International Journal of Educational Research Open 9 (2025) 100462

Contents lists available at ScienceDirect

International Journal of Educational Research Open

journal homepage: www.elsevier.com/locate/ijedro

Trends in digital technologies to address children's online safety education: A systematic scoping review

Maryam Esfandiari [a,*], Beatrice Sciacca [a], Sandra Feijóo [a], Derek Alan Laffan [b], Tijana Milosevic [c], Carol O'Toole [a], James O'Higgins Norman [a]

[a] Anti-Bullying Centre, Dublin City University, Ireland
[b] Mary Immaculate College, Limerick, Ireland
[c] University College Dublin, Ireland

ARTICLE INFO

Keywords:
Online safety
Online safety education
Internet safety
Children
Online risk
Scoping review

ABSTRACT

This scoping review aims to identify trends in studies related to children's online safety education facilitated by digital technologies. The review is guided by the five-stage framework developed by Arksey and O'Malley. We searched in four electronic databases: ERIC,Web of Science, Scopus, and the Association for Computing Machinery (ACM). The studies identified in the search were independently reviewed by two authors using the PRISMA checklist for scoping reviews and the Rayyan software. Following the study's inclusion and exclusion criteria, we incorporated 34 papers into the scoping review. Our analysis revealed a growing number of educational technologies designed for children's Internet safety education over the years. Among various approaches, game-based learning emerged as the most popular method for delivering educational content within the broader domain of online safety education for children. The majority of the studies focused on children aged 11–14 years old, with sample sizes ranging from 6 to 976 child participants. Additionally, intervention-based research designs were the most frequently employed methodology. Our study advances the knowledge base on technology-based education in online safety training of children by mapping the literature of this field and unveiling the trends over the past decade. These insights can shape future research directions in online safety education and inform the educational technology industry.

Introduction

Digital technologies are an integral part of children's daily lives which presents both opportunities and risks for them. While not all online risks may necessarily lead to harm (Livingstone, 2013), it is still crucial to equip children and young people with the necessary knowledge and skills to navigate the digital world safely and responsibly (Cortesi et al., 2020). Digital-based learning is a well-established way to encourage safer online behaviour among children and young people. Information and communication technologies (ICT) provide various resources and learning platforms to transmit educational content. According to Zhang-Kennedy & Chiasson (2022), digital and multimedia education tools can be defined as educational content that utilizes multiple modes of communication, which includes various elements such as text, images, audio, animation, video, and interactive features.

Defining key terms in this realm is essential to understanding online threats that children and young people may encounter. Various terminologies have been used to describe different types of online threats. 'Cyber Security' and 'Online Safety' are two standard terms to describe actions to prevent and reduce online threats. Understanding their differences is crucial in online and digital technology contexts. In recent years, scholars have increasingly considered cybersecurity from a wider perspective. For instance, Schatz et al. (2017) noted that traditional definitions of cybersecurity have been limited to technical aspects, disregarding the broader socio-technical systems in which these technologies operate. They described cybersecurity as the strategies and measures executed by organisations and governments to manage security risks, ensuring the confidentiality, integrity, and availability of data and digital assets in cyberspace.

Cybersecurity is increasingly acknowledged as a multifaceted

* Corresponding author at: SG04, Anti-Bullying Centre, All Hallows Campus, Dublin City University, Dublin, Ireland.
E-mail addresses: maryam.esfandiari@dcu.ie (M. Esfandiari), beatrice.sciacca@dcu.ie (B. Sciacca), sandra.sanmartinfeijoo@dcu.ie (S. Feijóo), 23600433@micstudent.mic.ul.ie (D.A. Laffan), tijana.milosevic@ucd.ie (T. Milosevic), carol.otoole@dcu.ie (C. O'Toole), James.OHigginsNorman@dcu.ie (J. O'Higgins Norman).

https://doi.org/10.1016/j.ijedro.2025.100462

Available online 31 March 2025

discipline that encompasses technical, legal, ethical, and policy aspects (Schatz et al., 2017). Von Solms and Van Niekerk (2013) emphasize the necessity of safeguarding entire digital environments, which include networks, computers, and data, against cyber threats, unauthorized access, and potential harm. This more comprehensive view of 'cyber security' involves the protection of both informational and non-informational assets for individuals and communities.

Online safety is another common term for protecting individuals from harm or danger on the internet. Online safety refers to minimising online risk and harm, and it involves individual behaviours and practices to stay safer online behaviour for both adults and children. In this context, Hartikainen et al. (2019) indicated that 'threat' pertains to anything that can exploit an existing flaw and cause some 'harm', intentional or unintentional. On the other hand, 'harm' is a recognisable negative consequence that can be measured objectively or subjectively through self-report. Livingstone and Smith (2014) define harm in the context of online risks as a probabilistic outcome, which is not inevitable for every encounter with online risk. They suggest conceptualising online risks as affording harm, where harm depends on various contingencies. Kimpe (2019) takes a comprehensive approach, emphasizing the importance of safeguarding personal and sensitive information and being aware of and mitigating various online risks like cyberbullying, identity theft, and exposure to inappropriate content. This underscores the significance of digital literacy and responsible online behaviour. By practising positive online behaviour, children and young people can decrease their risk of harm and increase their self-efficacy and resilience. While there is some overlap between cybersecurity and online safety, this study uses the terminology of online safety to align with the literature on education regarding internet harms.

