free games with paid add-ons. This might mean advertising - showing ads for more gameplay or for special items. This might also mean microtransactions: asking for small amounts of money for a chance to redo a level, get a power-up, a new outfit or something else. These microtransactions are not illegal but without proper cyber hygiene and understanding of how the system works, a children might spend their or their parents' money without realising or without realising the amounts. Cases like these are common, for example here. This is an issue that needs to be addressed as part of cyber hygiene training.

A more controversial change in this field is the introduction of loot boxes and other gambling mechanics in games. There is also an increasing number of add-ons that can be bought not outright but as "loot boxes" where the player might get something valuable or not. This is essentially gambling and has been targeted by governments but teaching children about this matter is still crucial.

3.1.4 Children as script kiddies

So far, the discussion has centred on children as the potential victims or collateral damage of cyber criminals. However, we must be aware that children may also become threats to cyber security or cyber criminals themselves. One of the balancing acts in cyber education is to make children aware of the dangers without making it easier for them to gain access to the tools. This can be likened to education about drugs or other illegal activity how do we give the students enough knowledge without encouraging them to try their own hands at it.

A less discussed but pertinent issue in the realm of Cybersecurity Education is the phenomenon of children becoming "script kiddies." The term refers to individuals who use pre-written software or code scripts to execute hacking activities without a deep understanding of the underlying technologies. While these activities may start as an exploratory endeavour or even a form of digital rebellion, they have serious legal and ethical implications.

There may be a belief among some stakeholders and parents that the skills and tools to be an effective hacker are beyond the level of children. This view is blatantly false and does not take into account the existence of script kiddies. This derogatory term given to beginning level hackers comes from the fact that they mostly use generated scripts and pieces of code found on the internet. They are often just beginning to hack and are inexperienced but can nonetheless cause chaos and confusion through their attacks. The attacks can be especially dangerous because the script kiddie does not have the necessary understanding of what the code is actually doing. This may lead to more damage to be caused than was initially intended.

The basic skills to run these attacks are very familiar to any student who has installed a mod into a game or even has a basic understanding of code or can follow directions. The code snippets or scripts can be found either via forum posts, community interest groups or possibly created with the use of AI.

Children in this category pose a twofold risk. First, they themselves become vulnerable to legal repercussions, even if unaware of the full extent of their actions. Second, they become conduits for cybercriminal activities, as their compromised systems can be used for more sophisticated attacks. Therefore, Cybersecurity Education should not only focus on defensive measures but also instil ethical guidelines and an understanding of the legal boundaries related to digital behaviour. This component is crucial for deterring potential script kiddies and guiding their curiosity toward more constructive avenues in the field of cybersecurity.

3.1.5 AI issues

Artificial Intelligence (AI) reduces the effective cost of entry to many fields by giving suggestions or support to people learning. Sadly, hacking and cyber threats are one of the fields that can be supported.

Chat GPT and other AI software can be used to write code for users who do not know how to write it themselves. While requests to write code for a key logger or for a denial-of-service attack will often generate refusals and warnings about the legal issues surrounding these. Asking more generic questions can allow the user to circumvent these issues. So, for example a request for a key logger will be refused but a request for a screen recording that then follows up to ask for keystrokes to be captured will generate a python script. These scripts were not tested but can form the basis for script kiddie attacks.

In addition to writing code AI can also be used to increase the believability of social engineering attacks. The emails can be constructed easily and quickly with fewer grammatical or other errors that may have been a red flag in previous phishing attacks.

AI introduces a novel set of challenges and opportunities in cybersecurity. On one hand, AI technologies can significantly augment cybersecurity measures, offering advanced monitoring and detection capabilities. On the other hand, they can also be weaponized to conduct more sophisticated attacks, making the cybersecurity landscape even more complex for children to navigate.

For instance, AI-powered chatbots could be employed in social engineering attacks targeted at children, who may not have the discernment to distinguish between human and AI interactions. Moreover, machine learning algorithms can also analyse user behaviour to create more effective phishing schemes that could deceive even vigilant users.

Given the rapidly advancing field of AI in cybersecurity, it is imperative to include this aspect in educational frameworks. Students should be made aware of the dual nature of AI in cybersecurity—its capacity for both protection and deception. A nuanced understanding of these issues will equip them with the skills to critically evaluate AI technologies they may encounter, fostering a more comprehensive cyber hygiene regimen.

Both of these sections, 3.4 and 3.5, indicate the necessity for a multi-faceted approach to Cybersecurity Education that not only focuses on the risks but also educates children on the ethical and technological complexities of the digital world.

3.1.6 Bullying and cyber transplantation of issues

A popular topic among parents and teachers is discussing bullying online. This is definitely a common problem and does have a cyber aspect, but the root cause is elsewhere. It is important to note that the issue of bullying is common outside the cyber world, but the cyber world may make it worse. There are multiple topics overlapping: communication online (communication competencies), recognising "fake news" (knowing that maybe the screenshots are wrong, or the information is wrong, and that the cyber world is not separate from the real world. There are also other topics that originate from elsewhere but bleed into cyber security: inequality, racism, sexism, homophobia etc. These issues are not cyber security issues, but the online circumstance might make them worse.

3.1.7 The Job Market

Estimates range from there being a shortfall of 3.4 million jobs in the field of cybersecurity worldwide. Inside the European union the need for cybersecurity experts has been increasing with some estimates of vacancies at over 300,000 in 2022 (*Cybersecurity Workforce Study*. 2022)

, 2022). The field of cybersecurity has been growing at a rate of 145 % per year and is expected to continue to increase into the future (CBR Staff, 2019). The job postings seeking cyber security professional increased by 94% from 2013 to 2019 whereas IT vacancies increased by only 30%. (European Union Agency for Network and Information Security., 2019). In addition, the rate of demand is far outstripping the supply of skilled professionals and the workforce gap has grown by 26.2% year-over-year. (ISC2, 2022)

The need for a cybersecurity work force has led to several governments setting up new university and postgraduate degrees, along with continuing education programs to retrain older members of the working population. The ENISA has created a "cybersecurity higher education database" (*CYBERHEAD -*

Cybersecurity Higher Education Database, n.d.) listing 146 programs across 28 countries in the EEA countries and Switzerland.

In the area of commercial training there are several organizations offering short courses in cybersecurity awareness. Examples include NATO CCDCOE, BHC, and CR14 in the small country of Estonia alone.

Estonia is one of the more cyber developed countries in Europe and has many programs aimed at children. There are cyber security educational materials for children, teachers and parents: targaltinternetis.ee (be smart on the internet) and there are experts, games etc. There are also private sector initiatives like Telia's (a northern European Telecom company) Suurim Julgus (The biggest bravery) program that tackles bullying.

Estonia also has multiple cyber expert competitions for children. European Cyber Olympic teams come from these competitions, but they also aim to raise awareness in general. KüberNaaskel, KüberPuuring and other similar initiatives target interested youth, especially focusing on bringing in more girls.

In Italy, several numerous initiatives are in place to raise awareness about cybersecurity issues. In addition to master's degree programs in IT Security, such as those offered by the University of Pisa and CNR, there are also other national-level opportunities available.

One such initiative is the CyberChallenge.IT project, which is organized by the Cybersecurity National Lab, with the support of cybersecurity experts. This program is designed to provide training for young individuals aged between 16 and 24, with the goal of enhancing their skills in cybersecurity tools and techniques.

Furthermore, the Cybersecurity National Lab hosts the Cyber Trial, which offers a set of free gaming and training programs tailored for women high school students.

Another noteworthy program is titled "Una vita da social". This is an awareness campaign organized in collaboration with the National Police that targets young people while also involving teachers and parents. The campaign's primary objective is to combat violence and abuse by young bullies. It has been developed under the umbrella of the Ministry Education's *Generazioni Connesse/Safer Internet Centre Italia* initiative.

3.2 Problem Statement. Why should schools care?

In the contemporary educational milieu, the significance of Cybersecurity Education for schoolchildren aged 8-13 is experiencing an unmistakable ascendance. This surge is not an isolated development but is indicative of a larger societal shift that places a heightened emphasis on fostering digital literacy and ensuring online safety. The urgency of this educational imperative is only compounded by the escalating complexity of the digital ecosystem, replete with diverse online threats and ethical conundrums.

Though the modus operandi of delivering Cybersecurity Education can differ considerably across nations and educational systems, an analysis of various curricula and teaching strategies reveals the emergence of some common pedagogical methodologies and instructional resources. These shared approaches serve as a sort of global pedagogical lexicon that transcends regional disparities, thereby offering a foundational structure on which diverse educational systems can build.

For instance, the integration of cybersecurity topics into broader, more established academic subjects—ranging from Information Technology and Computer Science to General Studies—serves as a universal tactic. This integrative approach allows for a more seamless insertion of cybersecurity principles into existing curricula, thus ensuring that students receive this vital instruction without necessitating a wholesale restructuring of the educational program. It also provides the advantage of contextualizing cybersecurity issues within a broader academic and practical framework, thereby enhancing the relevance and applicability of the concepts taught.

Further, beyond formal educational settings, the emergence of universally accessible resources—such as online courses, workshops, and educational games—signals a democratization of Cybersecurity Education. These platforms not only extend the reach of cybersecurity instruction beyond the classroom but also adapt to the diverse learning needs and paces of individual students.

In summation, while the specifics of Cybersecurity Education may be subject to regional variations and pedagogical philosophies, the overarching methodologies and resources employed exhibit a remarkable universality. This commonality suggests a collective, global recognition of the imperative to equip the younger generation with the competencies and ethical frameworks required to navigate an increasingly complex and perilous digital landscape.

3.2.1 Curriculum approaches

Within formal educational settings, cybersecurity topics are frequently incorporated into more expansive subjects such as Information Technology, Computer Science, or even General Studies. This integration serves a dual purpose: it not only familiarizes children with the rudimentary principles of online safety and data protection but also situates these principles within a broader educational context, thereby enriching their understanding. Stand-alone courses that exclusively focus on cybersecurity do exist, although these are comparatively rare for the age group in question, given the complexity of some topics and the need for foundational knowledge in computer science.

Beyond the traditional classroom, a plethora of alternative educational avenues are available. Workshops, camps, and online courses provide more specialized or flexible options for Cybersecurity Education. These settings often employ hands-on learning experiences to engage students actively, offering a different but complementary pedagogical approach compared to formal education.

Moreover, the advent of educational games like ‘Spoofy’ represents a novel strategy to make Cybersecurity Education more engaging for young learners. These games, sometimes integrated into a more comprehensive curriculum, employ interactive scenarios to teach key cybersecurity concepts. Through gaming, children can assimilate crucial knowledge in an experiential manner, thereby enhancing both their understanding and retention of the subject matter.

Thus, as digital threats continue to evolve, so too does the imperative for robust Cybersecurity Education. Whether embedded within broader academic subjects or explored through specialized courses and interactive games, the ultimate objective remains consistent: to equip the younger generation with the necessary skills and ethical understanding to navigate the digital world safely and responsibly.

3.2.2 Topics

In the realm of Cybersecurity Education for children, several key topics emerge as focal points for fostering a comprehensive understanding of the digital world. Among these, online safety takes precedence as an introductory subject. Here, children are taught about the inherent risks associated with their online behaviours, such as the potential hazards of sharing personal information indiscriminately.

Following closely is the concept of the digital footprint. This topic aims to educate young learners about the indelible nature of their online actions. In simple terms, they are made aware that what they do on the Internet can have a lasting impact, shaping their digital identity for years to come.

