



Empowering children online: a holistic skills framework for cybersecurity

Nicolai B. Plintz¹ · Dirk Ifenthaler^{1,2}

Received: 13 March 2025 / Accepted: 7 October 2025
© The Author(s) 2025

Abstract

As a part of the Erasmus+ funded project Super Cyber Kids, we have devised a skills framework to enhance the protection of children aged between 8 and 13 years in their Internet and online activities. The framework was developed through a systematic literature review, followed by a two-round Delphi study for validation. During this process, we identified $N=40$ relevant studies and obtained validation from up to $N=18$ professionals in cybersecurity, education, and cybersecurity education during the Delphi study. The resulting framework is presented as a matrix and offers a comprehensive set of skills aligned with the NIST (National Initiative for Cybersecurity Education) cybersecurity framework, specifically tailored to promote cybersecurity awareness among children in this age group.

Keywords Cybersecurity · Online safety · Children · Systematic review · Delphi study

Introduction

Every 11 s, an organization falls victim to a ransomware attack, and tragically, many of these cyberattacks prove to be successful. As of 2021, the global damage from cyberattacks is estimated to reach a staggering 5.5 trillion Euros (Baldini et al., 2020), which continues to rise steadily. Concurrently, cybersecurity-related issues, such as cyberbullying, are increasing (Santre, 2023). In light of these trends, it is essential to define cybersecurity clearly. Cybersecurity encompasses all measures required to safeguard cyberspace, its users, and affected individuals from cyber threats (ENISA, 2017). A particularly vulnerable user group comprises children and adolescents who remain inadequately protected from these threats (Quayyum et al., 2021; Rahman et al., 2020). For this reason, educating children about potential cybersecurity risks is essential while providing them with countermeasures and prevention techniques (Quayyum et al., 2021). Current research focuses on

✉ Nicolai B. Plintz
nicolai.plintz@uni-mannheim.de
Dirk Ifenthaler
dirk@ifenthaler.info

¹ Learning, Design and Technology, University of Mannheim, L4, 1, 68161 Mannheim, BW, Germany

² Curtin University, Perth, Australia

areas in which children and young people should be protected, such as cyberbullying, cryptography, or handling social media (Baciu-Ureche et al., 2019; Vanderhoven et al., 2016; Weeden et al., 2013; Zhu et al., 2021), yet specific actions are rarely discussed. Available holistic work also tends to identify scopes of action and related curricular content for this age group (Sağlam et al., 2023). However, there is currently no comprehensive and age-appropriate overview of relevant cybersecurity skills. Such an overview is essential to provide practitioners, parents, and curriculum designers with a foundation that can achieve comprehensive protection for children. In response, we conducted a systematic literature search and subsequently sought validation from professionals in cybersecurity, education, and cybersecurity education to identify these essential skills. For that reason, the Super Cyber Kids initiative is strategically aligned with the European Commission's Digital Education Action Plan 2021–2027 and is specifically designed to address the gap in cybersecurity education for children in the late primary education (8–10 years old) through to the early middle school years (10–13 years old).

Literature review

In the digital age, children are exposed to various online threats (Quayyum et al., 2021). The threats and cyber risks that children face cover a wide range and encompass multiple dangers such as grooming (Ringenberg et al., 2022), cyberbullying (Zhu et al., 2021), privacy threats (Buchanan et al., 2021), and exposure to inappropriate online content like contact with strangers, sexual messaging, content with violence or racism as well as pornography (Kenny et al., 2022; Livingstone & Smith, 2014; Livingstone et al., 2014), among many others. The initial problem with these threats is that the definition of risk often varies, and it is increasingly difficult to classify them accurately (Ibrahim et al., 2024; Ringenberg et al., 2022; Finkelhor et al., 2021; Cranmer et al., 2009; Stoilova et al., 2021; Tokunaga, 2010). In general, grooming can be understood as a process by which a potential adult abuser befriends a child to gain the child's trust and get them into abusive activities (Gillespie, 2002). Another type of threat emerging from online interaction with other people is cyberbullying. According to Tokunaga (2010), cyberbullying can be defined as any behavior by individuals or groups using electronic or digital media that repeatedly communicate hostile or aggressive messages intended to cause harm or discomfort to others. Additionally, privacy threats are defined as potential dangers that can affect the right of individuals, groups, or institutions to decide for themselves to what extent they share information about themselves with others (Westin, 1967). To ensure protection against these online threats, several frameworks address prevention and protection measures. However, most of these frameworks are designed for adults and companies.

These threat categories and measures, designed for organizations, may not sufficiently address children's particular vulnerabilities and needs.

The National Institute of Standards and Technology (NIST) framework (2024) is a multifaceted and adaptable framework designed to enhance organizations' cybersecurity posture. At its core, the framework is structured around five key functions: Identify, Protect, Detect, Respond, and Recover. These functional dimensions are crucial in safeguarding organizations against online risks and threats. Unfortunately, a large part of the NIST framework cannot be applied directly to children as it is too technical and complex for this age group. For instance, databases, networks, and software need to be identified and protected in an organizational context. This includes threat and vulnerability analysis and

risk assessment of these resources—requirements that are specific to organizations (NIST, 2024). Children, on the other hand, face other, simpler but no less dangerous threats for their age group.

While existing frameworks provide valuable foundations, they present significant limitations for children aged 8–13. For instance, the NICE Framework focuses primarily on workforce development with technical competencies for organizational cybersecurity roles UpGuardProcomservices might be inappropriate for young learners. Cyber.org's K-12 framework, while comprehensive in scope, lacks specific validation and detailed skill breakdowns for the critical 8–13 age group. The European Cybersecurity Skills Framework (ECSF) defines 12 professional role profiles that emphasize professional competencies rather than age-appropriate foundational skills. Most critically, existing frameworks either focus on technical workforce preparation or remain too broad across all school ages without addressing the unique developmental needs, limited abstract reasoning capabilities, and specific online threats that characterize the 8–13 age group. Therefore, a specialized framework validated specifically for this vulnerable population is essential. For this reason it is important to create a holistic overview that specifically addresses the threats children face online while considering the various reasons for attacks or cyber risks, including financial gain, entertainment (Chang et al., 2023), narcissism (Tanrikulu & Erdur-Baker, 2021) and in general that children considered as a particularly vulnerable group (Chang et al., 2023). Given these unique vulnerabilities and the distinct nature of online threats targeting children, our study aims to explore the necessary skills that are required to be fully covered in the area of cybersecurity for children aged eight until 13. Specifically, we aim to address the following research questions:

RQ1: What are the specific cyber security skills for children in the age range between 8 and 13 that are identified in the scientific literature and professionals' opinions?

RQ2: Which cybersecurity skills are targeted by the learning opportunities provided through games and platforms mentioned in studies on cybersecurity education for children?

RQ3a: How can the identified skills be categorized in a structured manner?

RQ3b: How can a structured framework be developed by integrating the dimensions of the NIST Framework with the potential identified cybersecurity categories for children aged 8–13?

The individual research questions act as necessary intermediaries that help answer the broad research question RQ3b by integrating the dimensions of the NIST framework with the identified cybersecurity categories for children ages 8 to 13.

Method

We deployed a two-phase approach consisting of a systematic literature review and validation through a two-round Delphi study to answer the research questions and create a holistic and comprehensive skill framework.

Systematic literature review

The systematic literature review followed largely the PRISMA statement (Preferred Reporting Items for Systematic Reviews and Meta-analysis; Page et al., 2021) and targeted the age group of 8–13-year-old children, focusing on relevant cybersecurity skills. Leading databases in the fields of IT, education, and psychology were used for the literature search.

The following databases were consulted: ACM Digital Library, ACM Guide to Computing Literature, ERIC, IEEE Xplore, Web of Science, and PsycINFO.

Search criteria

Three subject areas have been connected using an AND parameter for the search. One is the subject area (cybersecurity), the target group (8–13-year-olds), and the output (skill). Therefore, the following search strategy was implemented to search:

1. Cybersecurity and synonyms

“cybersecurity” OR “Cyber-security” OR “cyber security” OR “cybersecure*” OR “cyber-secure” OR “cyber safety” OR “cyber-safety” OR “cyber awareness” OR “Cyber-awareness” OR “IT-Security” OR “IT Security” OR “IT-Secure*” OR “IT Secure*” OR “Information security” OR “information technology security” OR “digital security” OR “digital-security” OR “digital-safety” OR “digital safety” OR “Online security” OR “online-security” OR “online safety” OR “E-Safety” OR “Online Security” OR “Computer security” OR “Computer-security”.