Children are a vulnerable segment of society. For instance, cyberbullying, misinformation and risks associated with artificial intelligence (AI) (Campbell et al., 2025) are some of the recent online risks towards children and young people in recent years. To tackle these risks and avoid harmful consequences, studies show that online and digital-based education is as effective as offline education (Pei & Wu, 2019).

As children engage more with online digital platforms, it is crucial to adopt relevant and engaging online safety education in order to protect them from online risks and harms. Digital technology plays a crucial role in improving online learning experinces. A recent systematic review by Zhang-Kennedy & Chiasson (2022) studied 119 tools designed to educate non-expert end-users on cyber security awareness. The review found that digital games, films and animations, games, learning modules, and comics are commonly used tools for delivering educational messages. However, it is important to note that this study focused exclusively on digital technology tools designed for the adult population, not children. The literature also demonstrates that studies' perspectives may vary slightly depending on their focus and goals. For instance, a systematic review of cybersecurity awareness research for children by Quayyum et al. (2021) found that most education programs for children primarily address risks such as privacy concerns, cyberbullying, and exposure to inappropriate content, including pornography. This suggests that studies focus on online harm rather than empowering children with broad internet safety skills to combat online harm. Furthermore, experts argue that online safety education should be integrated into established, evidence-based risk-prevention programs for associated offline risks, such as sexual health, well-being, and mental health (Finkelhor et al., 2021).

Current study

Researchers are keen on exploring digital based technology in online safety education from various angles, including their effectiveness and usability (Ghazinour et al., 2019; Nicolaidou & Venizelou, 2020). Examining these tools involves analysing their impact and assessing how well they facilitate learning and understanding the complex cyber threat landscape (e.g., Nicolaidou & Venizelou, 2020). This study highlights key trends and gaps in the literature that use digital technologies to educate children on online safety. Overall, the literature suggests that digital technology can be used effectively in children's online safety education to promote positive online behaviour and ensure their safety in the digital world (e.g., Giannakas et al., 2019). While various reviews (whether systematic or scoping) exist on online safety education, a significant gap exists in the literature concerning a specific focus on children. Accordingly, this scoping review aims to bridge this gap by identifying trends in studies related to children's online safety education using digital technologies. Scoping reviews are well-established for exploring topics beyond the effectiveness or impact of interventions, making them particularly valuable for integrating literature from diverse fields (Peters et al., 2015). Systematically analysing and mapping current trends in studies conducted on children is crucial because it addresses a distinct and highly vulnerable demographic and reveals the strengths and weaknesses of this field of study.

Specifically, this scoping review addresses **two primary research questions:** a) What digital technologies are currently being utilised to educate children about online safety? b) What are the opportunities and challenges of digital technology-based research in enhancing online safety education for children?

It is important to note that this scoping review focuses on studies related to general online safety education rather than specific online harm, such as cyberbullying. It provides an overview of the research landscape on the role of information and communication technologies (ICT) in advancing youth's online safety skills. The study offers several valuable contributions, including synthesising 34 documents on children's online safety education and making recommendations for researchers, educators, and educational industries.

Method

This study aimed to gain a better understanding of existing literature on digital technology trends in children's online safety education. To ensure transparency and accuracy in our research, we have registered our scoping review protocol on (AsPredicted #107292). We have employed the methodological framework introduced by Arksey and O'Malley, (2005) to conduct a scoping review. The framework consists of five key stages: identifying the research question, locating relevant studies, selecting appropriate studies, organising the gathered data, and summarising and reporting the findings. Throughout the process, we have adhered to the PRISMA Extension for Scoping Reviews guidelines to ensure transparency in our reporting (Liberati et al., 2009; Moher et al., 2009; and Tricco et al., 2018).

Search strategy and data sources

In November 2022, the first author searched four databases: ERIC, Web of Science, Scopus, and the Association for Computing Machinery (ACM), using English as the filtering language. The four databases were selected through a group discussion among the authors, as they provide coverage of indexed journals about children and education. The literature search utilised various keywords that can be divided into four concepts: 1) children, 2) online safety, 3) education, and 4) technology (Table 1). Within every category, keywords were combined through the Boolean operator "OR," and each category was combined with the others through the conjunction "AND."

Selection of the studies

The inclusion criteria allowed for the selection of studies that met the following conditions: 1) addressed online safety education with a digital component; 2) focused on children under 18 years old; 3) were written in English; 4) were peer-reviewed studies, dissertations, or conference proceedings; 5) were published from 2013–2022 (due to a significant technological shift in online education over the previous decade) and 6)

Table 1
Concepts and keywords.

Keyword	Search term
Children	(child* OR teen* OR young* OR adolescent* OR student* OR pupil* OR youth)
Online Safety	AND ("internet safety" OR "digital safety" OR "online safety" OR "mobile safety" OR "esafety" OR "cybersafety" OR "online privacy" OR "digital privacy" OR "internet privacy" OR "internet risk*" OR "online risk" OR "digital risk")
Education	AND (educat* OR promot* OR teach* OR train* OR tackl* OR program* OR prevent* intervention OR combat* OR effectiveness OR efficacy OR effect OR efficiency OR acceptance OR adoption OR acceptability)
Technology	AND (technolog* OR ICT OR game OR helper programs OR virtual learning environment OR application OR app OR simulation OR automatic OR robots OR chatbots OR software OR automatic detection OR AI OR artificial intelligence OR smartphone OR design OR mobile)

were empirical studies (qualitative, quantitative or mixed method). Studies were excluded from the scoping review if they: 1) pertained to educational interventions that solely utilised offline methods; 2) pertained to educational interventions that addressed only a specific aspect of online harm/safety (e.g., cyberbullying, grooming, identity theft); 3) were not written in English; 4) were not peerreviewed; 5) were published before 2013 and 6) were not empirical studies.