Basic cyber hygiene constitutes another essential topic in the curriculum. Children are imparted with practical knowledge about creating strong passwords, connecting to secure networks, and understanding the critical role of regular software updates in maintaining system security. These fundamental practices serve as the building blocks for more advanced cybersecurity concepts.

Understanding cyber threats is yet another crucial subject that is simplified for young learners. Through age-appropriate explanations, children are introduced to the basics of malware, phishing, and other common threats that lurk in the digital landscape. The objective is to equip them with the rudimentary skills required to identify and navigate around such hazards.

Last but not least, ethical conduct in the digital sphere is emphasized. This encompasses a broad range of issues, including plagiarism and respect for intellectual property, as well as guidelines for appropriate behaviour online. The aim is to instil a sense of digital citizenship, encouraging children to interact in the digital world with the same ethical considerations they would apply in the physical world.

Taken together, these topics provide a well-rounded foundation for children to navigate the increasingly complex world of cybersecurity, fostering both technical acumen and ethical awareness.

3.2.3 Assessment methods

With reference to assessment methods for Cybersecurity Education, a multi-faceted approach is typically employed to gauge a student's grasp of the subject matter. One common method involves administering knowledge quizzes, which are usually composed of multiple-choice questions. These questions are designed to test the student's understanding of key terminology and basic principles integral to cybersecurity.

In addition to knowledge quizzes, practical exercises serve as another vital component of the assessment strategy. These exercises task students with identifying potential threats within simulated environments, providing a hands-on experience that allows for the application of theoretical knowledge. The objective is to mimic real-world scenarios to evaluate how well the students can navigate cybersecurity challenges.

Beyond quizzes and practical exercises, behavioural assessment forms the third pillar of the evaluation process. In this context, educators observe students' behaviour in practical settings or simulations. The focus here is not just on what the students know, but how they apply this knowledge in real or simulated situations. This method aims to assess the students' understanding of cybersecurity best practices, including their ability to identify risks and respond appropriately.

Through this triangulated approach—comprising knowledge quizzes, practical exercises, and behavioural assessment—educators can obtain a comprehensive view of a student's cybersecurity acumen, thereby enabling more targeted and effective instruction.

3.2.4 The pivotal role of school heads in cybersecurity education

In this intricate educational landscape, the role of school heads becomes pivotal in orchestrating an effective Cybersecurity Education strategy. The school head serves as the linchpin that can either facilitate or impede the integration of cybersecurity topics into the existing curricula, depending on their administrative and pedagogical decisions. Their leadership is not merely administrative but extends to defining the educational ethos of the institution, thereby influencing how cybersecurity is valued, taught, and implemented.

Firstly, school heads are responsible for the strategic alignment of Cybersecurity Education within the broader educational objectives of the school. This involves scrutinizing the existing curricula to identify natural intersections where cybersecurity principles can be seamlessly integrated. The decision to either incorporate these topics into existing subjects or to introduce stand-alone courses on cybersecurity lies substantially with the school head.

Secondly, resource allocation is another crucial activity. School heads need to ensure that sufficient resources—be it time in the curriculum, qualified teaching staff, or technological tools—are allocated to make Cybersecurity Education effective. This also extends to procuring or creating instructional materials, including digital platforms and educational games that can enhance the learning experience.

Moreover, school heads are responsible for fostering partnerships with external organizations that can provide additional resources or expertise. This can range from liaising with governmental bodies for accreditation or funding, to collaborating with tech companies for resource provision, and even to networking with other educational institutions for knowledge exchange.

Additionally, assessment and evaluation mechanisms often fall under the purview of the school head. They must ensure that the teaching strategies employed are subject to rigorous evaluation for effectiveness, involving both formative and summative assessments. These assessment metrics not only serve to gauge student understanding but also act as performance indicators for the instructional approaches employed.

Lastly, the school head plays a role in continuous improvement by keeping abreast of global best practices and emerging threats in the field of cybersecurity. This involves ongoing professional development for themselves and their staff, as well as periodic curriculum reviews to incorporate the latest knowledge and strategies in the rapidly evolving field of cybersecurity.

In essence, the school head’s role is multifaceted, extending from strategic planning and resource allocation to external collaboration and continuous improvement. Their actions and decisions serve as a driving force that shapes the quality, effectiveness, and relevance of Cybersecurity Education in the school setting.

3.2.5 The crucial responsibilities of teachers and educators in cybersecurity education

In the context of the burgeoning emphasis on Cybersecurity Education for schoolchildren aged 8-13, the role of teachers and educators cannot be overstated. They serve as the front-line agents responsible for the effective dissemination and contextualization of cybersecurity knowledge and best practices. Unlike school heads, who engage in curriculum design, resource allocation, and policy formulation, teachers are tasked with the actual implementation of these directives.

Teachers are primarily responsible for adapting the cybersecurity curriculum to meet the specific needs and comprehension levels of their student body. This involves breaking down complex cybersecurity concepts into digestible pieces, creating interactive lesson plans, and utilizing educational technologies, such as cybersecurity games like ‘Spoofy,’ to augment the learning experience.

Moreover, educators often take on the role of continuous assessors. Through a variety of evaluation methods—ranging from knowledge quizzes to practical exercises—they gauge student understanding, track progress, and identify areas for improvement. This continuous assessment is vital for adjusting teaching strategies and ensuring that learning objectives are being met.

Furthermore, teachers play a crucial role in fostering a culture of online safety and ethical online behaviour. They not only teach the technicalities of cybersecurity but also instil a sense of digital citizenship, covering issues like plagiarism, intellectual property respect, and appropriate online conduct.

To fulfil these multifaceted roles effectively, ongoing professional development is imperative for teachers. They must stay abreast of the latest cybersecurity threats, technologies, and pedagogical strategies to integrate this evolving subject matter into their teaching methods.

In summary, teachers and educators hold the key to the successful implementation of Cybersecurity Education, as they navigate the complexities of delivering this vital subject matter to a young and diverse audience. Their role is multidimensional, encompassing curriculum adaptation, pedagogical innovation, continuous assessment, and the cultivation of ethical online behaviour.

3.3 National Initiative for Cybersecurity Education: A Case Study

In the context of defining global best practices and foundational structures for Cybersecurity Education, the National Initiative for Cybersecurity Education (NICE; see Newhouse et al. 2017) serves as an exemplary model worth consideration. Spearheaded by the National Institute of Standards and Technology (NIST) in the United States, NICE aims to fortify the cybersecurity capabilities of the nation by establishing a comprehensive and sustainable educational program.

One of the cornerstone contributions of NICE is the Cybersecurity Workforce Framework, which provides a standardized lexicon and skill set for cybersecurity roles. This framework serves as an instrumental resource for educators, offering a well-defined pathway for curriculum development and competency-based training. The model's structured approach enables educators to align learning objectives with industry demands, thereby enhancing the career readiness of students in the cybersecurity domain.

Importantly, NICE is not merely a nationalistic endeavour; it extends its utility by informing international efforts towards cybersecurity workforce development and education. Its frameworks and guidelines can be adapted and contextualized for varying educational systems and settings, thereby contributing to the global pedagogical lexicon highlighted earlier in this section.

However, it is pertinent to note that the applicability of the NICE framework requires thoughtful adaptation to local contexts and educational philosophies. Its predominantly U.S.-centric focus might necessitate adjustments to accommodate region-specific needs, regulatory requirements, and cultural considerations.

In summary, NICE serves as a significant touchstone in the evolving landscape of Cybersecurity Education. Its frameworks and methodologies offer a structured approach that can be adapted across different educational settings, contributing to the universality of Cybersecurity Educational strategies. While its primary focus remains within the U.S., the initiative’s principles and frameworks offer valuable insights that can inform and enrich Cybersecurity Education globally, thereby substantiating the imperative to equip younger generations with the skills and ethical considerations essential for navigating an intricate digital ecosystem.

While Nice acts as an exemplar of defining skills and associating tasks with the knowledge, skills and abilities to complete them. It is still focused on an adult workforce and like almost all of the preexisting frameworks ignores the role of educating children in the creation of an effective cyber security workforce for the future. Leaving us to wonder how are we to engage a younger audience with the complex issues surrounding cyber security? One potential solution is outline in part 4 along with the difficulties associated with it.

4 Videogames in education

When it comes to the education of even younger students, game-based learning is often viewed as a key method of engaging them. The National Security Agency (NSA) in the USA has developed a CyberSkills summer camp which includes the use of several games (Jin et al., 2018) to encourage high school students to consider a career in the field of cyber security.

The games that are used in cyber security training span a wide range of genres and can be both analogue and digital. These games could be used an all levels: teaching basic hygiene, engaging in media literacy or preparing for future education. These games include seminar wargames, cyber range activities, capture the flag competitions, board games, card games and even roleplaying games. Given the wide range of mediums and genres used in this field, some categorization is necessary. We will take a brief look at the following groupings: commercial games, technical games and serious games.

After establishing the importance and prevalence of game-based learning in Cybersecurity Education, it's critical to delve into the various types of games that are commonly employed. These games can be broadly categorized into commercial games, technical games, and serious games, each with its distinct characteristics and implications for educational settings.

4.1 Commercial games

This is the most polished and well-presented group of games in the field. Commercial games are usually produced by the private sector, they cost money, and the main goal is not usually education, it is profit. This is not necessarily a negative, they just have to be used correctly and the players need to understand that the main goal is not educational. These games can range from pen and paper roleplaying games like Shadowrun and Cyberpunk 2020, to card games like Net Runner and on to full on computer games like Sylvarcon 2049 and NITE TEAM 4.

The primary issues with the use of these types of game for teaching are:

- The cost, each game license or set retails between 20-50 Euros.
- The games are designed for entertainment first, this means that they may reinforce ideas that are more cinematic than actual. Or they may drastically simplify the activity for the purpose of maintaining game flow. (examples include XCOM 2's hacking system)
- Sourcing games, games may go out of print or be pulled from the marketplace without warning.
- The games may not be thematically appropriate for a younger age group.
- High cost of educator time. In the same way that a teacher should have read the book before bringing it into the classroom they should have played the game to be aware of the content. This is problematic given teachers' workloads and that the games can range in play times from 1 hour for a card game to 60+ hours for the computer games.

Commercial games represent a polished and well-crafted category of gaming, primarily designed with entertainment in mind. Although not primarily educational, these games can still offer valuable lessons in cybersecurity when employed appropriately. However, several challenges accompany the use of commercial games in educational settings, including but not limited to cost, thematic appropriateness, and the need for extensive educator preparation.

4.2 Technical games

Technical games focus primarily on developing technical skills within the domain of cybersecurity. Whether commercially produced or publicly funded, these games are more specialized and often require a certain level of existing knowledge or facilitation. Examples include cyber ranges, Capture the Flag (CTF) competitions, and other high-level cybersecurity activities.

While these games can be highly effective for skill development, they may not be universally accessible. The technical nature can be a barrier for beginners, and the games often require a knowledgeable facilitator to bridge the gap. Moreover, the focus on high-level skills makes them more suitable for advanced learners rather than novices.

The primary issues with the use of these games are

- The high cost of the facilities associated with setting them up and running them
- The games being aimed at a technically advanced audience
- Age appropriateness

4.3 Serious games

Serious games are defined as "games [which] have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement." (Abt, 1987) this type of game is normally designed and created with education in mind. This grouping can be broken up into free to play and the pay to play camps.

