International Journal of Child-Computer Interaction 30 (2021) 100343

Contents lists available at ScienceDirect

International Journal of Child-Computer Interaction

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

Review article

Cybersecurity awareness for children: A systematic literature review

Farzana Quayyum [a,*], Daniela S. Cruzes [a,b], Letizia Jaccheri [a]

[a] Norwegian University of Science and Technology (NTNU), Trondheim, Norway
[b] SINTEF, Trondheim, Norway

ARTICLE INFO

Article history:
Received 15 November 2020
Received in revised form 7 June 2021
Accepted 8 June 2021
Available online 16 June 2021

Keywords:
Cybersecurity
Online security
Awareness
Children
Systematic literature review

ABSTRACT

Cybersecurity for children has received much attention and has become a rapidly growing topic due to the increased availability of the internet to children and their consequent exposure to various online risks. This paper aims to summarize the current findings on cybersecurity awareness research for children and help guide future studies. We have performed a systematic literature review on cybersecurity awareness for children, analyzing 56 peer-reviewed studies that report in depth on various cybersecurity risks and awareness-raising approaches. The results of this review include a list of cybersecurity risks for children, a list of commonly used approaches and theories for raising cybersecurity awareness among children, and a list of factors that researchers have considered when evaluating cybersecurity awareness approaches and solutions.

Contents

* Corresponding author.
E-mail addresses: farzana.quayyum@ntnu.no (F. Quayyum), daniela.s.cruzes@ntnu.no (D.S. Cruzes), letizia.jaccheri@ntnu.no (L. Jaccheri).

https://doi.org/10.1016/j.ijcci.2021.100343

1. Introduction

All users, regardless of age, are exposed to various security risks when spending significant time on the internet. Different terms are used to address these risks that internet users get exposed to in their everyday lives. Cybersecurity, online security, online safety and internet security are used interchangeably in the literature to address security concerns in the digital world. Cybersecurity is a broadly used term with many different perspectives. It has no clear literal or operational definition upon which all scholars agree. However, the International Telecommunication Union (ITU) defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.[1]"

Children today spend a substantial amount of time online for either educational purposes or entertainment. The internet offers many opportunities and poses several risks. Given their age, it is difficult for them to assess the opportunities and risks of using the internet and digital systems, even as more and more of their lives are digitally recorded, potentially creating long-term effects on their privacy (Hourcade, 2015) and safety. Sometimes, they do not realize the dangers or risks until it is too late. Thus, they can easily fall victim to online abuses. Along with technical countermeasures, security awareness and practices can help users prevent or mitigate losses from cybersecurity risks. While security practices rely on several factors, one is the degree to which people are aware and able to assess risk and apply knowledge to mitigate threats (Gjertsen, Gjære, Bartnes, & Flores, 2017).

Cybersecurity awareness is defined "as a methodology to educate internet users to be sensitive to the various cyber threats and the vulnerability of computers and data to these threats" (Abd Rahim, Hamid, Kiah, Shamshirband, & Furnell, 2015). Shaw, Chen, Harris, and Huang (2009) also defined cybersecurity awareness as "the degree of users' understanding about the importance of information security and their responsibilities to exercise sufficient levels of information control to protect the organization's data and networks". Based on the definitions above, cybersecurity awareness has two primary purposes: alerting the internet users about cybersecurity risks and enhancing the internet users' understanding of cybersecurity risks to be sufficiently committed to embracing security during internet use. Therefore, mitigating human-related errors or vulnerabilities is a key factor in improving security at either the personal or organizational level (Giannakas, Papasalouros, Kambourakis, & Gritzalis, 2019). We can raise user awareness about cybersecurity and privacy issues.