Included studies

After a literature search, 2548 studies (Fig. 1) were found and uploaded to Rayyan, a web-based software platform for systematic reviews (Ouzzani et al., 2016). Following this, 103 duplicate studies were identified and subsequently removed from the list. 2445 studies were then independently screened by their titles and abstracts by the first two authors based on the predetermined inclusion and exclusion criteria. Of these, 2402 papers were excluded and did not meet the inclusion criteria. This process resulted in 43 relevant papers, read in full text and then selected independently by both authors. Of these, 21 studies were excluded due to various reasons, including not being an educational tool (n = 5), involving a nudge mechanism (n = 3), lacking the use of digital technology (n = 2), not presenting empirical research (n = 3), focusing on digital citizenship (n = 2), addressing cryptography (n = 1), discussing monitoring apps (n =1), dealing with social media literacy (n = 1), duplicating a thesis that was already included (n =1), having no full text available (n = 1), and not being specifically intended for children (n = 1).

Therefore, a total of 22 papers met the inclusion criteria. Furthermore, to increase the likelihood of identifying relevant studies (Horsley et al., 2011), we screened the reference lists of the 22 papers mentioned above by title. In total, we assessed 32 papers from these sources for eligibility, with 12 of them meeting our inclusion criteria. Consequently, our analysis comprised 34 studies conducted between 2014 and 2022. Any disagreements regarding the selection of these papers were discussed and resolved between the first two authors during a Zoom meeting.

Data charting and analysis

The purpose of analysing and charting data in a scoping review is to summarise and disseminate research findings and identify gaps in the existing literature. Below, we outline the data charting and analysis process in detail. All information from each included study was systematically recorded in a spreadsheet in Excel for further review and analysis. In order to effectively categorise and summarise the final articles in our research study, we utilised 14 key characteristics adopted from the literature. These characteristics align with the objectives of this scoping review. These characteristics included the authors' names, title, year of publication, origin, aim, sample size, sample age, sample gender, research design, type of assessment, designed program, technological tool, name of educational product, and main findings. To streamline the recording of this data, the first author created an Excel spreadsheet and conducted the charting data. Pilot testing of the form on a small number of studies was conducted to ensure it captured all necessary information and was easy to use. Throughout the extraction process, one reviewer was involved in line with group discussions and provided progress reports to the wider research group. In the event of any charting difficulties, the research group was consulted, and any issues were resolved during our weekly research meetings. After the compilation of charting, cross-checking against the original studies was conducted to verify the accuracy of the extracted data. This process ensured a thorough and reliable analysis of the data.

Finding

Study characteristics

Appendix 1 provides the details and characteristics of the included studies, including aspects such as the author(s), publication year, research aims, design, participants, and key findings. The review unveiled a considerable increase in the number of relevant studies in recent years investigating the role of digital technology in children's and youth's online safety education. About 61 % of the reviewed papers were published between 2019 and 2022 (n=21), while 13 were published between 2014 and 2018. Most studies were conducted in Western societies, with only two conducted in low-middle-income countries (Namibia) (see Fig. 2). Nine studies did not specify their origin. The included studies in our research have used three types of study design: n = 17 used quantitative methods (e.g., Baciu-Ureche et al., 2019; Ortega-Barón et al., 2021; Zahed et al., 2019), n = 10 used qualitative methods (e.g., Hardin & Dalsen, 2020; Hartikainen et al., 2019) and n = 7 have explored mixed methods (e.g., Chattopadhyay et al., 2022; Zhang-Kennedy & Chiasson, 2016). A diverse range of research methods was used. Of these, 20 studies opted for intervention-based approaches to test program efficacy as a standalone approach or combined with methods such as feedback evaluation (e.g., Maqsood et al., 2018; Usoro et al., 2016). Another approach, i.e., co-design, was adopted in six studies (e.g., Zhao et al., 2022; Mikka-Muntuumo & Peters, 2021; Raynes-Goldie & Allen, 2014; Bergen et al., 2019).

Opportunities of digital technology in online safety education

According to this scoping review, various digital technology approaches have facilitated and enhanced children's online safety education. Game-based learning was the most common educational approach to transfer online safety material to children (n=15). It was implemented in various methods, for instance, as a mobile application (e.g., (Giannakas et al., 2019; Lazarinis et al., 2020), as a web-based learning tool (e.g., Maqsood et al., 2018; Nicolaidou & Venizelou, 2020), as a simulation (Cardoso et al., 2022) or a computer game (Raynes-Goldie & Allen, 2014). Educational apps were also created (n=5) (Chattopadhyay et al., 2022; Zinkus et al., 2019). For example, Podila et al. (2020) developed an Android app to promote a online safety mindset among high school students. This app covers various aspects of technical online safety and promotes online safety through engaging activities such as quizzes and scenarios designed to identify cyber-attacks. For instance, Alemany et al. (2020) developed a gamified social network to educate children on online safety concepts. Participants in the gamified social network demonstrated better online protection than non-gamified participants. Apart from games, the review studies highlight various educational tools for online safety training. The second most common type of educational tool found in these studies was apps, which were available as both mobile and web applications (e.g., Perenič et al., 2017; Zhang-Kennedy et al., 2017). For instance, Zinkus et al. (2019) observed