2. Target group

“Primary School*” OR “Elementary School*” OR “grade school*” OR “lower school*” OR “grammar school*” OR “Secondary Schools” OR “middle school” OR “prep school” OR “Preparatory School” OR “Secondary aged” OR “primary aged*” OR “intermediate school*” OR “child*” OR “young people” OR pupil* OR kids.

Later added: K12.

3. Output

Framework OR “Frame of reference” OR “Set of skill” OR Skillset OR Competenc* OR Instruction* OR Skill*.

Inclusion and exclusion criteria

The search covered scientific literature published until February 2025. The inclusion criteria consisted of the following: (a) a focus on cybersecurity or measures to decrease cybersecurity-related risks, (b) mention of methods or skills, whether implicit or explicit, that enhance the understanding, knowledge, or awareness of the target group, and (c) inclusion of at least a specific age group to some extent. The exclusion criteria consisted of the following: (a) Pure implications for parents, (b) books, (c) articles that are not written in the English language, and (d) thesis. Furthermore, it also leads to exclusion (e) if the skills mentioned are inappropriate for the age group. If there was an overlap of age groups, for example, 4–18 years, these were initially included, and later, only the relevant skills for the target group were included. Specifically, (f) studies were excluded if they did not contain any skills for the target group. With the abovementioned criteria, we identified a total of $N=398$ studies from the database search. After cleaning the duplicates, $N=315$ remained, and after the title and abstract search, $N=160$ were left. In addition, $N=5$ studies were added to the reference list. After performing the full-text search, $N=39$ suitable studies

remained. In addition, $N=5$ games and $N=3$ platforms were identified as the basis for skill extraction. Figure 1 shows a detailed overview of the search process. From the remaining $N=39$ papers, we extracted (a) potential risks, challenges, and threat areas; (b) skills and games as well as platforms with specific content; and (c) interaction parties.

During the revision process, we transformed all extracted items into actionable skills. The original literature used varying formulations to describe children's cybersecurity competencies (e.g., "should know that", "are aware that", "can do", "should not"). To ensure consistency and systematic comparison, all statements were standardized in the format "Children can...", while preserving the original intent and meaning of each study's

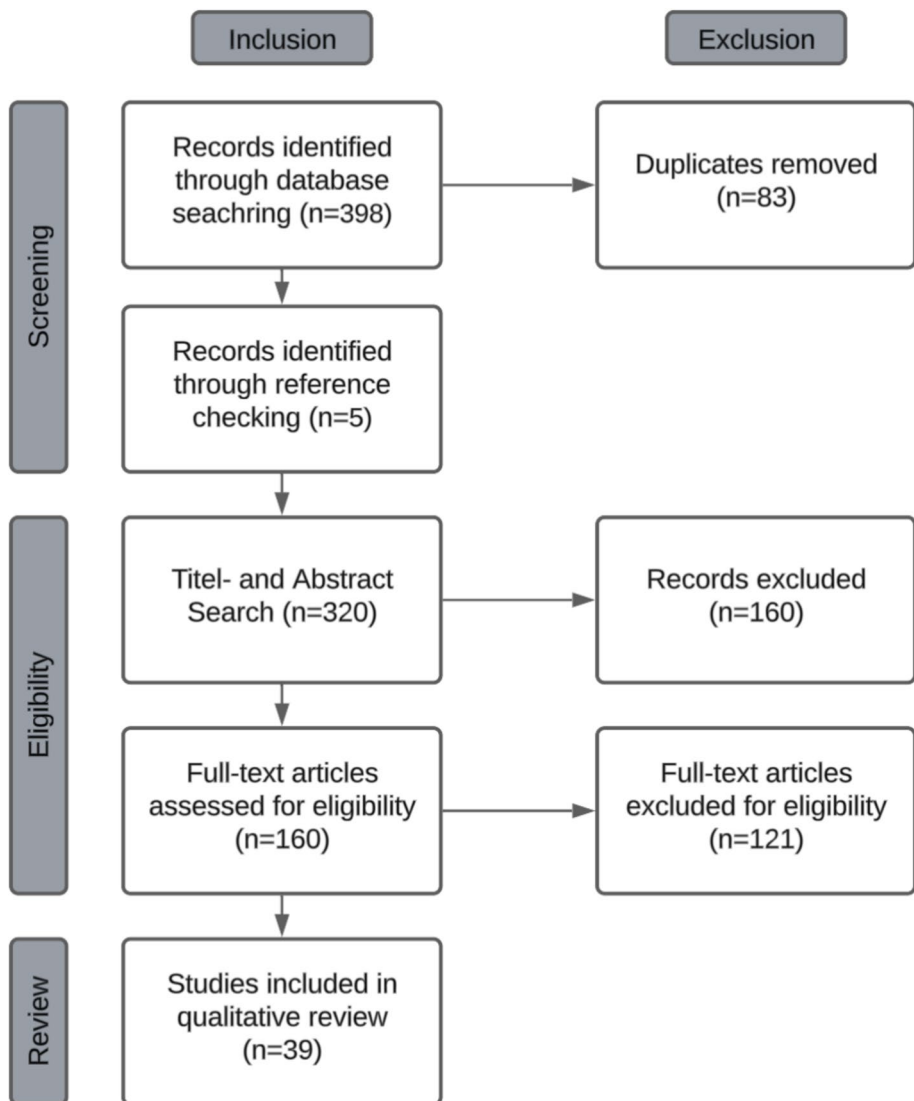


Fig. 1 Flow diagram of the systematic review process

findings. Items that originally described knowledge or awareness were reformulated as demonstrable capabilities (e.g., “Children can recognize that malware exists”), while action-oriented statements were maintained as “Children can [perform action]”. This ensures the framework focuses on practical abilities rather than theoretical knowledge. This ensures the framework focuses on practical abilities rather than theoretical knowledge. After completing the skill extraction and the transformation process, we categorized the skills into Identify, Protect, Detect, Respond, and Recover based on the NIST framework. We selected the NIST framework dimensions based on their structural and taxonomic sequence that remains logical and comprehensible for children. The five-stage progression from Identify through Protect, Detect, Respond, to Recover provides an intuitive learning pathway that can be translated into age-appropriate learning objectives while maintaining compatibility with the established NIST standard.

This adaptation required recontextualizing each dimension from organizational to child-oriented applications, following a pedagogically informed sequence: Identify builds fundamental awareness that online threats exist in general; Protect provides general protective measures and theoretical knowledge for threat recognition; Detect develops concrete skills to recognize when personally affected by a threat; Respond offers specific actions children should take when threats are identified; and Recover guides methods to restore safety after being affected by an incident. For example, while organizational “Protect” encompasses technical safeguards and policies, the children’s “Protect” dimension focuses on preventive behaviors, password hygiene, and privacy settings management. Our adapted NIST dimensions were treated as approximate taxonomies. The ‘Identify’ category encompassed fundamental knowledge and action-oriented skills. The ‘Protect’ dimension comprises general and specific measures to ensure preventive cybersecurity protection. The ‘Detect’ category included specific measures to identify the need for cybersecurity actions. ‘Respond’ refers to the skills necessary to respond to recognized threats, and the final dimension encompasses skills that contribute to restoring the original state. Afterward, the extracted skills were divided into six portions and proper categories: Malicious code, frauds, preventive technologies, abusive content, safety, and data privacy and awareness. The final result is a matrix-shaped framework with 30 fields comprising the NIST dimensions (X-axis) and the categories extracted from the literature (Y-axis).

Characteristics of included studies

For the systematic literature review, various study types were examined and included in the analysis. A total of five intervention studies were identified, while the majority consisted of survey studies ($n=9$) and evaluation studies ($n=4$). Additionally, the review incorporated two mixed-methods studies, two qualitative studies, two (systematic) literature reviews, and eleven conceptual studies. Further included were one comment, one quasi-experimental study, one comparative study, and one validation study. The analyzed studies were predominantly published in journals, with 26 journal articles, alongside eleven conference papers and two strategy papers. The publication years range from 2006 to 2025, with notable contributions in 2016 ($n=5$), 2021 ($n=7$), and 2024 ($n=5$). Geographically, the studies span multiple countries, with the majority originating from the USA ($n=12$), followed by the UK ($n=4$). Japan, Canada, Croatia, South Africa, Australia, and Malaysia each contributed two studies, while single studies came from France, the Netherlands, India, the Czech Republic, Poland, Greece, Portugal, Cyprus, Spain, Taiwan, and Turkey.