4.3.1 Free to play

These games tend to have been created as either parts of research projects, (thesis, EU and governmental grants) or by companies as a form of advertising. They tend to be less polished than the commercially focused games with less resources being spent on marketing etc.

A form of free to play games are those that are free for the end users but use funds from someone else. A good example is Hackshield, a cyber game from the Netherlands. The game is privately owned but funded by local governments and education districts who purchase it for their schools, the final product is free to use. Hackshiled's basic version is also free to use online, for everyone. The paid version comes with added study analytics and teacher accounts.

Completely free games like "Nabbovaldo and the Cyber Blackmail" and "Spoofy" are aimed at a younger audience and are freely available online and/or to download from app stores. Their aim is to make players aware of some of the key issues in cybersecurity for their age groups.

The issues with free to play serious games:

- Sourcing. The majority of cybersecurity games produced and used in academic studies are used for one study and then abandoned. This can make them almost impossible to get a hold of.
- More sustainable models require additional funding from target groups (like Hackshield) or corporate sponsorships (Spoofy).
- Variety of quality. The games can range from interesting and engaging to thinly disguised quizzes with minimum game play and next to no replay ability.
- The game used still has to be matched to the Intended learning outcome of the class.

4.3.2 The pay to play games

These are games that are offered by companies in the corporate training market. These include "Anti Phishing Phil" and the Deloitte training program.

The issues with pay to play serious games:

- Financial cost. As these games tend to be aimed at corporate training, the costs reflect the prospective budget of this group with licenses starting at 5,000 dollars and going upward to in excess of 500,000.
- Variety of quality. It is very hard to assess the quality of these game offerings because review copies are not made readily available. This can make it almost impossible for a teacher to match the game to the intended learning outcomes.
- Age appropriateness. The games are aimed at the workforce and as such may include themes or issues that are not necessary or appropriate to the student age group.

Having explored the various types of games used in Cybersecurity Education, it becomes evident that each category offers unique benefits and challenges. The subsequent sections will delve into the practical aspects of incorporating these game-based learning approaches into cybersecurity curricula, considering factors such as age appropriateness, educational outcomes, and budget constraints.

5 Recommendations for the design of the Ecosystem

The limitations of the free to play serious games can be addressed through the design and development of an ecosystem. This would allow teachers to more easily locate the games to use thereby solving the difficulty of sourcing the games. In addition, the ecosystem would allow teachers to leave comments and recommendations on the games improving the quality of the games being used. Finally, it would act as a repository of knowledge and future teacher training resources. To meet these goals key design considerations are discussed below.

5.1 Security of ecosystem

A note on security: anything associated with cybersecurity is a target for malicious actors on the Internet. In the best-case scenario white hat hackers find it amusing to compromise the security and then notify the owner before trying again. Appropriate care must be taken to ensure the confidentiality of all the users of the system, the integrity of the information contained and finally the availability of the system to be accessed.

5.2 Users? Or target group? Or the ecosystem?

The ecosystem around the games requires careful consideration in its design and development.

First of all, there are three separate classes of potential users.

The first and primary user class are the teachers who want or need to incorporate cybersecurity lessons into their curriculum. The second class are the school administrators, parents and other stakeholders in the educational process. The final grouping are the potential students or other interested parties whose focus is on playing the games themselves.

Each of these different classes of users have different needs from the ecosystem in terms of materials and access.

5.2.1 The 3rd parties

This group requires the least amount of access rights to the ecosystem. They are primarily interested in getting access to the games and reading the reviews posted by other members of the ecosystem. They are unlikely to want to log in, and they would not have any permissions to add to the ecosystem. (to post a review they would have to step up their engagement to that of a teacher or primary user).

5.2.2 The teachers and classroom users

This is possibly the most important target group for the success of the ecosystem as they provide the grassroots support and community to build the system up and out. Personas were gathered from all of the countries involved in the consortium and were synthesized into a key persona.

A persona built on descriptions of the potential users reveals some key findings.

- The teacher has limited time and mental resources to find the games.
- Even if they are found the teacher needs support in how to use them in the classroom.
- The teacher needs support in being able to select the games that suit their context.

Conclusions can be drawn about the ecosystem from this. First, from a design perspective, the system has to be clear and easy to use, the interface should not be overly busy, and the gamification elements used should be handled lightly (more like social media and less like Duolingo). If we want users to log in, we must give them some features to entice engagement. All of these systems described below are based on a login to the ecosystem which given the limited time of teachers should, if possible, include one click joining either via a Facebook or google account.

The first and fundamental feature is the search feature to allow them to find the games they are looking for. Search criteria should include the age level of the game, a description of the skills that the game covers, the amount of time it takes to play the game, and finally the modalities of play that are best suited to the game. This will address one of the fundamental problems of free to play serious games as described above.

The next prospective feature is to allow them to save their favourite games so that they do not need to keep searching for them every time they want to use them. This meets their needs for efficiency and reduces the amount of time that they must invest into the system long term.

To address the limitations about quality, a system which allows the ability to recommend games to other teachers is highly recommended; this should be achieved by a simple upvoting system. This will also satisfy some of the socialization needs with other teachers and help build a sense of community.

Building on the upvote system the user should be able to review the games and add their comments to them and upvote useful comments. They should get access to support materials and classroom guides to the games as well as eventually have the options to share and publish their own materials.

5.2.3 The administrators or stakeholders

This class differs in one key aspect: they require more hand holding and justification of game-based learning as a methodology. They are going to be much more interested in the efficacy of the ecosystem and the games that are recommended. They may also need to draw from the system support to be used in justifying the decisions to use this teaching method to parents and governmental bodies. A section of the ecosystem should therefore be devoted to the storage of positive news articles, case studies as well as summaries of why game-based learning is a valid and valuable approach to the learning of cyber security,

5.3 User Skill Progression: A Typological Approach

When discussing the ecosystem, it is useful to analyse the user's pathway through the system using the typology from Zichermann's Gamification by design (Zichermann & Cunningham, 2011). This typology traces the evolution of a user through the stages of novices, to problem solvers, and onto experts and finally to masters. We can chart the skill set and encourage the user to master the tools that are being provided. This helps with understanding when to introduce tools to the user and different design decisions that must be taken.

5.3.1 Novices

These are the people who have just started to use the system they may not even be logged in. They are unfamiliar with the interface and are most likely to get frustrated and leave. They need to be carefully onboarded and encouraged to explore the system. The goal with this group is to encourage them to finally log in to the system in full and to get them familiar with the search system.

5.3.2 The Problem Solvers

This group is starting to figure out how to navigate within the system. They have figured out how to use the search system and understand the rating system. This group needs to be encouraged to engage with the rating and reviewing system and how to find and download teacher created content.

5.3.3 The Experts

The ecosystem should be encouraging people who reach this skill level to produce content to be shared. They should have a firm grip on how the system works and how to get the most out of it. They are most likely to be the ones to write reviews and produce lesson plans for others to use.

5.3.4 The Masters

At this level the users are so familiar with the system that they become the community leaders. They are likely to act as moderators for the system, advisory board members for changes and mentors for those beginning to use the system.

Special care must be taken in encouraging users to slowly progress through the paths of mastery. The actions that each user can take must be defined and tied to an appropriate reward structure. With consideration being given to the interval and value being set.

5.3.5 Reward structures

A fundamental feature to a gamified system is the use of rewards to incentivise behaviour. Reward structures are defined by the acronym SAPS. which stands for Status, Access, Power, and Stuff. The ecosystem should aim to work primarily off the first two rewards with some use of power rewards as the user reaches the level of mastery. Stuff (the material real world rewards) should be avoided as it leads to increasing overhead in the operation of the ecosystem and may make it harder to maintain.

The primary reward should be status within the system. This is best achieved using badges that can be displayed by the user as a marker of status and recognition. Badges that are awarded by the system are less valuable than badges that have been awarded by peer users of the system. E.g., upvoter: you have upvoted 5 different posts by other user's vs popular: your posts have been upvoted by 5 different users. Status can also be achieved by posting a feed of popular and rising topics on a home page that all users can see.

Access as a reward will be fundamental inside the ecosystem. As a user moves through the steps of mastery, they should unlock the ability to do more with the system. So, a novice user who hasn't logged in yet will be able to use the search feature but a problem solver who has learned how to log in will have access to the favourite and upvote features. This will encourage users to take steps along the pathway to mastery at every step.

The interval for acquiring rewards and recognition must be carefully considered. A reward in the form of a streak of logging in every day may encourage users to do so but may not encourage them to stay and be active within the system. Conversely push notifications which can be seen as intrusive and annoying when advertising the system can be highly rewarding when it is informing the user of an upvote or other approval that they have received from a peer.

The system for rewards must be simple enough to get an intuitive feel for but not so simple that it becomes highly predictable.

6 Integration of the Ecosystem into the curriculum

In the educational framework aimed at enhancing cybersecurity literacy among schoolchildren aged 8-13, the provision of a resource-rich ecosystem is paramount. This ecosystem is designed to serve as a comprehensive toolkit for teachers, offering an array of resources that can be seamlessly integrated into the classroom setting. Central to this ecosystem is a model curriculum, crafted based on the SCK Skills Framework (WP2).

The model curriculum serves as a blueprint for educators, outlining the scope, sequence, and complexity of cybersecurity topics to be covered. It addresses various educational objectives, from instilling basic online safety principles to fostering advanced skills such as threat identification and mitigation. Designed to be flexible, the curriculum can be adapted to suit the unique needs of different educational settings and student demographics.

Complementing the model curriculum are supplemental resources that include lesson plans, activity sheets, and interactive learning modules. These additional materials are designed to enrich the classroom experience, providing hands-on opportunities for students to engage with cybersecurity concepts. They also serve to alleviate the preparation burden on teachers, offering ready-to-use resources that align with the curriculum's objectives.

Recognizing the dynamic nature of the cybersecurity landscape, the ecosystem also provides ongoing support and training for teachers. This professional development component is crucial for ensuring that educators are equipped with the latest knowledge and skills to effectively deliver the curriculum. Training modules, webinars, and workshops offer teachers the opportunity to deepen their understanding of cybersecurity trends, technologies, and pedagogical best practices.

In the overarching structure of this Cybersecurity Educational framework, the role of school heads is indispensable for successful implementation and ongoing efficacy. As custodians of educational quality and institutional strategy, school heads have the responsibility to facilitate the integration of this specialized curriculum into the broader educational context.

School heads are tasked with the initial adoption and institutionalization of the model curriculum based on the SCK Skills Framework. This involves strategic planning, resource allocation, and coordinating with key stakeholders, including teachers, parents, and educational boards. They must ensure that the necessary technological infrastructure is in place to support the digital components of the curriculum, such as interactive learning modules and online assessments.

Furthermore, school heads play a critical role in orchestrating professional development initiatives for teachers. This includes the arrangement of training modules, workshops, and seminars aimed at equipping educators with the requisite cybersecurity knowledge and pedagogical skills. By doing so, they not only enhance the teaching capabilities within their institution but also contribute to the broader goal of elevating Cybersecurity Education standards.

In addition, school heads are responsible for monitoring and evaluating the effectiveness of the curriculum's implementation. This entails the collection and analysis of various assessment metrics, such as student performance indicators, teacher engagement levels, and parental feedback. Such data-driven insights are crucial for making informed decisions on curriculum adjustments, additional resource allocation, and future scaling of the program.