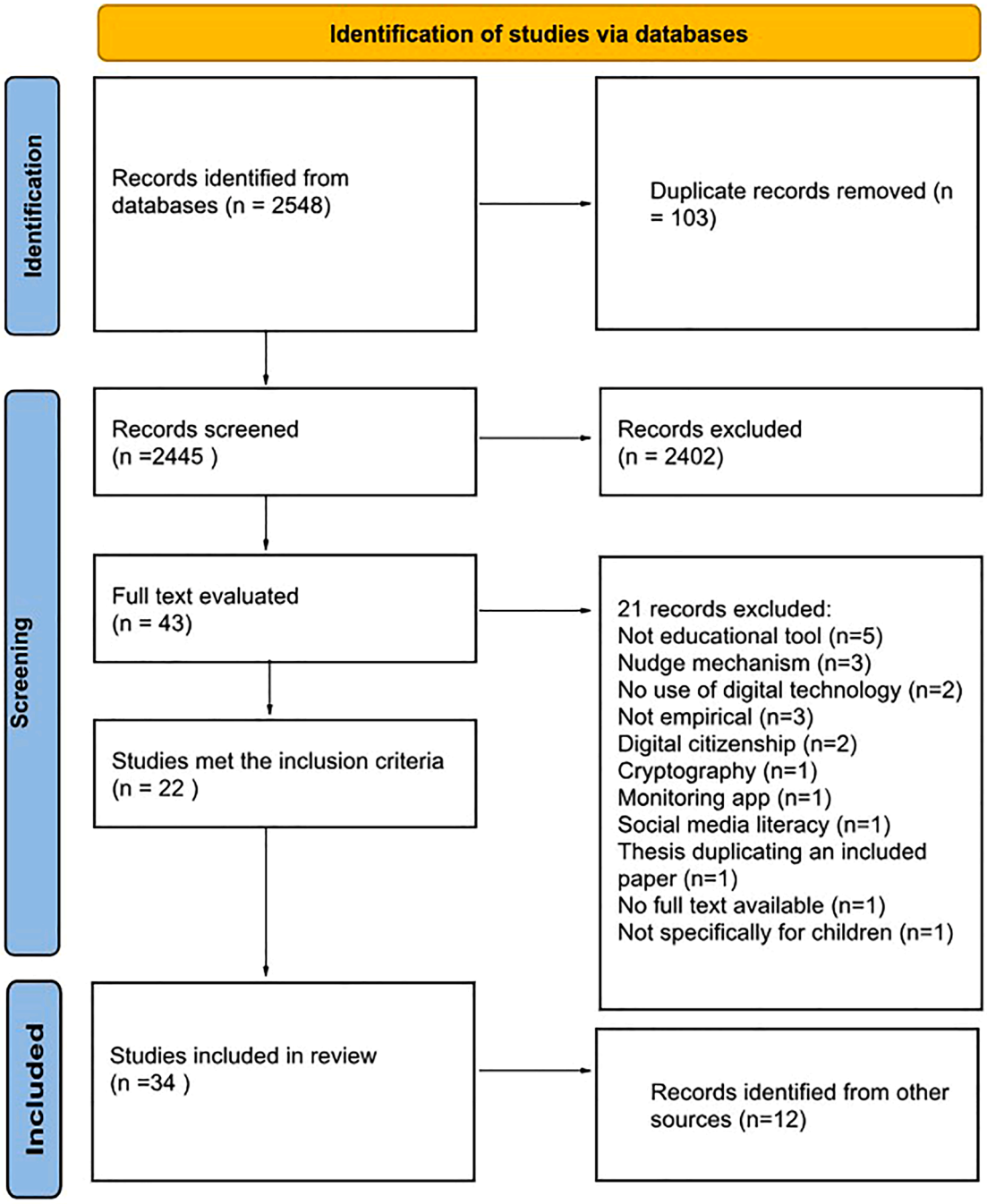

Fig. 1. Prisma flowchart: Number of records identified, screened, and included.

that students had some level of online risk understanding in a simulation-based web application. Through the intervention, they displayed a more profound comprehension of online harm. In addition, the results consistently demonstrate the effectiveness of digital tools in enhancing children's digital safety skills. For instance, a pre-post study conducted by Nicolaidou and Venizelou (2020) provides evidence of the effectiveness of web-based learning environments. The reviewed studies indicated a positive outcome regarding technology use in digital safety education, enhancing children's awareness (e.g., Alemany et al., 2020; Jin et al., 2018; Zhang-Kennedy & Chiasson, 2016). In addition, some of these studies have even suggested a positive impact on behavioural changes. For instance, a study involving 387 teenagers in the United States observed a significant change in children's online behaviour after using their education tool (Alemany et al., 2020). However, it is essential to note that the findings across studies are inconsistent regarding behaviour change. Some reviewed studies have reported limitations in the ability of digital safety education to improve children's online safety practices substantially despite successfully increasing their awareness (e.g., Berger et al., 2019). Regarding the teaching method, the included studies applied digital learning methods involving interpersonal communication with teachers and peers. For example, Liau et al. (2017) discovered that teachers' and peers' roles in digital-based learning can reinforce Internet safety education. This study highlighted that direct communication between educators and students and exchanging knowledge and experiences in physical educational environments play a vital role (Liau et al., 2017). This finding aligns with Vygotsky's sociocultural theory, indicating that learning is collaborative (Jaramillo, 1996).