Delphi-study

To validate the skills described in the literature and to extend the skills framework, we conducted a two-round Delphi study (Scheibe et al., 1975). While the typical Delphi process often involves three rounds, it can also be undertaken successfully with only two rounds (Roberson et al., 2005; Scheibe et al., 1975; Skulmoski et al., 2007). The typical characteristics of a Delphi study, such as conducting several rounds, anonymity of the participants, feedback loops, and striving for consensus, were considered in our study (Scheibe et al., 1975; Skulmoski et al., 2007). In the first round, we anonymously asked a group of professionals to identify the essential skills for the 8–13 age group in the area of cybersecurity from scratch. Subsequently, the identified skills were clustered, merged with the results from the literature, and presented to the participants as feedback in the second round to check the completeness and appropriateness of the skills for the target group. The study, conducted using Microsoft Forms, involved 18 professionals from the fields of cybersecurity ($n=6$), cybersecurity education ($n=5$), and general education ($n=6$), with one additional participant from another area. The participants, hailing from countries including Estonia, Germany, Italy, the USA, France, and Hungary, had varying levels of professional experience. In cybersecurity education, the 5 participants had an average of 15.2 years of experience, ranging from 4 to 19 years. The six participants in cybersecurity averaged 14.5 years, ranging from 5 to 21 years. Those in general education also totaled six, with an average experience of 14.83 years, ranging from 5 to 35 years. Regarding educational qualifications, six participants held a PhD, eleven had a university degree, and one person had a high school diploma. The median age of the participants fell within the 40–49 age group.

Round 1: generating skills through the subject matter professionals

In the first round, the $N=18$ professionals were asked to provide demographic information and identify skills children between the ages of 8 and 13 should have in cybersecurity. The professionals' answers were expected to be formulated starting with "Kids can do" and describe the skills that, in their opinion, are of great significance. The professionals identified over 100 skills that might be required. These results were mapped and incorporated into the framework for the second round.

Round 2: validation of the existing framework

In the second round, participants were provided with each of the thirty matrix fields consisting of the NIST dimensions (Identify, Protect, Detect, Response, and Recovery) as well as the action fields we identified (Malicious Code, Fraud & Preventive Technologies, Abusive Content, Safety, Data Privacy & Awareness) and asked to evaluate whether the skills were appropriately related to content and age, as well as comprehensive. This part also included annotating incorrect or inapplicable skills and adding missing skills via a free text field. For this purpose, the participants were provided with four links to evaluate the individual fields of the matrix: Link 1: Malicious code ($N=17$); Link 2: Frauds & Preventive Technologies ($N=14$); Link 3: Abusive Content & Safety ($N=13$); Link 4: Data Privacy & Awareness ($N=14$). To distribute the workload for the participants, we gave them different links in a randomized order. Only Malicious Code was the link to the evaluation of this

category for all participants. Therefore, the number of professionals per category varied. Based on the results from the second round of the Delphi study, the research team incorporated final adjustments to the framework.

Results

RQ1: What are the specific cyber security skills for children in the age range between 8 and 13 that are identified in the scientific literature and professionals' opinions?

From the systematic literature review, we initially extracted over 500 skills from different scientific papers, games as well as the platforms mentioned in those. After excluding those that were not age-appropriate and removing duplicates, $N=257$ relevant skills remained. In addition to the skills from the scientific literature, the professionals identified $N=101$ skills in the first round of the Delphi study. The skills identified by the SLR and the professionals in the first round of the Delphi study range from rather general and superficial skills to specific skills. The results are shown in Tables 1 and 2.

RQ2: Which cybersecurity skills are targeted by the learning opportunities provided through games and platforms mentioned in studies on cybersecurity education for children?

Different games and platforms are mentioned in the literature. Some of them still exist today, while others no longer do. Berson et al. (2008) identified and compared various platforms and games. Over a decade later, Shen et al. (2021) adopted a similar approach. They compared the games based on gamification elements, topics, and components to create a more comprehensive game called Cyber Security Awareness Games (CSAG). In general, the games differ in terms of quality, purpose, and content. While some games only deal with a specific area of cybersecurity for children, such as Anti Phishing Phil, which specializes in phishing, or CyberCiege, which is dedicated to computer and network security, other games try to cover several categories and areas, like CyberAware (Giannakas et al., 2015; Khan et al., 2022). The areas of the games and platforms are listed in Table 3. It is noticeable that cyberbullying, privacy and personal information, as well as netiquette and social media, occur more frequently.

RQ3a: How can the identified skills be categorized in a structured manner?

Once all the skills had been classified along the adapted NIST dimension, the next step was to create various categories. To do this, frameworks and skills classifications mentioned in the literature were first considered to make a potentially existing classification. The criteria for the categories were based on a possible adaptation to the age group 8–13 years, so frameworks, categories, and subject areas from adult education or the private sector were also considered. One possible classification was according to knowledge, attitude, and behavior, focusing on password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting

Table 1 Excerpt from the systematic literature search

Author(s)	Examples
Amo et al. (2019)	Children can decide whether a website is safe or suspicious Children can recognize that phishing, networking, and cryptography concepts exist
Anastasiades and Vitalaki (2011)	Children can recognize that internet risks, such as misleading or inappropriate information on the web, can appear
Antunes et al. (2021)	Children can recognize the importance of online privacy settings
Baciu-Ureche et al. (2019)	Children can identify if a network connection is secure (HTTPS)
Becta (2006)	Children can recognize that they may be exposed online to illegal material, such as images of child abuse
Buchanan et al. (2021)	Children can create a safe password Children know that they should change their passwords after phishing attacks arises
Cranmer et al. (2009)	Children can recognize that they can have guidance from teachers to decide if a website is age appropriate
Dönmez et al. (2017)	Children can use the internet in an appropriate way for searching educational content and information regarding education
Fujikawa et al. (2019)	Children can recognize and respect their own rights and those of others regarding private information
Hammond et al. (2022)	Children can accept negative online experiences Children can report users
Hudson et al. (2016)	Children can recognize that privacy settings (e.g., on social media) and other privacy skills are helpful in preventing harm
Hudson et al. (2015)	Children can recognize how to limit the visibility of posts and comments on SNS
Kenny et al. (2022)	Children can recognize that once they post something on the internet, they cannot delete it forever with a click
Kralj (2014)	Children can recognize that they should not share harmful photos of others
Kritzinger (2015)	Kids should manage their online profiles by privacy settings
Kritzinger and Padayachee (2013)	Children can recognize the dangers they are subjecting themselves to by using services on the internet (e.g., posting personal information on social media, sharing pictures, texting strangers on the internet, free apps, etc.)
Beranek (2009)	Children can recognize that malware (e.g., viruses, worms, Trojan Horses) exists
Nicolaidou and Venizelou (2020)	Children can use a pseudonym in online discussion forums to protect their personal data
Shen et al. (2021)	Children can recognize that phishing exists as an online threat
Skinner (2016)	Children can use different and strong passwords
Toledo et al. (2022)	Children can recognize different types of cyber-attacks
Wishart et al. (2007)	Children can recognize that they shouldn't give out personal data online
Witsenboer et al. (2022)	Children share their experience with a trusted adult if something strange happened online
Weeden et al. (2013)	Children can recognize the importance of creating privacy settings, assessing other online risks, and preventing cyberbullying
Blinder et al. (2024)	Children can deal with online information appropriately. information (derived from Would you rather give a stranger your house key OR let a stranger read your diary?)
Graafland (2018)	Children can distinguish fiction from fact

Table 1 (continued)