In essence, school heads act as the linchpin in the Cybersecurity Educational ecosystem, overseeing the curriculum's successful integration, ensuring quality control, and fostering an environment conducive for both teaching and learning. Their leadership and managerial acumen are vital for the effective and sustainable adoption of this specialized cybersecurity curriculum, thereby fulfilling its educational objectives and societal imperatives.

6.1 Framework Dimensions

- The "Preventive Techniques" category provides children with basic protection across the identified action areas. For more in-depth coverage, the other extracted skills were grouped and divided into the following categories.
- "Malicious Code" refers to technical attacks and malicious software associated with cybersecurity challenges.
- "Fraud" includes fraudulent activities in which attackers use false or stolen information to steal financial or personal data or make illicit gains. This can include phishing, identity theft, social engineering, or fake websites. The primary goal is to gain access to data or cause financial harm.
- "Data privacy and awareness" refers to the careful handling of both one's own data and that of others. This category includes all measures and threats regarding privacy settings.
- The "Safety" category is an adaptation of the term e-safety. Here we have grouped together various topics, such as cyberbullying, netiquette and general rules that should be observed on the Internet.
- "Offensive & Abusive Content" covers dangers and challenges that occur due to offensive, inappropriate, or discriminatory content.

6.2 Framework Categories

Within these categories, we then subdivided according to the main categories of the NIST Framework for Cybersecurity: identify, protect, detect, respond, and recover, which are understood as action taxonomic fields.

- **Identify** (I) is about providing basic knowledge so that children and young people understand what the challenges and risks are in general.
- The **Protect** (P) category addresses the development and implementation of preventive protective measures to mitigate the identified challenges (I).
- **Detect (**D) refers to methods and mechanisms to detect security incidents when they occur or have occurred.
- **Respond** (Res) covers the ability to act and react after a security incident has been identified. The goal is to respond appropriately to an acute incident and eliminate the threat.
- The last stage, **Recover** (Rec), is about teaching children and youths' measures to restore the original state that existed before the security risk or infraction.

In the following, we have extracted the identified skills from the framework and clustered them. For a more in-depth look, the framework including all cybersecurity-relevant skills for children and adolescents between the ages of 8 and 13 can be found in the appendix.

7 The SCK EU reference framework (first version)

Pedagogical Interventions and Measures for the Protection of Children in the online Sphere

7.1 Preventive Techniques (PT)

PT - Module 1: Behaviours and Basics

- Children should be able to name the basic rules of safe behaviour on the Internet. (I)
- Children should be able to name the basics of computer networks. (I)
- Children should be able to identify potential unsafe domains. (D)
- Children should be able to determine whether a website is authenticated, e.g., by examining URLs. (D)
- Children should be able to use the reporting function. (Res)
- Children should be able to apply light backups (WhatsApp, iCloud, etc.). (Rec)

PT – Module 2: Passwords and Encryption

- Children should be able to explain safe practices, such as password creation, hashing, as well as authentication. (I)
- Children should be able to create strong passwords. (P)
- Children should be able to use strong passwords. (P)
- Children should be able to change their passwords (of accounts and devices) after a cyberattack. (Res/Rec)
- Children should be able to outline the basics of cryptography and encryption. (I)
- Children should be able to protect themselves from cyberattacks by using encryption technologies. (P)

PT - Module 3: Security Software

- Children should be able to name the benefits of antivirus software. (I)
- Children should be able to use and install security and antivirus software. (P)
- Children should be able to name the benefits of firewalls. (I)
- Children should be able to name the benefits of multi-factor authentication (MFA). (I)
- Children should be able to use multifactor authentication to protect themselves. (P)
- Children should be able to describe the potential consequences of disabling antivirus programmes. (P)
- Children should be able to use their security software. (P)
- Children should be able to apply preventive measures to ensure their PC is protected from a hacker attack. (P)

PT - Module 4: Data management and data protection

- Children should be able to name the benefits of data backups. (I)
- Children should be able to name the benefits of online storage systems for secure data exchange. (I)
- Children should use child-friendly web browsers. (I)
- Children should be able to make (regular) backups. (P)
- Children should be able to use online storage systems to share personal/sensitive data. (P)

PT - Module 5: Basics of security in social media and online communication

- Children should be able to name the benefits of e-safety application. (I)
- Children should be able to name potential dangers of social media sites and apps (I).
- Children should be able to identify suspicious chats or emails and delete them. (P)

- Children should be able to recognise and report suspicious content and people online. (Res)
- Children should be able to use backups too easily (WhatsApp, iCloud etc.) (Rec)

7.2 Malicious Code (MC)

MC - Module 1: Basics of Malware (Identify)

- Children should know what malware is.
- Children should have a basic understanding of computers and the internet.
- Children should know types of malwares (for example, viruses, worms, spyware, packet sniffers & loggers).
- Children should understand how malware works and how it affects data security and the computer.
- Children should be aware of methods of spreading malware, such as pop-ups, malicious websites and links.

MC - Module 2: Preventive Measures against Malware (Protect)

- Children should use strong passwords.
- Children should be able to install and use anti-virus software.
- Children should be able to use security software.
- Children should generally be able to recognise and delete suspicious content.

MC – Module 3: Detecting Malware (Detect)

- Children should be able to identify different forms of cyber-attacks.
- Children should be able to recognise secure websites (HTTPS).
- Children should be able to analyse and interpret security warnings.
- Children should be able to identify and avoid unsafe content, links and bait messages.

MC - Module 4: Responding to Malware (React)

- Children should be able to report cybercrimes and potential threats.
- Children should be able to disconnect from the internet after being attacked by malware.
- Children should be able to contact a trusted adult in response to threats.

MC - Module 5: Recovery from Malware (Recover)

- Children should be able to deal with negative online experiences.
- Children should be able to reset their mobile devices to factory settings.

7.3 Safety (ST)

ST - Module 1: Basics of online/offline Behaviour and Netiquette

- Children should have a basic understanding of online behaviour and netiquette. (I)
- Children should be aware of the basic dangers of communicating online (SNS, stranger risks, chat dangers, non-anonymity, the internet never forgets). (I)
- Children should understand the basics of cyber hygiene. (P)
    - Children should know how to communicate on the internet. (P)
    - Children should know how to handle and protect their devices and accounts. (P)
- Children should be able to recognise situations where they should contact a trusted adult. (D)
- Children should know how to ask for help and use appropriate IeT vocabulary. (Res)

ST - Module 2: Basic Understanding of Cyber Security

- Children should know what cyber security means and the different aspects of it. (I)

- Children should know how to surf the internet safely. (P)
- Children should have a basic understanding of which websites are safe and which are suspicious. (P)

ST - Module 3: Cyber-Bullying

- Children should know the basics of online bullying (e.g., do not engage in cyber-bullying, understand the role of an ‘upstander’ and ‘bystander’, recognise the feelings of others during bullying). (I)
- Children should know what action to take in case of cyber-bullying, both for themselves and for others.
- Children should know how to collect evidence, e.g., by taking screenshots or saving chat logs. (Res)

ST - Module 4: Online-Communication

- Children should avoid dangerous websites and chats. (P)
- Children should not trust everyone they meet online. (P)
- Children should not meet strangers they have met in chat rooms in real life. (P)
- Children should be aware of what they can and cannot post online. (P)
- Children should consider the consequences before becoming active on social networking sites. (P)
- Children should be aware of the emotional and physical sensations they may experience in dangerous situations online. (D)
- Children should not click on every link they receive. (P)
- Children should be able to report a situation or person if they feel unsafe. (Res)
- Children should know how to collect evidence, e.g., by taking screenshots or saving chat logs. (Res)

ST - Module 5: Online-Payments

- Children should know what it means to use their parents’ credit card. (I)
- Children should be able to distinguish between paid and non-paid services. (D)
- Children should know that they should not sign online contracts. (D)
- Children should be able to check security information and certifications when making online payments. (D)

7.4 Abusive Content (AC)

AC - Module 1: Raising Awareness of online Content Dangers

- Children should be aware of the dangers of the online sphere, including inappropriate content, intolerance, harm, violence, pornographic material, false information, hate speech and illegal material. (I)
- Children should be able to name the various dangers that occur, such as grooming, sexual assault and child prostitution. (I)
- Children should be able to recognise how a stranger might ask for certain personal information and understand the risks involved. (P)
- Children should be able to recognise whether a website is age appropriate. (D)

AC - Module 2: Self-Protection and Avoidance Behaviour

- Children should be equipped with self-protection strategies for dealing with online dangers, including ignoring or withdrawing from certain media. (P)
- Children should know how to avoid dangerous chats or websites. (P)
- Children should know the importance of using appropriate privacy settings to minimise the risks of social networking sites (SNS). (P)
- Children should be able to recognise online risks and cyberbullying and take steps to stay away from them. (D)

AC - Module 3: Responding to inappropriate Content and Bullying

- Children should have basic knowledge about inappropriate online content(I)
- Children should be familiar with age-appropriate responses to cyberbullying, including actions such as blocking or reporting. (P)
- Children should know how to respond appropriately if they come across something inappropriate online, such as inappropriate images or text. (P)
- Children should know how to respond to instances of cyberbullying, e.g., by closing the game or website and reporting the incident. (Res)

AC - Module 4: Reporting and Search for Help

- Children should be able to recognise "red flags" indicating possible dangers on the internet. (P)
- Children should be able to recognise unsafe content. (D)
- Children should be able to recognise online enticement and sextortion. (D)
- Children should know how to report situations where they feel unsafe. (P)
- Children should understand the importance of contacting an adult if they experience something strange or uncomfortable online. (I)
- Children should know how to help others who are in a similar situation by helping them to contact the appropriate adult or person. (Rec)
- Children should know who to contact if such a situation has occurred and where to seek help. (Rec)

7.5 Fraud (FR)

FR - Module 1: Basics of online Fraud (Identify)

- Children should know the basics of online fraud and its effects.
- Children are aware of types of online fraud including social engineering, phishing, smishing, spoofing, grooming, scams, and identity theft.
- Children are aware of different techniques that fraudsters use to cause harm, such as links, attachments, and fake websites.

FR - Module 2: Preventive Measures against online Fraud (Protect)

- Children should know measures to protect themselves from social engineering attacks.
- Children should be able to check the security information and certifications of online payments.
- Children should know how to handle links and attachments in emails from unknown senders.
- Children should be able to configure device settings for secure connections.

FR - Module 3: Detecting online Scams (React)

- Children should know "red flags" of untrustworthy people on the internet.
- Children should be able to assess whether a website is safe.
- Children should be able to recognise attempts at grooming.
- Children should be able to decide whether a payment is safe or not.
- Children should be able to recognise phishing emails.
- Children should know the feelings that can occur during online manipulation.

FR - Module 4: Responding to online Scams (Respond)

- Children should be able to report cyber-attacks and grooming attempts.
- Children should be able to change their passwords after phishing attacks.
- Children should be able to contact a trusted adult after they have been the victim of a scam.

FR - Module 5: Recover from online Scams (Recover)

- Children should be able to change passwords after a scam.
- Children should contact a trusted adult for assistance in restoring devices or accounts.
- Children should be able to reset mobile devices to factory settings.

7.6 Data Protection and Data Awareness (DP & DA)

DP & DA - Module 1: Recognise Data Protection (Identify)

- Children should know the basics of data protection, data security and specific terms of online data protection.
- Children should recognise risks in data use, such as streaming or social media.
- Children should not give out personal information or location data online.
- Children should be aware that once information is published, it is almost impossible to delete it.
- Children should know that there are privacy settings on social media to prevent or at least discourage unsolicited contact.