Fig. 2. Geographical distribution of studies
Note. Ten studies did not specify the origin where the study was conducted.

Challenges of digital-based online safety education

Despite the facilitating role of technology in online safety education, the discussion on the impact of technology in education, particularly in online safety, is a complex issue that requires a balanced and precise approach. Regarding online safety, a wide range of topics were discussed in the education technologies discussed in the reviewed papers. For example, educational technology shows children how to practice safe behaviours online, such as not sharing personal information with strangers, avoiding contact with unfamiliar individuals (Mikka-Muntuumo et al., 2018) and refraining from responding to suspicious messages or emails (e.g., Cardoso et al., 2022; Lazarinis et al., 2020; Ortega-Barón et al., 2021), Internet risks were also among the safety educational programs (Cardoso et al., 2022; Ortega-Barón et al., 2021; Qusa & Tarazi, 2021; Bioglio et al., 2019) Few studies examine more complex issues regarding internet safety. According to (Finkelhor et al., 2021), online safety education extends beyond merely disseminating digital and media literacy skills and providing guidance on privacy protection (Berger et al., 2019). It encompasses a broader spectrum of knowledge and practices aimed at cultivating an environment of healthy, respectful, and secure interactions in the online domain. Intervention studies have been widely used to evaluate the effectiveness of digital-based educational materials (Zhang-Kennedy & Chiasson, 2022). However, many of these studies have not been rigorous enough in their evaluation due to high dropout rates (Baciu-Ureche et al. (2019). Future research should focus on using more robust methodologies, such as randomised controlled trials, and incorporating longterm follow-ups to provide a more comprehensive understanding of the efficacy of such programs.

Discussion

This scoping review examines research on educational technology related to children's online safety education from 2013 to 2022. This research emphasises important areas that need additional investigation and policy enhancement to promote more efficient prevention, intervention, and educational approaches. This study seeks to fill the gaps in the current knowledge base to help create evidence-based methods for safeguarding children against online threats. In this section, we outline the key findings from this scoping review and emphasise how these findings enhance the current understanding of the domain.

Need for defining what is online safety

This scoping review revealed a lack of in cohesive and holistic definition of online safety concept. The reviewed studies demonstrate a dispersion of approaches in studying and examining the concept of online safety and did not provide a clear and concise definition. While some studies approached online safety education from a purely technical perspective (Chiou et al., 2021), others emphasised more conceptual aspects of online safety. This dispersion in the literature can be attributed to the multifaceted nature of online safety education. To effectively promote safe online behaviors, online safety education should include both technical and non-technical skills and knowledge to address potential risks. Given these insights, it is crucial to define online safety education clearly and comprehensively, integrating both technical and critical elements. This approach will not only assist in the developing of impactful online safety education programs and policies but also enable the evaluation of their effectiveness. These findings offer a framework and a unified definition for online safety in general, as well as specifically for online safety education, with a particular emphasis on children and young adults.

Game-Based learning as a prominent tool

The review identifies game-based learning as a dominant tool for digital education in online safety, engaging children in an interactive and immersive learning process (Mikka-Muntuumo & Peters, 2021). Despite its potential, it is imperative for further empirical research to validate its effectiveness and identify best practices in game design that optimise learning outcomes, thereby ensuring that game-based learning's role in promoting online safety is both impactful and evidence-based. Herkanaidu et al. (2021) developed a practical online safety awareness education framework for young people in Thailand. The findings indicated the role of gamification and active learning strategies in delivering online safety awareness. These methods highlights engaging and effective approches in teaching complex topics like cyberbullying and computer security (Hswen et al., 2014). This finding aligns with a recent study on 12–14 years of the role of serious games in news literacy. The findings indicated that gamified educational resources improve students' ability to assess news credibility and enhance their news literacy (see: Capecchi et al., 2024).

One digital education for all

This scoping review also demonstrated that most studies examine children homogeneously and neglect differences. Literature suggested that researches should focus on identifying which children are more at risk of harm and why and designing education based on these specific questions (Livingstone, 2013). For instance, our findings highlight a significant gap in gender considerations within educational programs promoting safe online practices. All included studies have used the same educational materials for both genders without considering the differences in how boys and girls engage with digital environments. When

exploring ICT use among young people, age often emerges as a factor influencing online risk-taking. Research has found that males are more likely to engage in online risks than females, which can lead to greater exposure to online dangers (Popovac & Hadlington, 2020; Stamoulis & Farley, 2010). Therefore, it is essential to recognise how different genders interact with digital environments when creating educational content that addresses online safety, given the gender-specific differences in online behaviour and risk exposure.

Need for rigorous study design

This review has identified some areas for improvement in the research conducted on the use of technology in online safety education. The review criticises the prevalent use of inadequate research methods in this field, which rely heavily on small-scale and qualitative studies, thus limiting the generalizability of findings. The need for a more robust and quantitative research approach is evident, emphasising the necessity for comprehensive studies that can provide more substantial evidence to support the development of effective educational technologies and strategies for online safety education. From a theoretical perspective, there is a significant gap in the existing literature on developing digital educational tools. Most studies do not report any theoretical framework for their designs, which results in a fragmented understanding of the efficacy of educational technology in online safety education. It is recommended that established frameworks, such as Bloom's taxonomy, be incorporated to enhance the design and delivery of educational content by aligning with pedagogical principles that address the specific learning needs of children (Von Solms & Van Niekerk, 2013). This finding aligns with previous research, which found that many online safety messages lack a clear rationale for their effectiveness and do not incorporate proven educational strategies (Finkelhor et al., 2021).