Author(s)	Examples
Kralj (2016)	Children can respond appropriately if someone treats them in a hurtful and nasty way over the Internet or mobile phone
Martin et al. (2024)	Children can make smart choices about what to share with others
Martínez-de-Morentin et al. (2021)	Children can be careful about risk actions linked to what they publish online
Paudel & Al-Ameen (2025)	Children can recognize the importance of secure habits like creating strong passwords or recognizing suspicious activities online
Pooja & Shashidhar (2022)	Children can recognize password security
Tomczyk (2024)	Children can install software on mobile devices Children can configure internet access regarding confidential information
Tseng et al. (2022)	Children can regularly back up their mobile phone

Table 2 Excerpt of the first round of the Delphi study

- Children can differentiate between artificial and human-generated media
- Teenagers, mainly, can deactivate parental control for their tablets
- Children can understand many things and services online despite the fact that sometimes they are in other languages (e.g., even though they do not know English very well, while surfing they have the ability to do many things online)
- Children can identify cyber grooming attempts
- Children know that the “hacker” is not a hero
- Children can identify fake or doctored images
- Children can set their mobile devices to factory settings
- Children can distinguish Wi-Fi networks

Table 3 Platforms and games mentioned in the cybersecurity context

Name	Type
Hector’s World (Cyberbullying, Online security, Privacy and personal information)	Platform
Safe Online Surfing (Online-Behavior, Nettiquette, Smart Sharing, Protection against predators, Secure Systems, surf securely)	Game
CyberAware (protection of Internet-connected devices; safeguarding passwords; privacy issues; identity protection; safeguarding personal information online)	Game
Anti Phishing Phil (Phishing)	Game
NetSmartzKids (Cyberbullying, Live Streaming, Sexting, Smartphones, Gaming, Online Enticement, Sextortion, social media)	Platform
BrainPop	Game and Platform
Disney Surf Swell Island (privacy, viruses, or netiquette (guidelines for behavior on the Internet)	Game
beSeen (social network, secure personal and private info, protecting their online reputation, and defending peers)	Game and Platform
CyberCiege (computer and network security)	Game

(Parsons et al., 2014). Another framework is the eCSIRT.net Framework (Antunes et al., 2021), which was adjusted by ENISA (ENISA, 2018) to train people in the field of cybersecurity.

The categories abusive content, malicious code, information gathering, intrusion attempts, intrusions, availability, information content security, frauds, vulnerability, and other tests appear in this classification. Another grouping strategy could be to proceed according to existing curricula. The K-12 Cybersecurity Learning Standards (Anderson et al., 2021) could be considered. This curriculum contains three different pillars: computer systems, digital citizenship, and security. Computing Systems tend to refer to technical components such as computing and networking, as well as hardware and software.

Digital Citizenship, on the other hand, covers more general rules of behavior and dealing with cyberbullying in the category of 'online safety' (Anderson et al., 2021; Toledo et al., 2022). In addition to frameworks, games, and curricula, various topics are covered in the different papers. Some papers focus exclusively on the area of e-safety (Cranmer et al., 2009; Kenny et al., 2022; Kritzinger & Padayachee, 2013), Cyberbullying (Tanrikulu & Erdur-Baker, 2021; Santre, 2023) or social networks (Fujikawa et al., 2019, 2020). This diversity of topics, as well as the different clustering and inconsistent definitions, make it quite difficult to categorize them into existing classifications. Especially the definitions of terms are challenging. For instance, the term e-safety is used in similar contexts but is often very nebulous (Cranmer et al., 2009). The same picture seems to be repeated across most areas. For example, Finkelhor et al. (2021) note that there is also no uniform definition of privacy. They use components that they integrate into the area, such as identity theft, cyber-harassment, sexual predators, and damage to reputation.

There is also a lack of clarity in the definition of the term cyber-hygiene in academic research (Vishwanath et al., 2020). This seems to be a recurring theme. For this reason, the extracted skills were analyzed with a focus on their practical applicability for teachers, as well as on the coverage of the core topics from the areas of technical, legal, and social risks, with a view to the potential creation of curriculum units. After considering the individual papers, frameworks, and curricula, it was initially possible to divide them into more technical challenges and more non-technical measures. For example, these can be divided into computer networks (Amo et al., 2019), malicious code (Antunes et al., 2021), cryptography (Konak, 2014), abusive content (Kenny et al., 2022; Livingstone et al., 2014) and frauds (Antunes et al., 2021; ENISA, 2018), e-safety (Cranmer et al., 2009; Kenny et al., 2022; Kritzinger & Padayachee, 2013) or general behavior on the internet (Anastasiades & Vitalaki, 2011). In addition, some sources seem to focus more on the threats and how to deal with them (e.g., Kenny et al., 2022; Ringenberg et al., 2022; Santre, 2023), while others are more concerned with protection (e.g., Hudson et al., 2015; Konak, 2014). After a thorough analysis of all available information, consisting of various frameworks, existing scientific literature, and curricula, it became clear that it is essential to consider not only technical risks but also behavior-oriented risks and consider them when forming categories. For these reasons, the following categories were selected:

- **Malicious code:** In the area of malicious code, a basic understanding of malware, existing technical threats, and how to deal with them should be taught.
- **Frauds:** In the area of frauds, the basic awareness of fraud and how to deal with it should be created.
- **Abusive Content:** In the area of abusive content, a basic understanding of the types and handling of harmful or (age-)inappropriate content that may occur in cyberspace should be provided.

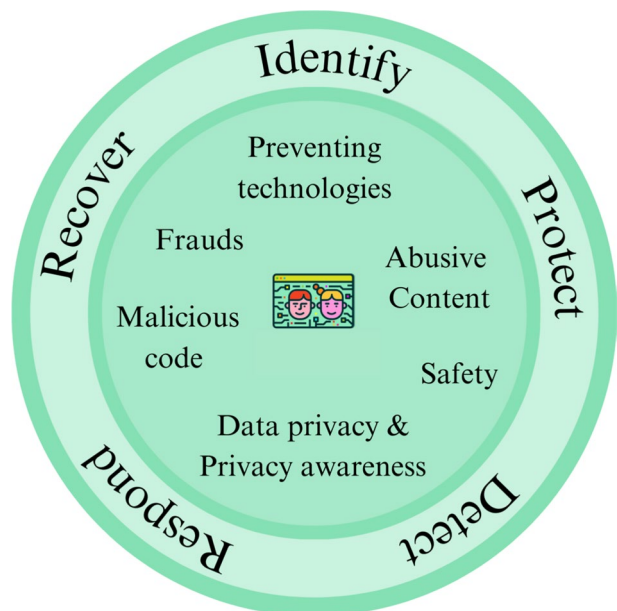
- **Preventing Technologies:** In the area of Preventing Technologies, a basic awareness of technologies that can protect them should be created.
- **Data Privacy and Awareness:** In the area of data privacy and awareness, an awareness of the handling and protection of personal data and privacy should be created, as well as an awareness of how to handle data.
- **Safety:** In the area of safety, a basic awareness of general safety practices, dealing with cyberbullying, and using the internet and digital devices should be taught.

Figure 2 shows the dimensions and categories that were processed into a matrix. After this matrix was created, the skills were subdivided and ranked by two independent researchers.

RQ3b: How can the identified cybersecurity skills for children aged 8–13 be integrated into a matrix-based skill framework using the dimensions of the NIST framework and our identified dimensions?

To answer this research question, two independent raters classified the skills, which we extracted from the scientific literature, the first round of the Delphi study, and the games and platforms into the matrix-based framework. We subsequently gave the professionals each of the 30 fields for evaluation, asking them to assess them for completeness, age appropriateness, and correct categorization. The final result of this process can be seen in Fig. 3.