In the last few years, cybersecurity awareness research and education programs for children have received significant attention from both industry and researchers. Though childhood is divided into different developmental stages, for this study we have adopted the definition of 'child' used by the World Health Organization (WHO), UNICEF,[2] and the Child Rights International Network (CRIN)[3]: anyone under 18 years of age is a child. Studies have examined a number of potential cybersecurity risks for children, including password practices (Prior & Renaud, 2020), online privacy (Kumar et al., 2018; Zhao et al., 2019), and phishing (Lastdrager, Gallardo, Hartel, & Junger, 2017). In addition, many applications and platforms have been developed to teach children about cybersecurity risks, and related topics (Desimpelaere, Hudders, & Van de Sompel, 2020; Giannakas, Kambourakis, Papasalouros, & Gritzalis, 2016; Zhang-Kennedy, Abdelaziz and Chiasson, 2017).

Given this attention from both researchers and practitioners, there is a need for a systematic review of this area to understand the state of the art, identify risks, gaps and needs from current research, and explore the conditions that can enable successful and sustainable solutions for children's cybersecurity awareness education. A review of the published research would also help develop future research agendas and road-maps. This literature review provides a review of research on cybersecurity awareness for children to summarize the findings, understand the risks children are most exposed to, and identify how different approaches to raising awareness of children's cybersecurity risks are being implemented . We also consider how all these approaches affect children's experience, evaluating the approaches and solutions that researchers have proposed. Therefore, this study poses the following research questions:

RQ1. Which cybersecurity risks are addressed in current research for children?

RQ2. What are the approaches used in raising cybersecurity awareness among children?

RQ3. How do researchers evaluate cybersecurity awareness in children?

The main findings from the review are (i) an overview of the identified cybersecurity risks for children, (ii) a thematic map of different approaches to raise cybersecurity awareness and their effects, (iii) a map of the factors that have been used to

[1] https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[2] https://www.unicef.org/sudan/stories/universal-definition-what-it-means-be-child.

[3] https://www.who.int/hiv/pub/guidelines/arv2013/intro/keyterms/en/.

evaluate awareness solutions and approaches, and, (iv) a set of recommendations for both practitioners and researchers.

The rest of the paper is organized as follows: Section 2 presents the study background and related literature reviews. Section 3 describes our research methods, while Section 4 presents our results. Section 5 discusses the findings and Section 6 concludes the paper by presenting the implications of the findings and suggesting future research directions.

2. Background and related studies

Security is an important characteristic of all software products, but security concerns become even more crucial when children are involved. Security entails challenges in several areas, one of the most critical of which is cybersecurity; when children are involved, cybersecurity is related to all the online risks that may affect them and the countermeasures to support them and their caregivers, including the awareness that children have about the various cybersecurity risks. Children's security and privacy have always been a concern for researchers in the child–computer interaction (CCI) research community. In 2013, Read and Markopoulos (2013) summarized the state of CCI research in a literature review of the field. They identified four key challenges for the CCI community, one of which was the penetration of social and cloud technologies in CCI and the resulting risks to children's privacy and security. These risks have now become a part of children's everyday lives because they grow up immersed in technology to a degree that earlier generations would have found unimaginable (Read & Markopoulos, 2013).

Children are now frequent users of the internet and increasingly have their own online devices. They can familiarize themselves with electronic devices very quickly. Thus, the popularity of the internet and social networks are increasingly high among this age group. Tsirtsis, Tsapatsoulis, Stamatelatos, Papadamou, and Sirivianos (2016) conducted a literature review concerning the internet activity and motivation for use by children and identified several risks to which they are exposed. They classify the risks into five categories: (i) content risks, (ii) contact risks, (iii) children targeted as consumers, (iv) economic risks, and (v) online privacy risks. The authors further divide content-related risks into the three broad categories of illegal content (e.g., content about the sexual exploitation of children), harmful content or age-inappropriate content (like pornography), and harmful advice regarding alcohol and drugs, suicide, and psychological and nutritional disorders. For contact-related risks, the authors cite cyberbullying and cybergrooming. Along with categorizing the risks, their study also presents a high-level software architecture designed to account for contemporary online security and privacy risks. Researchers have previously shown that using social media increases the risk of harm for children (Livingstone, Hasebrink, & Görzig, 2012; Staksrud, Ólafsson, & Livingstone, 2013). Thus, it was assumed that children below age 12 might experience fewer risks, especially privacy risks, than teenagers, since children in the younger age group may not use social media as intensively or spend as much time online as teenagers. However, this view may no longer be accurate; even younger children who do not use social media are now vulnerable to privacy risks because of smart toys. de Paula Albuquerque, Fantinato, Kelner, and de Albuquerque (2020) reviewed 26 primary studies investigating privacy risks for children relating to smart toys. They discuss two classifications of risks – technical and domain-specific – and solutions that have been proposed. The authors report the three most frequently found privacy risks in smart toys in their review, which refer to the first three ISO privacy principles: use, retention, and disclosure limitation; consent and choice; and openness, transparency, and notice. Moreover, the authors propose technical and domain-specific solutions to prevent privacy risks in smart toys.