Combination of offline and online education together

Most studies explore the use of educational technology in combining offline activities with online safety education. The literature suggests that integrating internet safety into established programs that address related offline harms may be more effective than standalone online programs. This is because integrated programs can build on more robust evidence bases and address common risk factors. According to a recent review, the most effective approach to preventing online harms is through integrated and comprehensive programs focusing on offline and online risks and dynamics together (Finkelhor et al., 2021).

Fast changes in digital technologies

Online safety education faces a significant challenge due to the rapid pace of technological development. Keeping up-to-date skills and creating new forms of protection from harm is crucial. While digital-based learning can help promote internet safety, it is important not to overstate its effectiveness. Some studies suggest ongoing upgrades and updates of technologies and content are necessary for their success. For example, Cukurova et al. (2019) noted that evaluating the impact of technology in education can be difficult due to constant innovation and change. Yap and Lee (2020) also emphasised the importance of keeping educational resources up-to-date for online privacy, as information can quickly become outdated. However, meeting this need for ongoing updates can financially burden educational institutions, requiring equipment and technical expertise.

Implication

This scoping review has practical and theoretical implications that can improve future studies. Most tools included in the review lack a solid theoretical foundation to guide their design and implementation. Therefore, future studies should prioritise a theoretical and evidence-based approach to create more informed and comprehensive educational content. For example, future studies should investigate the potential of game-based learning, exploring different game formats and their varying effects on children's online safety awareness and behaviour (Jin et al., 2018). Furthermore, the findings of this review offer valuable insights to industry stakeholders, enabling them to identify knowledge gaps in this field and make informed decisions regarding the creation and collaboration of educational technology for children and young people. Leveraging the insights from this review can help industries foster innovation in digital technology for children's cyber safety education and make well-considered strategic choices.

Limitations and future directions

This study has limitations that can be addressed in future research. One limitation is associated with the nature of a scoping review. We did not undertake an extensive synthesis or statistical analysis of the study findings. Moreover, it is essential to note that the findings derived from our scoping review may only be generalised across some contexts or populations. This review's scope might have been limited to specific geographic regions or study designs. Therefore, the relevance of our results in broader contexts could be limited. Most of the included studies were carried out in Europe and North America. It is crucial to emphasise that our analysis was restricted to publications in the English language. Therefore, we cannot definitively determine whether non-Western societies have been overlooked in educational research. Our analysis only covers a portion of the literature in this field, and we recommend future research to investigate technology education and online safety for children in languages other than English.

Additionally, our scoping review is grounded in the literature available until November 2022. Given the dynamic nature of research, it is conceivable that innovative studies and developments have emerged after that time frame. Furthermore, our review primarily relies on published studies in English, excluding relevant grey literature. Future research should incorporate interdisciplinary approaches combining expertise from education, psychology, technology, and law enforcement, ensuring the development of comprehensive, practical, research-based educational technology for children's online safety training (Finkelhor, 2021). In addition, future studies would be more effective if they clearly defined the concept of "online safety" to specify their research objectives better. Furthermore, over the past two years, the consumption of artificial intelligence in the public domain has amplified. This innovative technology is going to change the landscape of education, especially for children and young people. by providing features such as personalised learning experiences and AI-based gamification to enhance children's engagement in education. Therefore, it is essential for future research to examine how emerging technologies, such as artificial intelligence, can be utilised for online safety education for children and young people.

CRediT authorship contribution statement

Maryam Esfandiari: Writing – review & editing, Writing – original draft, Visualization, Software, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Beatrice Sciacca:** Writing – review & editing, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Data curation. **Sandra Feijóo:** Writing – review & editing, Conceptualization. **Derek Alan Laffan:** Writing – review & editing, Conceptualization. **Tijana Milosevic:** Writing – review & editing, Conceptualization. **Carol O'Toole:** Writing – review & editing, Supervision, Funding acquisition, Conceptualization. **James O'Higgins Norman:** Writing – review & editing, Supervision, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding

Vodafone Ireland Foundation and Department of Education.

Data availability statement

The data supporting this study's findings are available on request from the corresponding author, Maryam Esfandiari.

Ethics approval statement

Ethical approval is not needed as this study is a scoping review of previously published summary data.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.ijedro.2025.100462.

References

Alemany, J., Val, E. D., & Garcia-Fornes, A. (2020). Assessing the effectiveness of a gamified social network for applying privacy concepts: an empirical study with teens. *IEEE Transactions on Learning Technologies, 13*(4), 777–789. https://doi.org/10.1109/TLT.2020.3026584

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology, 8*(1), 19–32. https://doi.org/10.1080/1364557032000119616

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/10.1145/3349266.3351399.

Bergen, E., Sæthre, T. H., & Divitini, M. (2019). *Supporting the Co-design of Games for Privacy Awareness | SpringerLink*. https://link.springer.com/chapter/10.1007/978-3-030-11932-4_82.