Fig. 2 Design of the skills framework for cybersecurity



Conclusion and scientific significance

In this study, we developed a skill framework tailored to children aged 8–13, encompassing a comprehensive selection of skills extracted from scientific literature, cybersecurity games, and an online platform. To ensure the framework's validity, we conducted a two-round Delphi study, following the robust approach outlined by Scheibe et al. (1975) for

SKF Framework	Identify	Protect	Detect	Respond	Recover
Malicious code	Children can recognize... - that malware exists as a general online threat - that there are different types of malicious software (viruses, worms, spyware, trojans) - that hackers use malware to damage data and steal personal information - that malware can reach computers through various entry points - that infected files can cause computers to malfunction or stop working - that packet sniffing is a threat on unsecured wireless networks - that keyloggers can secretly record what they type - that pop-ups and malicious links are common unsafe content examples - that the internet and computers have basic vulnerabilities that can be exploited - that malware can have serious effects on their devices and personal data - that malicious websites can be designed to steal data or install malware - that email attachments can contain hidden malware	Children can... - apply basic security measures like strong passwords, antivirus software, and secure connections - apply safe email practices by avoiding suspicious attachments and unknown senders - apply careful browsing habits by reading before clicking on links - apply secure Wi-Fi practices by avoiding unsecured networks - that packet sniffing is a threat on unsecured wireless networks - use secure password creation techniques - use safety checks before downloading or opening files - avoid clicking on suspicious links without verification - avoid connecting to unsecured wireless networks - avoid visiting potentially dangerous websites, apps, or links	Children can... - spot signs of cyber attacks - identify whether a website is authenticated or not - recognize different forms of cyberattacks and cybercrime - identify when a network connection is secure (HTTPS) or not - discuss examples of unsafe content, such as pop-ups and malicious links - evaluate alarm messages and security alerts appropriately - recognize unsecured environments (websites, apps, links) and identify 'bait' messages to understand what they agree to by clicking	Children can... - report cybercrime - respond to potential threats online - respond to malware or cyberattacks by consulting a trusted adult - contact the right people and know how to react to cyberattacks and cybercrime - understand basic attacks they might be victims of and know what to do, specifically who to turn to - recognize when they need help with online predators and know who to turn to for help	Children can... - accept negative online experiences - cope with negative experiences and avoid them in the future - reset their mobile devices to factory settings
Data Privacy & Awareness	- that personal data protection is necessary - that they need to keep private data safe - that there are consequences of exposing personal data - that passwords can help to protect computer files and information - the concept of online privacy and that there are different levels of privacy - what possibly happens when they post a comment in a social media app - how to authenticate - the basics of an individual account in an app - security risks when streaming - that engaging in the illicit downloading of copyrighted materials is not appropriate - that a person can be identified by knowing only a few pieces of information about them, and that they must therefore be careful about what information they provide online - what forms 'personal information' can take - how to identify different types of personal information that may be elicited in the online environment - some of the techniques that are used in the online environment to elicit their personal information - how to demonstrate an awareness of why it may be unwise to disclose their personal details online - about disclosure of personal information and commercial exploitation - how to understand and respect their own rights and those of others regarding private information - what personal information and safety procedures are - how to classify personal data - that they shouldn't post their location online - the concept of privacy of personal data of third parties - the concept of digital footprints - that once they post information on the internet it can't ever truly be erased - the security issues caused by social media usage - about privacy settings and what they entail - that someone they don't know can send them a private message or direct message - their rights (e.g. on their own picture) - what information they can share - the concept of copyright - how copyright relates to fair use - examples of how fair use can help protect an author/creator's rights while promoting the sharing of ideas - that downloading copyrighted materials e.g. music and films can be risky - about sharing and authoring rights	- handle their own personal data responsibly - distinguish between private and public information by discussing age-appropriate examples of privacy, what is okay to share about themselves, and how that relates to confidentiality - distinguish which data to share or provide online and which to withhold - decide whether posting information is appropriate or not - decide whether to give out personal data without parental permission - decide whether it is appropriate to post their location online - protect their personal data in an online context - protect their digital identity by knowing what information to share online and what not to share - create and manage secure user accounts (e.g., guest accounts) with strong passwords for different purposes (social media vs. school accounts) and multi-factor authentication when available - prevent themselves from sharing school passwords with classmates and keep all passwords confidential - set and manage privacy settings across different platforms and services to minimize social network risks, avoid online enforcement and extortion, and stay safe during gaming - regularly check the privacy settings of their social media accounts - use privacy settings on social networking sites for reporting, blocking, and saving their data - use online privacy settings as a preventive measure to decrease the likelihood of being cyberbullied in the future - limit the visibility of posts, comments, and personal information on social media platforms - avoid giving out personal data and information to unknown sources - avoid posting everything on the internet and understand the consequences - avoid sharing private or personal information about themselves or others with strangers - react appropriately if a stranger asks for personal information - use a pseudonym in online discussion forums to secure their personal data effectively - clean their browser cache regularly for privacy protection - use online storage systems to exchange and keep personal or sensitive information securely - be aware of online privacy and understand different levels of privacy - understand the implications of posting a comment on a social media app - demonstrate an understanding of why it may be unwise to disclose personal details online - understand that privacy settings allow users to limit who can access the content they share online (e.g., pictures, comments, personal information) - update their computer when security warnings appear - destroy or erase information and protect data appropriately when necessary	- recognize when websites, apps, programs, or emails request personal data that should not be given out - provide examples of how copyright equates to ownership, such as "Who wrote the document," "Anything I create that is new to the world is mine," and "I need to give credit to any content not created by me."	- cope with negative experiences - understand how to destroy or erase information and protect their data appropriately	- know how and who to turn to for help if they receive inappropriate content from an adult or face a cyberbullying threat - know how to react if they accidentally send out an inappropriate picture - understand how they might assist others who are feeling sad or upset due to online threats
Frauds	- about phishing and what it entails - the basics of social engineering attacks - that email phishing attacks are possible - about pharming and what it entails - that grooming exists - the meaning of grooming - that using communication technologies can lead to sexual assault and/or child prostitution - about loggers and what they entail - about smishing - about botnets and what it entails - about scams (commercial and financial) and what they entail - about identity theft and what it entails - about online predators and what this entails - about spoofing and what it entails	- maintain integrity and confidentiality against web tracking and phishing - check the security information and certification of online payments - avoid clicking on links in emails from strangers - avoid opening email attachments from unknown senders - adjust settings on their phone to prevent automatic connection to insecure wireless networks - use strategies for handling suspicious attachments	- recognize red flags from untrustworthy people in the online world - determine if a website is safe to register on - identify cyber grooming attempts - decide whether or not to make an online payment - identify unsafe content online - recognize a phishing email - detect online enticement and sextortion by discussing online manipulation - name the feelings they may experience when dealing with something or someone untrustworthy	- report an impostor - report cyber attacks - respond appropriately to grooming - change their password after a phishing attack - contact a trusted adult if they experience fraud	- change their passwords after falling victim to a scam - know who to ask for help to recover their device or account - reset their mobile devices to factory settings