With the expansion of digital spheres and advancements in technology, bullying on digital platforms has become another increasingly common online security topic that has received much attention from researchers and society more generally. In 2017, Pinter, Wisniewski, Xu, Rosson, and Caroll (2017) conducted a literature review on adolescent online safety, reporting important trends by synthesizing 132 peer-reviewed publications. Among other thought-provoking findings, the researchers report that 66% of the reviewed articles were focused on cyberbullying. Indeed, there have been several literature reviews on cyberbullying. For example, Aponte and Richards (2013) review the literature on inappropriate online (and some offline) behaviors by or directed at children. The researchers focus on cyberbullying and identify types of cyberbullying threats and their consequences; the former include flaming, cyber-harassment, denigration, impersonation, masquerading, outing, trickery, ostracism, and exclusion. After identifying the threats, the authors review existing non-technological and technology-based strategies implemented or proposed to avoid or minimize the likelihood and impact of the different kinds of cyberbullying they identify and finally recommend strategies to prevent these risks and their consequences. Watts, Wagner, Velasquez, and Behrens (2017) investigate the historical basis of cyberbullying among adolescents and examine its related factors and effects. Notar, Padgett, and Roden (2013) define cyberbullying and investigate various factors connected to it, such as the role of persons involved and statistics of who is being targeted, reasons for cyberbullying, the differences between traditional bullying and cyberbullying, and gender comparisons related to cyberbullying. Reed, Cooper, Nugent, and Russell (2016) also review the literature, examining interventions for 12 to 18-year-old adolescents experiencing depressive symptoms as a consequence of cyberbullying. The study findings reveal an association between cyberbullying and loneliness, and depression.

Exposure to inappropriate content is another common concern for children, especially adolescents. Owens, Behun, Manning, and Reid (2012) reviewed the literature regarding the impact of internet pornography on adolescents. In examining the existing literature on the impact of online sexually explicit material on adolescents, Owens et al. (2012) focuses on adolescents' attitudes, beliefs, behaviors, self-concept, social development, and brain development. Alotaibi, Furnell, Stengel, and Papadaki (2016) explore the potential of gaming technology to support several key areas of security awareness and learning; they review studies focusing on gaming applications and the effectiveness of their use in creating cybersecurity awareness. The authors divide their study into two parts; the first focuses on a review of the research literature, and the second focuses on the gaming application search. The findings support the positive impact of gaming on creating cybersecurity awareness and identify multiple limitations that call for attention from researchers. In 2015, Cullinane, Huang, Sharkey, and Moussavi (2015) researched and evaluated seven cybersecurity games that were then available. With an end goal of developing new game platforms to teach cybersecurity, the researchers tested the seven games on their effectiveness in imparting the material and keeping students engaged. After the evaluation, the researchers identified strong and weak game-play elements and different ways to deliver cybersecurity knowledge to children. The researchers aimed to use their findings to develop new games designed to teach cybersecurity concepts to minors.

Though all these review studies are relevant to our work, they only partly deal with our topic of interest. Our review study views cybersecurity risks from a broader scope. We consider studies focused on all kinds of cybersecurity risks for children rather than a specific risk. Moreover, in our work, we explore the different approaches to raising cybersecurity awareness and their effects, and we investigate cybersecurity awareness evaluation methods along with the risks. To the best of our knowledge, no other review study is similar in work and scope.