Berger, E., Sæthre, T. H., & Divitini, M. (2019). PrivaCity. In S. N. Pozdniakov, & V. Dagienė (Eds.), *Informatics in Schools. New Ideas in School Informatics* (pp. 293–304). Springer International Publishing. https://doi.org/10.1007/978-3-030-33759-9_23.

Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., & Pensa, R. G. (2019). A social network simulation game to raise awareness of privacy among school children. *IEEE Transactions on Learning Technologies, 12*(4), 456–469. https://doi.org/10.1109/TLT.2018.2881193

Campbell, M., Barthwal, A., Joshi, S., Shouli, A., & Shrestha, A. K. (2025). Investigation of the privacy concerns in AI systems for young digital citizens: A comparative stakeholder analysis. *arXiv preprint. arXiv:2501.13321*.

Capecchi, S., Lieto, A., Patti, F., Pensa, R. G., Rapp, A., Vernero, F., & Zingaro, S. (2024). A gamified platform to support educational activities about fake news in social Media. *IEEE Transactions on Learning Technologies*.

Cardoso, F., Andreoletti, D., Ferrari, A., Botturi, L., Fioroni, T., Beretta, C., Picco-Schwendener, A., Marazza, S., & Giordano, S. (2022). Playing for Privacy awareness: learning from a *"wow-moment" with iBuddy*. In *ECGBL 2022 16th European Conference on Game-Based Learning*.

Chattopadhyay, A., Poe, T., Nguyen, H., Tsegaye, A., & Moua, L. (2022). Covert eye op app: an offense based learning approach towards developing mobile security awareness and interest in cybersecurity. In *Proceedings of the 23rd Annual Conference on Information* (pp. 29–36). https://doi.org/10.1145/3537674.3554741. *Technology Education*.

Chiou, Y.-M., Barnes, T., Jelenewicz, S. M., Mouza, C., & Shen, C.-C. (2021). Teacher views on storytelling-based cybersecurity education with social robots. *Proceedings of the* 20th Annual ACM Interaction Design and Children Conference, 508–512. https://doi.org/10.1145/3459990.3465199.

Cortesi, S., Hasse, A., Lombana-Bermudez, A., Kim, S., & Gasser, U. (2020). *Youth and Digital* Citizenship+ (Plus): Understanding Skills for a Digital World (SSRN Scholarly Paper 3557518). https://doi.org/10.2139/ssrn.3557518.

Cukurova, M., Luckin, R., & Clark-Wilson, A. (2019). Creating the golden triangle of evidence informed education technology with EDUCATE. *British Journal of Educational Technology, 50*(2), 490–504.

Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2021). Youth Internet Safety education: aligning programs with the evidence base. *Trauma, Violence, & Abuse, 22*(5), 1233–1247. https://doi.org/10.1177/1524838020916257

Ghazinour, K., Messner, K., Scarnecchia, S., & Selinger, D. (2019). Digital-PASS: A simulation-based approach to privacy education. *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society, 162–174*. https://doi.org/10.1145/3338498.3358647

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective, 28*(3), 81–106. https://doi.org/10.1080/19393555.2019.1657527

Hardin, C. D., & Dalsen, J. (2020). Digital Privacy Detectives: An Interactive Game for Classrooms. 2020 IEEE 44th Annual Computers, Software, and Applications Conference *(COMPSAC)*, 184–189. https://doi.org/10.1109/COMPSAC48688.2020.00033.

Herkanaidu, R., Furnell, S. M., & Papadaki, M. (2021). Towards a cross-cultural education framework for online safety awareness. *Information & Computer Security, 29*(4), 664–679.

Hartikainen, H., Iivari, N., & Kinnula, M. (2019). Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction, 22*, Article 100146. https://doi.org/10.1016/j.ijcci.2019.100146

Horsley, T., Dingwall, O., & Sampson, M. (2011). Checking reference lists to find additional studies for systematic reviews. *Cochrane Database of Systematic Reviews, 8*.

Hswen, Y., Rubenzahl, L., & Bickham, D. (2014). Feasibility of an online and mobile videogame curriculum for teaching children safe and healthy cellphone and internet behaviors. *The Digital Wellness Lab*. https://digitalwellnesslab.org/press/feasibility-of-an-online-and-mobile-videogame-curriculum-for-teaching-children-safe-and-healthycellphone-and-internet-behaviors/.

Liau, A. K., Park, Y., Gentile, D. A., Katna, D. P., Tan, C. H. A., & Khoo, A. (2017). iZ HERO adventure: evaluating the effectiveness of a peer-mentoring and transmedia cyberwellness program for children. *Psychology of Popular Media Culture, 6*(4), 326–337. https://doi.org/10.1037/ppm0000094

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *Annals of Internal Medicine, 151*(4). W-65.

Livingstone, S. (2013). Online risk, harm and vulnerability: reflections on the evidence base for child internet safety policy. *ZER: Journal of Communication Studies, 18*(35), 13–28.

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.

Pei, L., & Wu, H. (2019). Does online learning work better than offline learning in undergraduate medical education? A systematic review and meta-analysis. *Medical education online, 24*(1), Article 1666538.

Maqsood, S., Mekhail, C., & Chiasson, S. (2018). A day in the life of jos: A web-based game to increase children's digital literacy. Proceedings of the 17th ACM Conference on *Interaction Design and Children*, 241–252. https://doi.org/10.1145/3202185.3202753.