DP & DA - Module 2: Preventive Measures against Data Protection (Protect)

- Children should know how to create a guest account and a user account.
- Children should know age-appropriate examples of privacy protection and what information should and should not be shared online.
- Children should be able to use mechanisms to avoid privacy breaches (e.g., not sharing passwords, using privacy settings on websites or social media).
- Children should have an awareness and understanding of the different privacy settings and what they mean. For example, being able to prevent in SNS/cyberbullying risks or privacy violation risks in general.
- Children should know that they should change their passwords regularly.
- Children should know examples of appropriate information to post online and how to find out what is safe and what they should not post.
- Children should know mechanisms to protect their data and themselves (privacy and chat settings, clearing browser cache, blocking certain websites/people, limiting visibility of posts and comments/personal information, using a pseudonym online, etc.).

DP & DA - Module 3: Recognise Data Protection (Detect)

- Children should know techniques to recognise when personal data is unsafe. (e.g., by looking at a social media account "as a stranger would see it").

DP & DA - Module 4: Responding to Data Protection (React)

- Children should know mechanisms to destroy/delete information and protect their data.
- Children should know how to deal with a privacy breach and how to change their password.

DP & DA - Module 5: Restoring Data Protection (Restore)

- Children should know ways to respond if they have posted something inappropriate online.
- Children should know that they can turn to a trusted adult.

From the above measures, there is coverage across all relevant areas of cyber safety for children and young people aged 8-13 years identified in the systematic literature review area and the Delphi study.

8 How to use Game Based Learning in the Cyber security curriculum for 8–13-year-olds

Before an appropriate game can be selected to use in an educational context the teacher must answer two incredibly important questions. First what purpose does the game serve and second where is it going to be played (context of use)?

8.1 Game selection. Why do I want to use the game?

Marshev and Popov (1983) identified three purposes games could serve beyond entertainment. These were educational functions, research functions, and operational functions. The educational function is of course the one of most interest to the task at hand. The research function is more concerned with the verification of concepts and testing of ideas, whereas the operational is using games to construct plans etc. The educational function of games was further broken down into sub functions.

8.1.1 Educational functions

8.1.1.1 Demonstration

In this function the game is used in a similar way to a text. It demonstrates principles, concepts and systems that are needed to further understand. Where the game differs from a static text is in its interactivity and the ability of the student to explore multiple potential readings of the text.

8.1.1.2 Training function

The game serves as a practice space for the skills that the student is trying to learn. Games are especially suited to this type of learning as they offer a space with reduced consequences for failure. If a game is being selected to fulfil this function it is important that the game mirrors the real world as closely as possible. Flight and driving simulators are exemplars of this type of game function.

8.1.1.3 Motivation

The offer to play a game can be motivating. Teachers have often used the promise of games as a method to reward students' positive behaviour. If a game is being selected to fulfil this function, in a classroom the amount of engagement it generates is the primary consideration.

Games get the blood flowing; they can help to wake a person up and get them to start to think a bit more deeply. If a game is being selected for this function it should be a shorter game as arousal falls over time. The teacher can use this type of game as a warmup style activity to get the class to engage with the topic.

It is important to remember that the reasons for adopting a game can entail more than one function. So, for example, a game that is being used as a technological gateway should demonstrate the principles of use (demonstration) and allow the player to experiment and try using the system (training).

8.2 Games as assessment

The final function of games for learning of interest to teachers is the potential to use them as a form of assessment.

Before exploring how games can be used as an assessment tool there are some issues that must be addressed.

Games can only be used as a formal assessment if they produce some form of artifact. This artifact can be produced inside the game. In this case it may take the form of progression check points (did the student get past point x), trace data (recording of students playing either in video or in numerical abstraction), or in game questions. All these functions normally need to be incorporated into a game during the design stages of the game. The formal assessment may also take place external to the game. In this case it may take the form of quizzes etc. In both cases the artifact produced must be stored and available to both students and other stakeholders.

Games may lose some of their inherent learning value if they are too closely tied to summative assessment. One of the primary learning values of a game is that they allow a player to fail with reduced consequences. This encourages players to take risks, to test theories and to explore the system more freely. When consequences of a grade are added, the students are more likely to become risk averse, less creative in their responses, and more focused on goal completion than learning.

With these two caveats aside, games can offer excellent tools in assessment.

8.2.1 Games and formative assessment (informal assessment)

Games which have been selected for training are exceptionally well suited for formative assessment as they encourage trial and error. If a player is not able to get past a certain point they are encouraged to theorize as to why or to use meta learning strategies like asking for help to overcome the problem. Observation of game play and debrief by the teacher can further increase the value of the game as a formative assessment tool.

8.2.2 Games and summative assessment

There are two basic summative assessment forms that can be associated with games. These are assessments internal to the game and assessments external to the game.

Internal game assessment is most attempted through the use of stealth assessment. Stealth assessment is a process in which the player or student is not aware that they are being assessed. Putting aside the obvious ethical implications, there is a negative impact on learning if the student becomes aware that they are being manipulated and this almost certainly raises legal problems associated with capturing the actions of 8–13-year-olds online.

Then the teacher is left with the question: what (if any) features does this game have to collect the data? Most free to play serious games do not include the features necessary to capture in game play. In addition, it is important that the game not only captures the data of play but has some method of associating that data with a specific player. This requires a login system and data storage system that most serious game developers do not have the time or resources to develop or support.

Out of game assessment on the other hand can use standard assessment tools that teachers are already familiar with. In this form of summative assessment, the game acts as the text that the student has consumed. The teacher can then use quizzes, essays, interviews, reports, or any other assessment tool to test the student's comprehension of the materials presented. The validity and reliability of these tools will depend on the familiarity of the creator of the tool with the game it is being based on. In general, the more open ended the assessment, the easier it will be to create. Two examples are given below.

8.2.3 Quizzes (declarative knowledge)

In general, it is useful to ensure that this form of assessment focuses on what the player must learn in order to play the game successfully. In addition, questions should be avoided about content that might only be found in a side quest that players may have missed. When it comes to cybersecurity games, remembering who was upset because their phone was hacked, is of less value than a question about how their phone was hacked.

8.2.4 The Game report

If students are asked to produce a written or oral report on the game, careful consideration should be given to the rubric that will be used to assess the report. The rubric should be published beforehand so that students are aware of the criteria which they will be judged on so they can tailor their report accordingly.

8.3 Conclusions - games as assessment

While potentially valuable, in-game assessment is much rarer than the other forms of assessment. This is probably due to its problematic legal and ethical implications. It is also much more expensive for developers of the game to implement.

In contrast games are especially well suited to formative assessment methodologies. This is because they offer a view of a student actively engaging with the material that has been presented. However, this can be difficult to quantify and may not be regarded as appropriate in all of the EU educational contexts for which this project has been developed.

8.4 Games and their context of use

In the same way that the reason a game has been selected for use will impact its utility, so will how it be used. There are ais a variety of ways in which a player can interact with a computer game. This section will examine the most common interaction patterns that are used in serious games and make recommendations on how this pattern can be used inside a classroom.

In the following diagrams the arrows indicate the pathway of interactions, St stands for students and T stands for teachers.

8.4.1 Basic interaction pattern

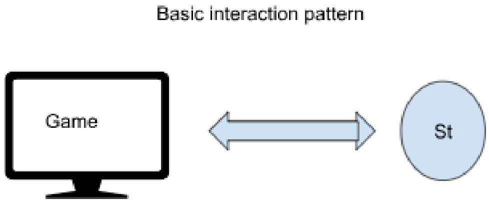


Figure 1. Basic Interaction Pattern.

This is the pattern that is most commonly associated with computer game play. The game is given to the student and the interaction is limited to just the student and the game. Each individual student has access to their own copy of the game and the technology to play it on. In education terms this is the pattern used when a game is assigned as homework, or played in a class while the teacher engages in other tasks. The issue from an educational standpoint is that the play is unmonitored, and the teacher needs to use quizzes or other assessment tools to ensure that the student has completed the activity satisfactorily (this could take the form of completion of the game or reaching some milestone inside the game). In addition, the student/player has no one to support them if they reach a stumbling point inside the game.

8.4.2 Teacher Monitored use

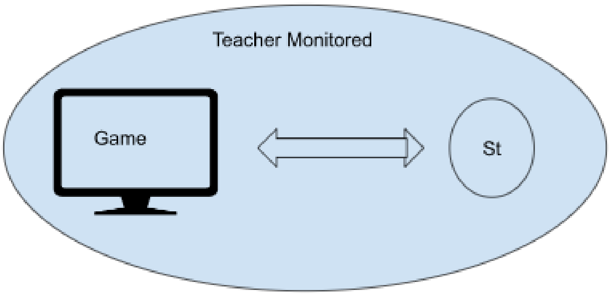


Figure 2. Teacher Monitored.

In this pattern the teacher observes the game during play. Each student has access to their own individual copy of the game and system required for play. It is important that the student is still the one who makes the decisions and interacts with the game systems, not that the teacher begins playing over the student's shoulder. In education this is the most commonly used format within classroom settings. The teacher is present to provide support for students who are having difficulty or to help to bring students back onto task. In this model the teacher can use observation to assess both the levels of engagement and student completion of tasks.

8.4.3 Group play

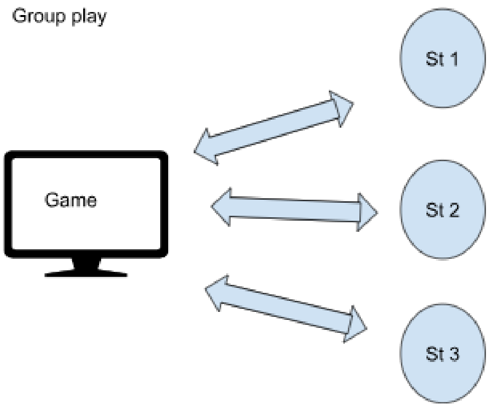


Figure 3. Group Play.

This is when two or more students share access to the copy of the game and the technology to play it on. This can be monitored by a teacher inside the classroom or unmonitored. In educational terms this is very useful if there are limited numbers of machines available. It also promotes conversation and discussion between the students engaging with the game. It is better suited for games which are being used as texts rather than being used as training for specific skills. It is also important for the teacher to monitor to ensure that one student does not dominate and ignores the others in the group.

8.4.4 Multiplayer

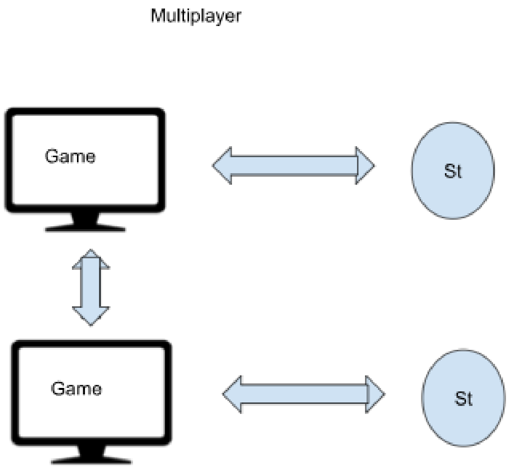
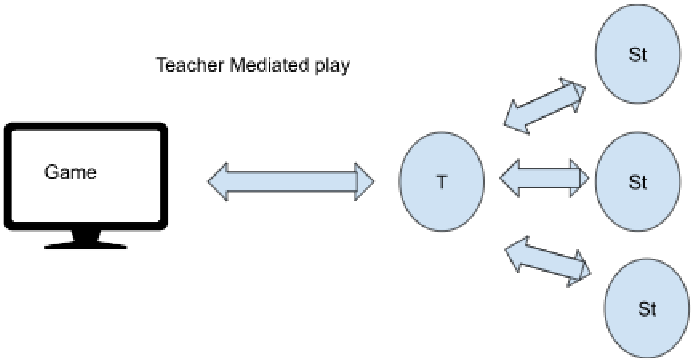


Figure 4. Multiplayer.