Fig. 3 Final skills framework for cybersecurity

Preventing technologies	- that password vulnerabilities exist that make passwords necessary - that weak passwords create security dangers - that security threats exist that require strong passwords - that threats exist that make enhancing security necessary (e.g. secure passwords, not clicking links) - that vulnerabilities exist that passwords help protect against in computer files and information - that security threats exist that require secure use of technology (passwords to antivirus) - that threats exist that security software is designed to prevent - that network vulnerabilities exist that need to be understood - that security threats exist that cryptography can protect against - that attacks exist that firewalls are designed to prevent - that online threats exist that make child-appropriate web browsers and SMS necessary	- use and install security or antivirus software - use passwords effectively - choose strong passwords - protect their mobile devices and computers - distinguish between different Wi-Fi networks - secure data on the internet by using strong passwords, hashing, and authentication - protect themselves from hackers or attackers who aim to damage important data and obtain private information by using safe passwords, antivirus software, and encryption - protect systems from attacks by using encryption techniques - make backups and understand the importance of backups - create a safe password by using a combination of letters, numbers, and symbols - use online storage systems to exchange and keep personal or sensitive information securely - understand the effects of disabling the antivirus system - grasp the basics of computer networks - update security software regularly - understand important terms related to password management - avoid viruses by deleting suspicious emails from their PC and using an antivirus system - back up their data regularly - use e-safety applications designed for kids - keep their passwords confidential - block other cyber user if necessary - take steps to prevent their PCs or other devices from being hacked, such as setting strong passwords - protect themselves by using multi-factor authentication (MFA)	- decide if a website is authenticated or not - identify a potentially problematic domain by scanning network protocols - check the URL of a website if there is any suspicion	- locate and use reporting functions for online problems - recognize when to change their password after experiencing a phishing or cyberattack - change passwords on their tablets/mobile phones easily	- make light backups as a preventive technique (e.g., WhatsApp chats, iCloud, etc.) - understand that they should change their password after a phishing or cyberattack
Abusive Content	- that inappropriate content could appear online - that intolerant content could appear online - that hate speech could appear online - that violent content could appear online - that illegal materials such as images of child abuse could appear online - that online gambling services exist - that pornographic content exists online - that sexual or harmful content exists online - that false or untrue content exists online as well as fake news - that bullying via websites, mobile phones or other forms of communication devices is possible - that chatrooms on the internet can be an unsafe place - that downloading data, like music from unlicensed sources can be dangerous - that a stranger can ask them for personal information - the meaning of grooming - that using communication technologies can lead to sexual assault and/or child prostitution	- classify age-appropriate websites by using their knowledge of what constitutes a child-friendly website - create online content safely - decide if a website is age-appropriate - self-protect in an online environment by ignoring or retreating from harmful media - determine whether a website is safe or suspicious - avoid dangerous chats and internet sites entirely - use appropriate privacy settings to minimize social networking site (SNS) risks, assess other online risks, and recognize cyberbullying - assess the security of websites before entering personal information - handle privacy settings to avoid online enticement and seduction - identify "Red Flag" and malicious intentions of strangers related to online enticement and seduction - ask a trusted adult for help to determine if their online activity is age-appropriate - seek guidance from teachers to decide if a website is age-appropriate - decide whether or not to respond to interactions in cyberspace - determine whether information found in cyberspace is credible or not - recognize and avoid inappropriate material (such as illegal or pornographic content) - use strategies to prevent cyberbullying - protect themselves from harm on the internet - browse safely and securely - practice basic cyber hygiene, including behavior, communication, and care for their devices and accounts - decide whether a website is safe or suspicious - make backups of important data and understand the importance of backups - avoid dangerous chats and websites entirely - refrain from meeting up with people from chatrooms - be cautious and not fully trust what people say on the internet - keep their laptop, iPad, or mobile device locked when working in the classroom - avoid clicking on links in messages (email, SMS, chat) unless they come from someone they know - assess the security of websites before entering personal information - not open email attachments from unknown senders - avoid posting everything on the internet - understand that downloading data, such as music, from unlicensed sources can be dangerous - identify situations where it is wise to seek help from a trusted adult - understand that their emotions can be a powerful tool in assessing unsafe situations - recognize physical sensations that alert them to unsafe situations - anticipate and avoid dangerous or hazardous situations (such as meeting strangers in person) - understand the importance of consulting an adult before participating in the online environment - recognize that not everyone they meet, whether in the real world or online, is trustworthy - check files with an adult before downloading them - ask teachers for help to stay safe on the internet - decide whether to follow or click on a link - consider the impact of their actions on others and society before acting in a social networking environment - understand the meaning of entering into contracts and avoid doing this on their own - use future-oriented coping strategies, or "preventive coping," to address potential stressors before they become a problem - identify qualities that can help assess if a person is trustworthy - recognize physical sensations that alert them to unsafe situations	- recognize inappropriate and harmful media content - identify safe and unsafe internet sources - identify unsafe content online - recognize a phishing website - detect online enticement and seduction by discussing online manipulation	- know how to cope with negative online experiences - help others who are feeling sad or upset due to online threats	- know how to cope with negative online experiences - help others who are feeling sad or upset due to online threats
Safety	- what cybersecurity is - the meaning of the term "reporting" - what a bystander and an upstander are in regard to cyberbullying - the risks associated with internet use and digital environments - the various forms and behaviors of harmful digital actions - that there are dangers associated with social networking - the risks associated with social networking sites (SNS) - that dangerous situations can arise during the use of SNS - that nothing posted on the internet is truly safe or secure - that people can be manipulated online - what an "online predator" is - the possible risks and negative effects of the internet on their physical and psycho-social development - the issues related to computer and internet addiction, including physical and mental health problems from excessive technology use - that not every sender of an email is trustworthy - how online actions have real world consequences, and that laws and regulations apply online as well - about inappropriate and bullying behaviors and how these impact the feelings of others - about the prevention of cyberbullying - that they are not anonymous while using the internet - that their digital and real identities are heavily connected - that the internet doesn't forget - the difference between right and wrong online behavior - the different motivations that influence right and wrong online behaviors - what it means to use a "parent" credit card - the reality of payments conducted online - that they should be nice and polite to others on the internet - the principle of online etiquette, including the roles of an upstander and a bystander - how to treat others online with respect - the importance of considering the impact on others and society before acting online - netiquette, online communication, and collaboration - not to open frivolous email attachments if the sender is unknown - the difference between right and wrong uses of digital devices - not to download every piece of content or visit every website - that they should assess a website before opening it - the importance of considering the negative consequences before posting something on social media - not to send abusive texts or emails - that teachers can help them stay safe on the internet - how to use the internet safely, such as not chatting with strangers, not sending personal information or photos, and not meeting people they only know online - not to give out personal information - how to anticipate and avoid dangerous or hazardous situations, such as meeting strangers in person - how to avoid activities that harm their health, such as excessive smartphone use - how to protect their computer	- differentiate between paid and non-paid services online - check the security information and certification for online payments - identify and name the feeling they may experience when dealing with something or someone untrustworthy - know where to ask for help and how to explain their digital safety issues using basic yet proper IT vocabulary (such as phishing, cyberbullying, etc.) - implement appropriate actions against cyberbullying and help others in similar situations - recognize the importance of acting on their feelings (intuition) to avoid or escape unsafe situations - report the situation or the person if they feel unsafe - know how to document evidence, such as screenshots or saved conversations, to support their claims	- know where to ask for help and how to explain their digital safety issues using basic yet proper IT vocabulary (such as phishing, cyberbullying, etc.) - implement appropriate actions against cyberbullying and help others in similar situations - recognize the importance of acting on their feelings (intuition) to avoid or escape unsafe situations - report the situation or the person if they feel unsafe - know how to document evidence, such as screenshots or saved conversations, to support their claims	apply lessons learned from safety issues to improve future online behavior and prevent similar problems	apply lessons learned from safety issues to improve future online behavior and prevent similar problems

Fig. 3 (continued)

determining crucial forecasts or policy positions. During the validation process, we considered the feedback from up to 18 professionals in cybersecurity, education or cybersecurity education. Most of the skills identified by the participants were adopted. In the second round, which we used as a validation process, we received valuable feedback from the participants, including comments on individual skills that were missing from the framework or considered too complex for the target age group. For example, in the category of malicious code and recovery, four participants (02AG, 25TI, 24MG, 18BH) expressed that the skill “Children can restore files after a cyber-attack by means of a backup” was not suitable for the 8–13 age group. A proportionately more common participant comment was that certain skills were considered too advanced for 8–10-year-olds (18BH) or that certain components of skills would be more appropriate for 12–13-year-olds (21TE).

In addition, a subdivision within skills by further age categories was suggested (18TE). We decided against this suggestion because we chose to maintain a holistic view to ensure a comprehensive approach. This decision allowed flexibility in implementing the framework and enabled personalized didactic adjustments based on the individual needs of trainers and teachers during practical use.

Furthermore, the resulting matrix-shaped framework effectively classifies different skills based on the NIST framework (X-axis) and cybersecurity problems relevant to 8–13-year-olds (Y-axis). The choice of the NIST framework dimensions was deliberate, as it offers a holistic and well-defined approach, covering essential stages of cybersecurity problems and facilitating a taxonomic understanding suitable for our target group. Furthermore, the framework’s classification facilitates deriving direct action recommendations after identifying specific skills. Additionally, by incorporating existing literature, cybersecurity games, and various frameworks, we ensured the robustness of the Y-axis categories. While we considered an alternative classification based on cyber-awareness, cyber-hygiene, and cyberbullying, we recognized the lack of clear definitions in academic research, for example, for cyber-hygiene (Vishwanath et al., 2020) and the potential overlap with the NIST framework categories. We chose not to adopt this approach to avoid ambiguity and maintain clarity. Another important aspect is the differentiation and specific impact of the required skills and threats. Many of the skills mentioned in the literature are rather general (e.g., Hammond et al., 2022; Skinner, 2016; Wishart et al., 2007), which has the advantage that they can be interpreted differently in various countries. However, this also has a disadvantage: this generalization and the resulting superficiality of the skills make it more difficult to effectively address specific problems, such as fake news, which is increasing in Europe and the United States (Vlachos, 2022). A more detailed differentiation between misinformation, disinformation, and malinformation would be useful in this context (Armitage & Vaccari, 2021; Carmi et al., 2020). This would enable a more targeted approach to challenges such as radicalization, misogyny, and other negatively connoted social phenomena that can influence children (HOUSE, O. C., 2019). In addition to this rather superficial definition, there seems to be a general lack of standardized definitions and clear delineation of problem areas and their subtopics (Cranmer et al., 2009; Finkelhor et al., 2021; Vishwanath et al., 2020), which means that individual abilities can be interpreted differently. In future research, the individual terms could be extracted from the skills and then defined in a dedicated manner. This contrasts with the constantly changing landscape of threats. Risks and challenges change regularly (Patterson et al., 2023; Al-Rimy et al., 2018), which argues against narrowing definitions. In addition, future research and practice could focus on the segmentation of skills and how these can be effectively delivered to the appropriate target group. In this context, the developed framework and the extracted competencies served as the project’s foundation. From the framework, an

ontology was created to identify the knowledge elements and competencies required for the proposed demographic. These competencies are then used to evaluate different games and to create a learning outcome evaluation that will be made available to the public. Additionally, the framework requires empirical validation through pilot implementations in educational settings to assess real-world effectiveness and identify implementation challenges such as teacher training requirements.