Mikka-Muntuumo, J., Peters, A., & Jazri, H. (2018). CyberBullet - share your Story: an interactive game for stimulating awareness on the harm and negative effects of the internet. Proceedings of the Second African Conference for Human Computer*Interaction: Thriving Communities*, 1–4. https://doi.org/10.1145/3283458.3283482.

Mikka-Muntuumo, J., & Peters, A. N. (2021). Designing an interactive game for preventing online abuse in Namibia. 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 1–6. https://doi.org/10.1109/IMITEC52926.2021.9714592.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., Altman, D., Antes, G., Atkins, D., Barbour, V., Barrowman, N., & Berlin, J. A. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement (Chinese edition). *Journal of Chinese Integrative Medicine, 7*(9), 889–896.

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). https://doi.org/10.3390/mti4020010. Article 2.

Ortega-Barón, J., González-Cabrera, J., Machimbarrena, J. M., & Montiel, I. (2021). Net: A pilot study on a Multi-risk internet prevention program. *International Journal of Environmental Research and Public Health, 18*(8), 4249. https://doi.org/10.3390/ijerph18084249

Ouzzani, M., Hammady, H., Fedorowicz, Z., & Elmagarmid, A. (2016). Rayyan—A web and mobile app for systematic reviews. *Systematic Reviews, 5*, 1–10.

Perenič, S., Mihelič, M. Ž., & Šerbec, I. N. (2017). Using massive open online courses to raise awareness of safe internet usage in the last three-year cycle of primary school. 2017 16th International Conference on Information Technology Based Higher Education and *Training (ITHET)*, 1–6. https://doi.org/10.1109/ITHET.2017.8067790.

Peters, M. D. J., Godfrey, C. M., Khalil, H., McInerney, P., Parker, D., & Soares, C. B. (2015). Guidance for conducting systematic scoping reviews. *JBI Evidence Implementation, 13*(3), 141. https://doi.org/10.1097/XEB.0000000000000050

Podila, L. M., Bandreddi, J. P., Campos, J. I., Niyaz, Q., Yang, X., Trekles, A., Czerniak, C., & Javaid, A. Y. (2020). Practice-oriented smartphone security exercises for developing cybersecurity mindset in high school students. *2020 IEEE International Conference on* Teaching, Assessment, and Learning for Engineering (TALE), 303–310. https://doi.org/10.1109/TALE48869.2020.9368440.

Popovac, M., & Hadlington, L. (2020). Exploring the role of egocentrism and fear of missing out on online risk behaviours among adolescents in South Africa. *International Journal of Adolescence and Youth, 25*(1), 276–291.

Qusa, H., & Tarazi, J. (2021). Cyber-Hero: A gamification framework for Cyber security awareness for high schools students. In *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0677–0682). https://doi.org/10.1109/CCWC51732.2021.9375847

Raynes-Goldie, K., & Allen, M. (2014). Gaming privacy: A Canadian case study of a co-created privacy literacy game for children. https://dro.deakin.edu.au/articles/journal_contribution/Gaming_privacy_a_Canadian_case_study_of_a_co-created_privacy_literacy_game_for_children/20934706/1.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law, 12*(2), 8.

Stamoulis, K., & Farley, F. (2010). Conceptual approaches to adolescent online risktaking. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 4*(1).

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D., Horsley, T., & Weeks, L. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. *Annals of Internal Medicine, 169*(7), 467–473.

Usoro, I., Connolly, T., Raman, S., French, T., Caulfield, S., & Connolly, S. (2016). Using massive open online courses to raise awareness of safe internet usage in the last three-year cycle of primary school. *European Conference on Games Based Learning*, 704.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security, 38*, 97–102.

Yap, C. E. L., & Lee, J.-J. (2020). "Phone apps know a lot about you!": Educating early adolescents about informational privacy through a phygital interactive book. *Proceedings* of the Interaction Design and Children Conference, 49–62. https://doi.org/10.1145/3392063.3394420.

Zahed, B. T., White, G., & Quarles, J. (2019). Play It Safe: An Educational Cyber Safety Game for Children in Elementary School. 2019 11th International Conference on Virtual Worlds and Games for Serious Applications (VS-Games), 1–4. https://doi.org/10.1109/VS-Games.2019.8864594.

Zhang-Kennedy, L., Baig, K., & Chiasson, S. (2017). Engaging children about online privacy through storytelling in an interactive comic. *Electronic Visualisation and the Arts (EVA2017)*. https://doi.org/10.14236/ewic/HCI2017.45

Zhang-Kennedy, L., & Chiasson, S. (2016). Teaching with an interactive E-book to improve children's online privacy knowledge. In *Proceedings of the The 15th International Conference on Interaction Design and Children* (pp. 506–511). https://doi.org/10.1145/2930674.2935984

Zhang-Kennedy, L., & Chiasson, S. (2022). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys, 54*(1), 1–39. https://doi.org/10.1145/3427920

Zhao, J., Duron, B., & Wang, G. (2022). KOALA hero: inform children of privacy risks of mobile apps. In *Proceedings of the 21st Annual ACM Interaction Design and Children Conference* (pp. 523–528). https://doi.org/10.1145/3501712.3535278

Zinkus, M., Curry, O., Moore, M., Peterson, Z., & Wood, Z. J. (2019). Fakesbook: A social networking platform for teaching security and privacy concepts to secondary school students. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (pp. 892–898). https://doi.org/10.1145/3287324.3287486