This is when two or more students have individual access to the game and digital device, but the machines are networked, so that the students can be present in the same game world. This is most commonly seen in the use of Minecraft in education or other multiplayer games. While it is a lot less common in serious games, the pattern has been included here for completeness. In a classroom setting this style of play can be monitored physically or via the teacher being present in the shared virtual space. If the teacher is monitoring physically (wandering around the classroom), attention should be paid to whether the students are on task and any emerging need for support. If the monitoring is being mediated by computer, the teacher can actively take part in the tasks that the students are engaged with. In this case, it is important for the teacher not to take over the tasks and to be aware of how the students are interacting.

8.4.5 Teacher mediated Play



In this pattern the students do not interact directly with the game; instead, the teacher acts as the interface with the computer. This form is only suited to an in-class context as access to the technology is prescribed. This form is very useful in sparking discussion and debates about the actions that players should take. It also reduces the number of technological resources needed to use the game for learning. This pattern is more useful for games that require strategic decisions and can be paused so that the decisions can be considered.

https://commons.wikimedia.org/wiki/File:EModule.png - CC BY-SA 4.0 DEED

8.5 Lesson walkthrough examples

8.5.1 Learning Design for a Lesson on "Basics of Online/Offline Behaviour and Netiquette" (From ST - Module 1 of the SCK EU Framework) with "SPOOFY"

Table 1. Lesson on "Basics of Online/Offline Behaviour and Netiquette" (From ST - Module 1 of the SCK EU Framework) with "SPOOFY"

Learning context	• Age Group: 8-10 years old • Class Size: 25 students • Duration: 45 minutes • Location: Classroom equipped with a projector and screen • Resources: Internet-connected computer for the teacher, Spoofy game with lesson materials, whiteboard
Objectives	• For School Heads: o Ensure that the lesson aligns with overall school objectives regarding online safety. o Confirm that the required technical resources, such as projectors and computers, are available and functional. • For Teachers: o Students should understand the basics of online behaviour and netiquette (Educational Function: Demonstration). o Students should be aware of the basic dangers of communicating online (Educational Function: Training). o Enhance participation and class discussion about online behaviour (Educational Function: Motivation).
Topic	• Basics of Online/Offline Behaviour and Netiquette
Lesson Flow	• For School Heads o Preparation: Verify that the classroom is technologically ready, with working projector and computer. o Support: Provide teachers with the Spoofy game's user guide and additional lesson materials. o Quality Assurance: Arrange for a post-lesson review to collect feedback on lesson effectiveness. • For Teachers o Introduction (5 minutes): Introduce the topic and its importance in cybersecurity. Discuss the objectives of the lesson. o Direct Instruction (10 minutes): Use a presentation to delve into the basics of online/offline behaviour and netiquette, including potential dangers. o Game-Based Learning Activity with Spoofy (20 minutes): ▪ Open the Spoofy game on the screen. ▪ Opt for an assignment in the game that ties well with the topic. ▪ Read the assignment out loud with the class. ▪ Discuss each player option with the class. ▪ Interaction Pattern: Teacher Mediated Play. o Class Discussion (5 minutes): After the game, initiate a discussion about what was learned and why netiquette is essential.

	○ Wrap-up (5 minutes): Summarize the key takeaways and inform students of future assessments on this topic.
Assessment	• For School Heads: ○ Ensure that teachers have access to other formative and summative assessment tools. • For Teachers: ○ Formative Assessment: Use the class discussion and interaction during the Spoofy game to gauge understanding and engagement. ○ Summative Assessment: Plan for a quiz or written assignment for a later class that tests the students' understanding of online/offline behaviour and netiquette.

8.5.1.1 An example with "SPOOFY"

An example of this play can work with the cyber security game Spoofy.

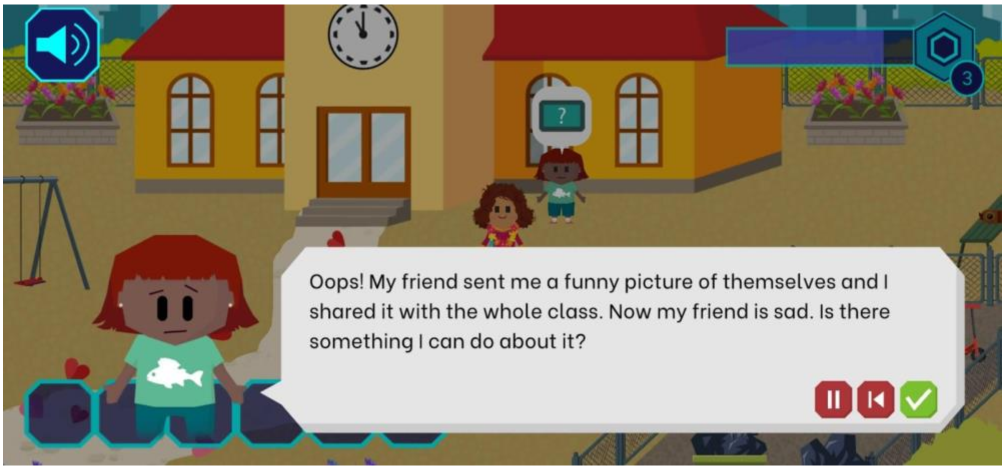
Preparatory Phase. Before initiating the classroom activity, the teacher invests time in meticulously planning the lesson. This involves identifying which topics within the domain of cybersecurity will be covered. The teacher also examines the additional lesson materials provided with the Spoofy game, selecting those that best complement the chosen topics. *Note for School Heads: Ensure that the selected lesson materials and topics align with the school's broader objectives regarding online safety. Verify that all required technical resources are functional prior to the lesson.*

Lesson Introduction (5 minutes). As students settle into the classroom, the teacher employs the projector to open the Spoofy game on the screen. The lesson kicks off with a brief introduction about the significance of the day's topic within the broader context of cybersecurity. The teacher outlines the learning objectives, thereby setting the stage for active engagement. *Note for School Heads: Ensure that the teacher has access to a user guide for Spoofy and any additional lesson materials to facilitate a smooth introduction.*

Direct Instruction (10 minutes). Transitioning to a formal presentation, the teacher explicates the rudiments of the topic, elucidating potential threats and why the chosen focus is pivotal. *Note for School Heads: Quality assurance can include a brief review of the presentation slides or teaching materials to ensure they are pedagogically sound.*

Game-Based Learning with Spoofy (20 minutes). Three steps:

1. Selection of Assignment: The teacher either preselects an assignment or lets the students choose.



Oops! My friend sent me a funny picture of themselves and I shared it with the whole class. Now my friend is sad. Is there something I can do about it?

Figure 5. SPOOFY. Screenshot.

2. Collective Reading: The assignment appears on the screen, and the class reads it aloud collectively.
3. Interactive Discussion: Each player option within the game is scrutinized, and a discussion ensues. The teacher discusses each player option together with the class: what do these options mean? What would be a good response? Why this response?

Note for School Heads: For quality assurance, consider observing this part of the lesson to evaluate both the effectiveness of the game-based learning activity and the degree of student engagement.

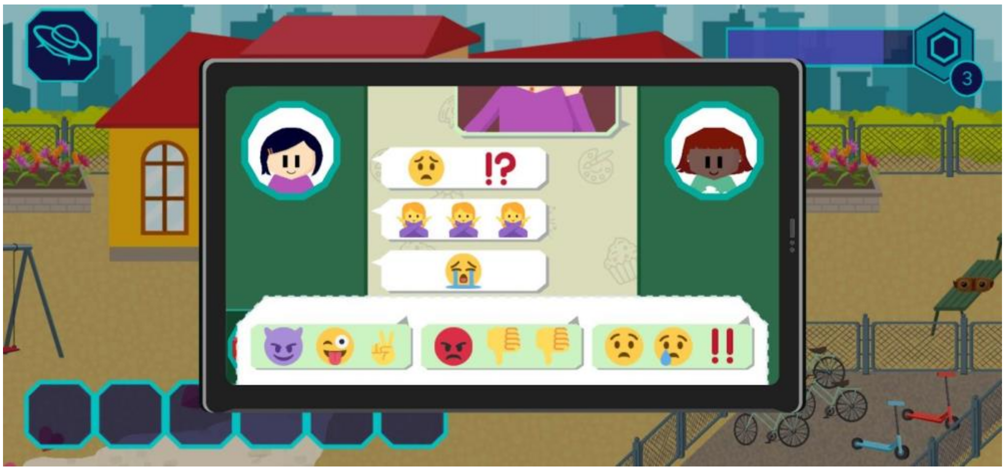


Figure 6. SPOOFY. Screenshot.

Class Discussion (5 minutes). Post gameplay, the teacher instigates a class-wide dialogue to recapitulate what has been gleaned. *Note for School Heads: It may be beneficial to collect feedback from students after the lesson, to be used for future improvements.*

Lesson Wrap-up (5 minutes). The teacher summarizes the salient points and informs the students of impending assessments that will test their comprehension. *Note for School Heads: Ensure that teachers have access to a variety of formative and summative assessment tools to accurately gauge the effectiveness of the lesson.*

This way allows the teacher to control the gameplay, include different children and make sure the lessons are learnt the way the teacher intends. It is a slower method than individual play but can be done at different lengths and as part of any class. In essence, this methodology allows the teacher to judiciously manage the gameplay, ensuring that pedagogical objectives are met while maximizing student involvement. The approach is flexible in duration and can be seamlessly integrated into the existing curriculum.

8.5.2 Learning Design for a Lesson on "Password and Encryption" (From PT – Module 2 of the SCK EU Framework) with "Nabbovaldo e il ricatto dal cyberspazio"

Table 2. Lesson on "Password and Encryption" (From PT – Module 2 of the SCK EU Framework) with "Nabbovaldo e il ricatto dal cyberspazio"

Learning context	• 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	• For School Heads: o Ensure that the lesson integrates seamlessly into the existing cybersecurity curriculum. o Confirm the adequacy of technical resources such as computers and game software. • For Teachers: o Students should be able to explain safe practices, such as password creation and hashing (Educational Function: Demonstration). o Students should be able to create and use strong passwords (Educational Function: Training). o Increase motivation and engagement in the subject matter (Educational Function: Motivation).
Topic	• Password and Encryption
Lesson Flow	• For School Heads o Preparation: Ensure that the computer lab is available and that the educational game software on password security is installed and functioning on all computers. o Support: Provide teachers with a quick guide on how to use the educational game and its features for assessment. o Quality Assurance: Schedule a post-lesson review with the teacher to gather feedback on the effectiveness and engagement levels of the lesson. • For Teachers o Introduction (5 minutes): Briefly introduce the topic and its importance in cybersecurity. Explain the learning objectives. o Direct Instruction (10 minutes): Use a presentation to explain the basics of strong passwords, hashing, and encryption. Highlight the dangers of weak passwords. o Game-Based Learning Activity (20 minutes): ▪ 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. o Class Discussion (5 minutes): After the game, facilitate a class discussion about what they learned, what was surprising, and why strong passwords are crucial. o Wrap-up (5 minutes): Summarize key takeaways and inform students that they will be assessed on this topic in a future lesson.
Assessment	• For School Heads: o Ensure that the game software has built-in analytics to track student progress for formative assessment. o Ensure that the teachers have access to external assessment tools like quizzes for summative assessment. • For Teachers: o Formative Assessment: Utilize the game's analytics to monitor which students were able to successfully create strong passwords during the game.

	o 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.