Furthermore, while our international literature base provides broad applicability, regional variations in cybersecurity threats (e.g., different fake news patterns across Europe vs. Asia) may require local adaptations of the framework's generalized skills. Future research should examine regional customization needs while maintaining the framework's core structure.

To sum up, this study contributes a specialized skill framework that addresses the cybersecurity needs of children aged 8–13, providing guidance and resources to foster safe online practices. By utilizing the NIST framework and incorporating cybersecurity professionals' insights, we have enhanced the framework's validity, making it a valuable tool for promoting online safety among this vulnerable age group. However, it is important to note that this framework should be empirically tested in future studies to further validate and optimize its effectiveness in practice. In extension, a compacted and easy-to-use version should be created for practice and teaching.

Author contributions Nicolai Plintz: Conceptualization, Data curation, Investigation, Methodology, Writing—original draft. Dirk Ifenthaler: Conceptualization, Resources, Supervision, Writing—review and editing.

Funding Open Access funding enabled and organized by Projekt DEAL. This work was co-funded by the Erasmus+ Programme of the European Union under Project No. 101087250—ERASMUS-EDU-2022-PI-FORWARD.

Data availability The relevant materials/resources are listed under the references cited. Sources marked with an asterisk are included in the systematic review.

Declarations

Conflict of interests Nicolai Plintz and Dirk Ifenthaler declares that he has no conflict of interest.

Ethical approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards. This article does not contain any studies with animals performed by any of the authors. This study involved the collection of professional opinions through a Delphi process. As the research did not involve direct interaction with vulnerable populations or the collection of sensitive personal data and was limited to professional opinions, it was determined in accordance with the University of Mannheim guidelines that ethics committee approval was not required. However, participants were fully informed of the aims of the study and were provided with a privacy statement, and participation was entirely voluntary and confidential.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the

material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

The references marked with an asterisk (*) are those that were included in the systematic literature review

- Al-Rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, 74, 144–166. <https://doi.org/10.1016/j.cose.2018.01.001>
- *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, S., Bastian, B., Bellew, K., Bonzon, T., Braught, T., Carter, P., Chen, B., Day, C., Dungan, C., George, K., Gibson, R., Hartkopf, J., Henderson, W., Hendricks, N., Herbel, K., Hof, L., Hughes, C., Jacobson, D., ... Underwood, J. (2021). K-12 cybersecurity learning standards. Retrieved from <https://cyber.org/standards>.
- *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), 11269. <https://doi.org/10.3390/app112311269>
- Armitage, R., & Vaccari, C. (2021). Misinformation and disinformation. In *The Routledge companion to media disinformation and populism* (pp. 38–48). <https://doi.org/10.4324/9781003004431-5>.
- *Baciu-Ureche, O. G., Sleeman, C., Moody, W. C., & Matthews, S. J. (2019). The adventures of scriptkitty: Using the raspberry pi to teach adolescents about internet safety. *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, 118–123. <https://doi.org/10.1145/3349266>
- Baldini, G., Barrero, J., Chaudron, S., Coisel, I., Draper Gil, G., Duch Brown, N., Eulaerts, O., Geneiatakis, D., Hernandez Ramos, J., Joanny, G., Junklewitz, H., Kampourakis, G., Kerckhof, S., Kounelis, I., Lewis, A., Martin, T., Nai Fovino, I., Nativi, S., ... Tirendi, S. (2020). *Cybersecurity, our digital anchor* (I. Nai Fovino, G. Barry, S. Chaudron, I. Coisel, M. Dewar, H. Junklewitz, G. Kampourakis, I. Kounelis, B. Mortara, J. Nordvik, & J. Sanchez Martin, Eds.). Publications Office of the European Union. <https://doi.org/10.2760/967437>
- *Becta (2006). Safeguarding children in a digital world. Coventry: British Educational Communications and Technology Agency.
- *Beranek, L. (2009). Information systems security education for future teacher at secondary and primary schools. *Journal of Technology and Information Education*, 1(2), 89.
- *Berson, I., Berson, M., 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*, 8(3), 222–243.
- *Blinder, E. B., Chetty, M., Vitak, J., Torok, Z., Fessehazion, S., Yip, J., Fails, J. A., Bonsignore, E., & Clegg, T. (2024). Evaluating the use of hypothetical 'Would You Rather' scenarios to discuss privacy and security concepts with children. *Proceedings of the ACM on Human-Computer Interaction*, USA, 8(CSCW1), Article 165, 1–32. <https://doi.org/10.1145/3641004>
- *Buchanan, L., Scarlatos, L., & Telendii, N. (2021). Curriculum to broaden participation in cybersecurity for middle school teachers and students. In *2021 IEEE Integrated STEM Education Conference (ISEC)* (pp. 63–70). <https://doi.org/10.1109/isec52395.2021.9763930>
- Carmi, E., Yates, S. J., Lockley, E., & Pawluczuk, A. (2020). Data citizenship: Rethinking data literacy in the age of disinformation, misinformation, and malinformation. *Internet Policy Review*, 9(2), 1–22.
- Chang, V., Golightly, L., Xu, Q. A., Boonmee, T., & Liu, B. S. (2023). Cybersecurity for children: An investigation into the application of social media. *Enterprise Information Systems*, 17(11), 2188122. <https://doi.org/10.1080/17517575.2023.2188122>
- *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>