8.5.2.1 An example with "Nabbovaldo e il ricatto dal cyberspazio"

An example of this play can work with the cyber security game Nabbovaldo.

Preparatory Phase. Before initiating the classroom activity, the teacher gives the pupils the task of playing Nabbovaldo at home, in single-player mode. Furthermore, the teacher invests time in meticulously planning the lesson. This involves identifying which topics within the domain of cybersecurity will be covered. The teacher also examines the additional lesson materials provided with the game, especially the Teacher's Guide (available on Ludoteca del Registro .its website), selecting those that best complement the chosen topics. *Note for School Heads: Ensure that the selected lesson materials and topics align with the school's broader objectives regarding online safety. Verify that all required technical resources are functional prior to the lesson.*

Lesson Introduction (5 minutes). As students settle into the classroom, the teacher employs the projector to open the Nabbovaldo game on the screen. The lesson kicks off with a brief introduction about the significance of the day's topic within the broader context of cybersecurity. The teacher outlines the learning objectives, thereby setting the stage for active engagement. *Note for School Heads: Ensure that the teacher has access to a user guide for Nabbovaldo and any additional lesson materials to facilitate a smooth introduction.*

Direct Instruction (5 minutes). Transitioning to a formal presentation, the teacher explicates the rudiments of the topic, elucidating potential threats and why the chosen focus is pivotal. *Note for School Heads: Quality assurance can include a brief review of the presentation slides or teaching materials to ensure they are pedagogically sound.*

Game-Based Learning with Nabbovaldo (30 minutes). Three steps:

1. Opening of the video Game Chapter on IWB: The teacher announces the chosen scene on the Map.
2. Brief discussion in class: The chosen scene and characters appear on the screen, and the teacher asks children how much they believe these elements are related to the day's topic. This narrative approach (the game is an adventure) is possible thanks to the visual power of the videogame, built on metaphors around the domain of cybersecurity.
3. Shared Gaming Session: The players take turns using IWB, while the teacher discusses each player option together with the class: What does this character represent? What about his/her behaviour? What is the meaning of this word? In particular, the discussion focuses on the options given in the Dialogues and on the Definitions of the Nabbopedia encyclopedia.

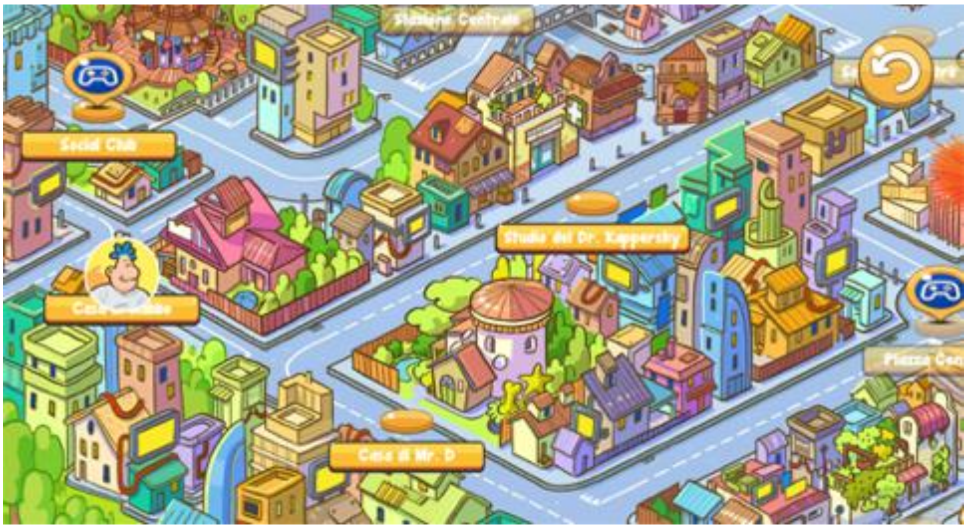
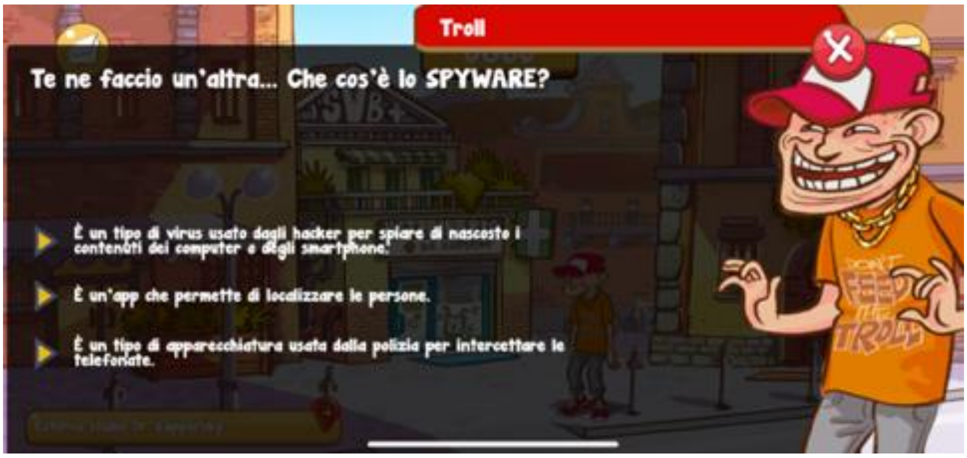


Figure 7. Nabbovaldo e il ricatto dal cyberspazio. Screenshot.

In-depth activities (10 minutes): Starting from the references of the Teacher's Guide, the teacher shows a short video or suggests a group activity (i.e., crossword puzzle, anagrams, simulation games). All these activities have the aim of further fixing the concept encountered in the game chapter and chosen scene.



Te ne faccio un'altra... Che cos'è lo SPYWARE?

- È un tipo di virus usato dagli hacker per spiare di nascosto i contenuti dei computer e degli smartphone.
- È un'app che permette di localizzare le persone.
- È un tipo di apparecchiatura usata dalla polizia per intercettare le telefonate.

Figure 8. Nabbovaldo e il ricatto dal cyberspazio. Screenshot.

Class Discussion (5 minutes). Post gameplay, the teacher instigates a class-wide dialogue to recapitulate what has been gleaned. *Note for School Heads: It may be beneficial to collect feedback from students after the lesson, to be used for future improvements.*

Lesson Wrap-up (5 minutes). The teacher summarizes the salient points and informs the students of impending assessments that will test their comprehension. *Note for School Heads: Ensure that teachers have access to a variety of formative and summative assessment tools to accurately gauge the effectiveness of the lesson.*

This way implies that the children have already played at home. The activity carried out in classroom by the teacher therefore provides an important moment to establish and deepen the concepts, as in "flipped classroom" method. This methodology allows the teacher to judiciously manage the gameplay, ensuring that pedagogical objectives are met while maximizing student involvement. The approach is flexible in duration and can be seamlessly integrated into the existing curriculum.

8.6 Recommendations for designing a lesson on Cybersecurity

8.6.1 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.

8.6.2 For Teachers

- Content Variables:
    - 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 PT, MC, ST, AC, FR, DP & DA.
- 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.

9 Final remarks

In conclusion, the establishment of an EU reference framework for integrating a game-based learning ecosystem on cybersecurity into the curriculum for schoolchildren is of significant importance. However, it is crucial to approach this with an interdisciplinary lens, considering pedagogical, ethical, and legal aspects. While the framework holds the promise of advancing Cybersecurity Education, ongoing research and evaluation are essential for its continual refinement and effectiveness.

The SCK Framework emerges as a pivotal reference model that could significantly influence the standardization of Cybersecurity Education across European educational systems. The framework's comprehensive structure and adaptability make it a robust tool for integrating Cybersecurity Education into existing curricula while addressing the unique educational objectives, content variables, and assessment metrics of different educational settings.

For school heads, the SCK Framework offers a standardized point of reference for curricular development and strategic planning. By aligning with this framework, school heads can adopt a unified approach that is both rigorous and adaptable. For instance, the framework's focus on age-appropriate topics and evaluation methods could be integrated into national or regional educational standards, thereby ensuring a level of uniformity in Cybersecurity Education across Europe. This would also facilitate cross-border collaborations and exchange programs, enhancing the quality and reach of Cybersecurity Education at a continental level.

For teachers and educators, the SCK Framework provides a rich repository of pedagogical resources and teaching strategies. The framework's modular design allows for flexibility, enabling educators to tailor their cybersecurity lessons to fit the broader educational context and the specific needs of their students. For example, an educator in Estonia teaching about online safety could utilize the framework's guidelines and resources to develop an interactive lesson that incorporates national cultural nuances, while a teacher in Germany could adapt the same guidelines to focus on data protection laws specific to that country.

Moreover, the framework's emphasis on diverse assessment methods aligns well with the ongoing European efforts to develop comprehensive educational evaluation standards. Schools could employ the SCK Framework's multi-faceted assessment approach, including knowledge quizzes, practical exercises, and behavioural assessments, to gauge students' cybersecurity competencies and adjust educational strategies accordingly.

In conclusion, the SCK Framework's structured yet flexible design makes it a viable candidate for serving as a European reference model in the integration of Cybersecurity Education into existing curricula. By adopting this framework, European educational systems can ensure a consistent, high-quality, and culturally sensitive approach to Cybersecurity Education, thereby equipping the younger generation with the essential skills and ethical understanding needed to navigate an increasingly interconnected and complex digital landscape.

10 References

Abt, C. C. (1987). *Serious games*. University Press of America.

Amo, L., C., Liao, R., Frank, E., Rao, H., R. & Upadhyaya, S. (2019). Cybersecurity Interventions for Teens: Two Time-Based Approaches. *IEEE Transactions on Education*, *62*(2), 134–140. https://doi.org/10.1109/TE.2018.2877182

Anastasiades, P. S. & Vitalaki E. (2011). Promoting Internet safety in Greek primary schools: The teacher's role. *Journal of Educational Technology & Society*, *14*(2), 71–80.

Anderson, L. W. & Krathwohl, D. R. (2001). A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. New York: Longman.

Antunes, M., Silva, C., & Marques, F. (2021). An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Applied Sciences*, *11*(23). https://doi.org/10.3390/app112311269

Berson, I. R., Berson, M. J., Desai S., Falls, D., & Fenaughty, J. (2008). An Analysis of Electronic Media to Prepare Children for Safe and Ethical Practices in Digital Environments. *Contemporary Issues in Technology and Teacher Education (CITE Journal)*, *8*(3), 222–243.

Bloom, B.S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain.

Buchanan, L., Scarlatos, L. & Telendii, N. (2021). *Curriculum to Broaden Participation in Cybersecurity for Middle School Teachers and Students*. 63–70. https://doi.org/10.1109/ISEC52395.2021.9763930

Burkett, R. (2013). *An Alternative Framework for Agent Recruitment: From MICE to RASCLS*. *57*(1).

Carretero, S.; Vuorikari, R. and Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use, EUR 28558 EN, doi:10.2760/38842

Council of Europe. Council for Cultural Co-operation. Education Committee. Modern Languages Division. (2001). Common European framework of reference for languages: Learning, teaching, assessment. *Cambridge University Press.*

CBR Staff. (2019, November 7). Europe's Cybersecurity Skills Gap Has Doubled: Report. *Tech Monitor.* https://techmonitor.ai/technology/cybersecurity/cybersecurity-job-gap

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. In *Computer Science Review*. Elsevier. https://doi.org/10.1016/j.cosrev.2021.100361

Cranmer, S., Selwyn, N., & Potter, J. (2009). Exploring Primary Pupils' Experiences and Understandings of `e-Safety'. *Education and Information Technologies*, *14*(2), 127–142. https://doi.org/10.1007/s10639-008-9083-7

CYBERHEAD - Cybersecurity Higher Education Database. (n.d.). [CYBERHEAD Map]. ENISA. Retrieved October 29, 2023, from https://www.enisa.europa.eu/topics/education/cyberhead

Cyber Kill Chain®. (n.d.). Lockheed Martin. Retrieved May 6, 2023, from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Cybersecurity Workforce Study. (2022). Retrieved October 31, 2023, from https://www.isc2.org/research

DeFranco, J. F. (2011). Teaching Internet Security, Safety in Our Classrooms. *Techniques: Connecting Education and Careers*, *86*(5), 52–55.

Economou, A., (2023). SELFIEforTEACHERS Toolkit - Using SELFIEforTEACHERS, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/626409, JRC129699

EPRS - European Parliamentary Research Service, Binder K., (2023). "Progress on the European Commission's 2021-2027 digital education action plan". European Parliament Briefing paper PE 745.689 – March 2023. © European Union. Retrieved 05-06-2023 at https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)745689

European Commission (2022). Discover the Digital Potential of Your School – SELFIE Questionnaires (EN). Retrieved 07-06-2023 at https://education.ec.europa.eu/sites/default/files/2022-07/SELFIE_Questionnaires_EN.pdf

European Commission (2021). SELFIE Guide for School Coordinators. Retrieved 07-06-2023 at https://education.ec.europa.eu/document/setting-up-selfie-in-your-school-detailed-guide-for-selfie-school-coordinators

European Commission, Directorate-General for Education, Youth, Sport and Culture, (2023). What can schools do about bullying?, Publications Office of the European Union, https://data.europa.eu/doi/10.2766/809742

European Commission, Directorate-General for Education, Youth, Sport and Culture, (2021). Blended learning for high quality and inclusive primary and secondary education – Handbook, Publications Office of the European Union, https://data.europa.eu/doi/10.2766/237842

European Commission, (2020). Digital Education Action Plan 2021-2027: Resetting education and training for the digital age. Retrieved 05-06-2023 at https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0624

European Commission, Directorate-General Education, Youth, Sport and Culture, Unit B.2: Schools and multilingualism (2020). Blended learning in school education – guidelines for the start of the academic year 2020/21. Retrieved 07-06-2023 at: https://www.schooleducationgateway.eu/downloads/Blended%20learning%20in%20school%20education_European%20Commission_June%202020.pdf

European Commission, Joint Research Centre, Punie, Y., Pujol Priego, L., Carretero, S. et al., (2018). DigComp into action, get inspired make it happen – A user guide to the European Digital Competence framework, Punie, Y. (editor), Carretero, S. (editor), Vuorikari, R. (editor), Publications Office, https://data.europa.eu/doi/10.2760/112945

European Union Agency for Cybersecurity, ECSF, (2022). European cybersecurity skills framework, https://data.europa.eu/doi/10.2824/859537

European Union Agency for Cybersecurity. (2022). *ENISA threat landscape 2022: July 2021 to July 2022*. Publications Office. https://data.europa.eu/doi/10.2824/764318

European Union Agency for Cybersecurity (ENISA), (2022). User Manual, ECSF - European Cybersecurity Skills Framework. ISBN: 978-92-9204-583-8 – DOI: 10.2824/95989

Finkelhor, D., Jones, L., & Mitchell, K. (2021). Teaching privacy: A flawed strategy for children's online safety. *Child Abuse & Neglect*, *117, 1-5*. https://doi.org/10.1016/j.chiabu.2021.105064

Fujikawa, M., Ikehara, H., & Abe, Y. (2020). SNS Education Game for Upper-Grade Elementary School Students: Evaluation of Prototype. *Proceedings of the 2020 8th International Conference on Information and Education Technology*. 137–141. https://doi.org/10.1145/3395245.3395248

Fujikawa, M., Kanou, R., Itoh, A., & Abe, Y. (2019). Development of an SNS Education Game for Higher-Grade Elementary School Children. *Proceedings of the 10th International Conference on E-Education, E-Business, E-Management and E-Learning*. 130–134. https://doi.org/10.1145/3306500.3306501

Graafland, J. H. (2018). New Technologies and 21st Century Children: Recent Trends and Outcomes. *OECD Education Working Papers, No. 179. OECD* Publishing, 1–60. https://doi.org/10.1787/e071a505-en

Hammond, S.P., Polizzi, G. & Bartholomew, K. (2023) Using a socio-ecological framework to understand how 8–12-year-olds build and show digital resilience: A multi-perspective and multimethod qualitative study. *Educ Inf Technol* **28**, 3681–3709. https://doi.org/10.1007/s10639-022-11240-z

Hudson, C. C., Lambe, L., Pepler, D. J., & Craig, W. M. (2016). Coping While Connected: The Association among Cybervictimization, Privacy Settings, and Reporting Tools in Youth. *Canadian Journal of School Psychology*, *31*(1), 3–16. https://doi.org/10.1177/0829573515619623

IEEE Draft Standard for Age Appropriate Digital Services Framework—Based on the 5Rights Principles for Children. (2021). *IEEE P2089/D4, September 2021*, 1–60.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150–158. https://doi.org/10.11591/edulearn.v12i1.7736

Joint Research Centre, Institute for Prospective Technological Studies, Devine, J., Punie, Y., Kampylis, (2015). Promoting effective digital-age learning – A European framework for digitally-competent educational organisations, Publications Office, https://dx.doi.org/10.2791/54070

HSE cyber-attack: Irish health service still recovering months after hack. (2021, September 5). *BBC News*. https://www.bbc.com/news/world-europe-58413448

Kenny, M. C, Long, H., Billings, D., & Malik F. (2022). School-based abuse prevention programming: Implementation of child safety matters with minority youth. *Child Abuse Review*, *31*(3). https://doi.org/10.1002/car.2742

Kilavo, H., Kondo, T. S, & Hassan, F. (2022). The impact of teaching computer programming in Tanzanian primary schools. *INTERACTIVE LEARNING ENVIRONMENTS*. https://doi.org/10.1080/10494820.2022.2115078

Klabbers, J. H. G. (2006). *The magic circle: Principles of gaming & simulation* (Third ed). Sense Publishers.

Konak, A. (2014). A cyber security discovery program: Hands-on cryptography. *IEEE Integrated STEM Education Conference*. 1–4. https://doi.org/10.1109/ISECon.2014.6891029

Kralj, L. (2014). *Children's safety on the Internet-development of the school curriculum*. 593–596. https://doi.org/10.1109/MIPRO.2014.6859637

Kralj, L. (2016). E-SAFETY AND DIGITAL SKILLS AS PART OF SCHOOL CURRICULUM. *Medijske Studije = Media Studies*, *7*(13), 59–75. https://doi.org/10.20901/ms.7.13.4

Kritzinger, E. (2015). *Enhancing cyber safety awareness among school children in South Africa through gaming*. 1243–1248. https://doi.org/10.1109/SAI.2015.7237303

Kritzinger, E. & Padayachee, K. (2013). *Engendering an e-safety awareness culture within the South African context*. 1–5. https://doi.org/10.1109/AFRCON.2013.6757708

Lancia, F. (2012). T-lab Pathways to Thematic Analysis. Retrieved 15-06-2023 at: https://mytlab.com/tpathways.pdf

Martínez-de-Morentin, J. I., Lareki A., & Altuna, J. (2021). Risks Associated With Posting Content on the Social Media. *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje*, *16*(1), 77–83. https://doi.org/10.1109/RITA.2021.3052655

MITRE ATT&CK®. (n.d.). Retrieved November 19, 2021, from https://attack.mitre.org/

Nicolaidou, I. & Venizelou, A. (2020). Improving Children's E-Safety Skills through an Interactive Learning Environment: A Quasi-Experimental Study. *Multimodal Technologies and Interaction*, *4*(2), 10. https://doi.org/10.3390/mti4020010

Piccolo, L. S., Godoy, T. P., & Alani, H. (2021). *Chatbots to Support Children in Coping with Online Threats: Socio-Technical Requirements*. 1504–1517. https://doi.org/10.1145/3461778.3462114

Pooja, R. P. & Shashidhar R. (2022). EVALUATION OF STUDENTS' AWARENESS TOWARDS CYBER SECURITY. *Phronimos*, *2*(4), 33–40.

Reeder, J. R., & Hall, T. (2021). Cybersecurity's Pearl Harbor Moment. *The Cyber Defense Review*, 25.

Redecker, C. (2017). European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

Standards National Institute of & Technology. (2017). *Digital Identity Guidelines: NIST SP 63a*. CreateSpace Independent Publishing Platform.

Scheibe, M., Skutsch, M., & Schofer, J. (1975). Experiments in Delphi methodology. In H. A. Linestone & M. Turoff (Eds.), The Delphi method - techniques and applications. 262–287. Boston, MA: Addison-Wesley.

Shen, L. W., Mammi, H. K. & Din, M. M. (2021). *Cyber Security Awareness Game (CSAG) for Secondary School Students*. 48–53. https://doi.org/10.1109/ICoDSA53588.2021.9617548

Toledo, W., Louis, S. J. & Sengupta, S. (2022). NetDefense: A Tower Defense Cybersecurity Game for Middle and High School Students. *2022 IEEE Frontiers in Education Conference (FIE)*. 1–6. IEEE https://doi.org/10.1109/FIE56618.2022.9962410

Vinayakumar, R., Soman, K. P. & Menon, P. (2018). *Digital Storytelling Using Scratch: Engaging Children Towards Digital Storytelling*. 1–6. https://doi.org/10.1109/ICCCNT.2018.8493941

Vuorikari, R., Kluzer, S. and Punie, Y., (2022). DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415

Weeden, S., Cooke, B., & McVey, M. (2013). Underage Children and Social Networking. *Journal of Research on Technology in Education*, *45*(3), 249–262. https://doi.org/10.1080/15391523.2013.10782605

Willard, N. (2012). Cyber savvy: Embracing digital safety and civility. Corwin Press.

Wishart, J. M., Oades, C. E., & Morris M. (2007). Using online role play to teach internet safety awareness. *COMPUTERS & EDUCATION*, *48*(3), 460–473. https://doi.org/10.1016/j.compedu.2005.03.003

Witsenboer, J. W. A., Sijtsma K., & Scheele F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *COMPUTERS & EDUCATION*, *186*. https://doi.org/10.1016/j.compedu.2022.104536

Yu, W. D., Gole, M., Prabhuswamy, N., Prakash, S. & Shankaramurthy, V. G. (2016). An Approach to Design and Analyze the Framework for Preventing Cyberbullying. *2016 IEEE International Conference on Services Computing (SCC).* 864–867. IEEE https://doi.org/10.1109/SCC.2016.125

Zichermann, G., & Cunningham, C. (2011). *Gamification by Design.* O'Reily.