- *Dönmez, O., Odabasi, H. F., Kabakçi Yurdakul, I., Kuzu, A., & Girgin, Ü. (2017). Development of a scale to address perceptions of pre-service teachers regarding online risks for children. *Educational Sciences: Theory and Practice*, 17(3), 923–943. <https://doi.org/10.12738/estp.2017.3.0022>
- European Union Agency for Cybersecurity (ENISA). (2017, Sept). Overview of cybersecurity and related terminology (Version 1). Retrieved from <https://www.enisa.europa.eu/publications/overview-of-cyber-security-and-related-terminology>
- European Union Agency for Network and Information Security. (2018). *Reference incident classification taxonomy: Task force status and way forward*. Retrieved from <https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy>
- *Finkelhor, D., Jones, L., & Mitchell, K. (2021). Teaching privacy: A flawed strategy for children's online safety. *Child Abuse & Neglect*, 117, Article 105064. <https://doi.org/10.1016/j.chiabu.2021.105064>
- *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* (pp. 130–134). <https://doi.org/10.1145/3306500.3306501>
- *Fujikawa, M., Ikehara, H., & Abe, Y. (2020). SNS Education Game for Upper-Grade Elementary School Students. In *Proceedings of the 2020 8th international conference on information and education technology* (pp. 137–141). <https://doi.org/10.1145/3395245.3395248>
- Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015). CyberAware: A mobile game-based app for cybersecurity education and awareness. In *2015 International conference on interactive mobile communication technologies and learning (IMCL)* (pp. 54–58). IEEE. <https://doi.org/10.1109/IMCTL.2015.7359553>
- Gillespie, A. A. (2002). Child protection on the internet-challenges for criminal law. *Child & Fam. LQ*, 14, 4.
- *Graafland, J. H. (2018, September 17). New technologies and 21st century children: recent trends and outcomes. *OECD Education working papers*, No. 179. OECD Publishing (pp. 1–60). <https://doi.org/10.1787/e071a505-en>
- *Hammond, S. P., Polizzi, G., & Bartholomew, K. J. (2022). Using a socio-ecological framework to understand how 8–12-year-olds build and show digital resilience: A multi-perspective and multimethod qualitative study. *Education and Information Technologies*, 28, 3681–3709. <https://doi.org/10.1007/s10639-022-11240-z>
- HOUSE, O. C. (2019). Disinformation and 'fake news': Final Report. London: House of Commons.
- *Hudson, C. C., Lambe, L., Pepler, D. J., & Craig, W. M. (2015). Coping while connected. *Canadian Journal of School Psychology*, 31(1), 3–16. <https://doi.org/10.1177/0829573515619623>
- *Hudson, C. C., Lambe, L., PREVNet National Youth Advisory Committee, 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>
- *Ibrahim, A., McKee, M., Sikos, L. F., & Johnson, N. F. (2024). A systematic review of K-12 cybersecurity education around the world. *IEEE Access*, 12, 59726–59738. <https://doi.org/10.1109/ACCESS.2024.3393425>
- *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*. <https://doi.org/10.1002/car.2742>
- Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-021-10807-6>
- *Konak, A. (2014). A cyber security discovery program: Hands-on cryptography. *IEEE Integrated STEM Education Conference*, 2014, 1–4. <https://doi.org/10.1109/ISECon.2014.6891029>
- *Kralj, L. (2014). Children's safety on the Internet-development of the school curriculum. In *2014 37th international convention on information and communication technology, electronics and microelectronics (MIPRO)*, Opatija, Croatia (pp. 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*, 7(13), 59–75.
- *Kritzinger, E., & Padayachee, K. (2013). Engendering an e-safety awareness culture within the South African context. In *2013 Africon*, Pointe aux Piments, Mauritius (pp. 1–5). <https://doi.org/10.1109/africon.2013.6757708>
- *Kritzinger, E. (2015). Enhancing cyber safety awareness among school children in South Africa through gaming. In *2015 Science and information conference (SAI)*, London (pp. 1243–1248). <https://doi.org/10.1109/SAI.2015.7237303>

- Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). In their own words: What bothers children online? *European Journal of Communication*, 29(3), 271–288. <https://doi.org/10.1177/0267323114521045>
- Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry*, 55(6), 635–654. <https://doi.org/10.1111/jcpp.12197>
- *Martin, F., Mushi, D., Bacak, J., Wang, W., Ahlgrim-Delzell, L., & Polly, D. (2024). Elementary student experiences from digital safety immersion summer program. *Educational Media International*, 61(3), 321–343. <https://doi.org/10.1080/09523987.2024.2389485>
- *Martínez-de-Morentin, J.-I., Lareki, A., & Altuna, J. (2021). Risks associated with posting content on the social media. *IEEE Revista Iberoamericana De Tecnologías Del Aprendizaje*, 16(1), 77–83. <https://doi.org/10.1109/RITA.2021.3052655>
- National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. <https://doi.org/10.6028/NIST.CSWP.29>
- *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), Article 10. <https://doi.org/10.3390/mti4020010>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, 132, 103309. <https://doi.org/10.1016/j.cose.2023.103309>
- Paudel, R., & Al-Ameen, M. N. (2025). “It’s definitely new and different...it’s really engaging”: Understanding the power of storytelling towards secure password creation. *International Journal of Human-Computer Interaction*. <https://doi.org/10.1080/10447318.2024.2444046>
- *Pooja, P. R., & Shashidhar, R. (2022). Evaluation of students’awareness towards cyber security. *Phronimos*, 2(4), 33–40.
- Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343. <https://doi.org/10.1016/j.ijcci.2021.100343>
- *Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, 10(5), 378–382. <https://doi.org/10.18178/ijiet.2020.10.5.1393>
- Ringenberg, T. R., Seigfried-Spellar, K. C., Rayz, J. M., & Rogers, M. K. (2022). A scoping review of child grooming strategies: Pre- and post-internet. *Child Abuse & Neglect*, 123, Article 105392. <https://doi.org/10.1016/j.chiabu.2021.105392>
- Roberson, Q. M., Collins, C. J., & Oreg, S. (2005). The effects of recruitment message specificity on applicant attraction to organizations. *Journal of Business and Psychology*, 19, 319–339.
- Sağlam, R. B., Miller, V., & Franqueira, V. N. (2023). A systematic literature review on cyber security education for children. *IEEE Transactions on Education*, 66(3), 274–286. <https://doi.org/10.1109/TE.2022.3231019>
- Santre, S. (2023). Cyberbullying in adolescents: A literature review. *International Journal of Adolescent Medicine and Health*, 35(1), 1–7. <https://doi.org/10.1515/ijamh-2021-0133>
- Scheibe, M., Skutsch, M., & Schofer, J. (1975). Experiments in Delphi methodology. In H. A. Linestone & M. Turoff (Eds.), *The Delphi method—Techniques and applications* (pp. 262–287). Addison-Wesley.
- *Shen, L. W., Mammi, H. K., & Din, M. M. (2021). Cyber security awareness game (CSAG) for secondary school students. In 2021 *International conference on data science and its applications (ICoDSA)* (pp. 48–53). Bandung. <https://doi.org/10.1109/ICoDSA53588.2021.9617548>
- *Skinner, G. (2016). Cyber security for younger demographics: A graphic based authentication and authorisation framework. In 2016 *IEEE Region 10 Conference (TENCON)* (pp. 2487–2490). IEEE. <https://doi.org/10.1109/TENCON.2016.7848481>

- Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The delphi method for graduate research. *Journal of Information Technology Education: Research*, 6(1), 1–21.
- Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online—A systematic evidence mapping. *Information, Communication & Society*, 24(4), 557–575. <https://doi.org/10.1080/1369118X.2019.1657164>
- Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), 277–287. <https://doi.org/10.1016/j.chb.2009.11.014>
- Tanrikulu, I., & Erdur-Baker, Ö. (2021). Motives behind cyberbullying perpetration: A test of uses and gratifications theory. *Journal of Interpersonal Violence*. <https://doi.org/10.1177/0886260518819882>
- *Toledo, W., Louis, S. J., & Sengupta, S. (2022). NetDefense: A tower defense cybersecurity game for middle and high school students. In *2022 IEEE frontiers in education conference (FIE)* (pp. 1–6) Uppsala. <https://doi.org/10.1109/FIE56618.2022.9962410>
- *Tomczyk, Ł. (2024). Digital transformation and digital competences of urban and rural Polish youths. *Politics and Governance*. <https://doi.org/10.17645/pag.7381>
- *Tseng, S. S., Yang, T. Y., Shih, W. C., & Shan, B. Y. (2022). Building a self-evolving iMonsters board game for cyber-security education. *Interactive Learning Environments*, 32(4), 1300–1318. <https://doi.org/10.1080/10494820.2022.2120015>
- Vanderhoven, E., Schellens, T., Vanderlinde, R., & Valcke, M. (2016). Developing educational materials about risks on social network sites: A design based research approach. *Educational Technology Research and Development*, 64, 459–480. <https://doi.org/10.1007/s11423-015-9415-4>
- *Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128, Article 113160. <https://doi.org/10.1016/j.dss.2019.113160>
- VLACHOS, S. (2022). The link between mis-, dis-, and malinformation and domestic extremism. Council for Emerging National Security Affairs
- *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>
- Westin, A. (1967). *Privacy and freedom*. Atheneum.
- *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, Article 104536. <https://doi.org/10.1016/j.compedu.2022.104536>
- Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. *Frontiers in Public Health*, 9, Article 634909. <https://doi.org/10.3389/fpubh.2021.634909>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Nicolai B. Plintz completed his master's degree in business education. His main research interests lie in the fields of artificial intelligence and emotional research in educational contexts, with a particular emphasis on optimizing learning outcomes through adaptive systems and emotion-aware technologies.

Dirk Ifenthaler is Professor and Chair of Learning, Design and Technology at the University of Mannheim, Germany and UNESCO Deputy Co-Chair on Data Science in Higher Education Learning and Teaching at Curtin University, Australia. Dirk's research focuses on the intersection of cognitive psychology, educational technology, data analytics, and organizational learning.