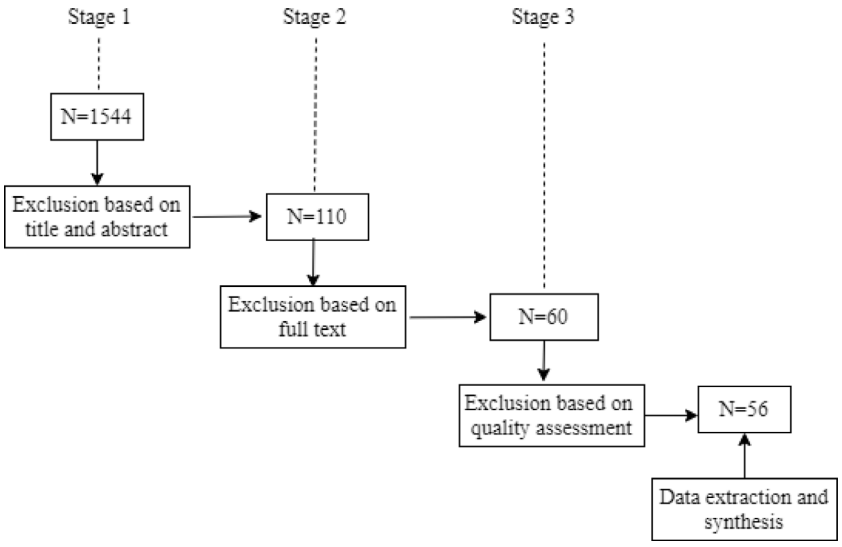

Fig. 1. Study selection process.

3. Review method

This study is a systematic literature review based on the guidelines proposed by Kitchenham (2004). It was undertaken in different stages: the development of review protocol, the identification of inclusion and exclusion criteria, a keyword search in bibliographic databases for relevant studies, critical appraisal, data extraction, and data synthesis. In this section, we describe the details of each of the steps taken and methods used.

3.1. Protocol development

We developed a protocol for the systematic review by following the Kitchenham's (2004) guidelines and procedures. The protocol identified the research questions, search strategy, criteria for study inclusion and exclusion, quality assessment procedures, data extraction procedure, and methods of synthesis.

3.2. Data sources and search strategy

We conducted a literature search of several electronic bibliographic databases in May and June of 2020: ACM Digital Library, IEEE Xplore, ISI Web of Science, ScienceDirect — Elsevier, and Scopus. In the databases, we searched article titles, abstracts, and keywords in stage 1, using two different sets of keywords. The following keywords and combinations were used for the search:

Set 1 — ("Cyber security" OR "Cybersecurity") AND ("Children" OR "Child*" OR "Teen*")

Set 2 — (("Internet" OR "Online") AND "Privacy") AND ("Children" OR "Child*" OR "Teen*")

In addition to the electronic databases, we hand-searched in Google Scholar with the same keywords to ensure maximum inclusion of relevant papers.

From the literature, we have observed that many researchers use terms like "privacy and online security" or "privacy and internet safety" in their research (Baciu-Ureche, Sleeman, Moody, & Matthews, 2019; Desimpelaere et al., 2020; Just & Berg, 2017; Valente & Cardenas, 2017; Zhang-Kennedy, Abdelaziz et al., 2017), which gives the impression that some researchers may not consider privacy included in the cybersecurity framework directly and may not use terms like "cybersecurity" or "online security" in their privacy-focused studies. Given this observation, we have included "privacy" separately in the keyword list. Here, it is important to note that we did not want to focus on any particular cybersecurity risk; rather, we sought all the risks relevant to children from our review. Thus, we did not use any specific risk terms, other than "privacy", as keywords in our search. We included terms like "online" and "internet" to ensure the maximum inclusion of relevant papers. Our various search queries resulted in a total of 1862 hits that included 1544 unduplicated citations.

3.3. Inclusion and exclusion criteria

Studies were eligible for inclusion if they:

- Presented empirical (qualitative or quantitative) data on cybersecurity awareness research for children.
- Appeared in 2011 or later (we selected this time frame as we wanted to focus on the latest developments in this field).
- Were written in English,
- Were published in a journal or conference proceedings.
- Focused on children.

If a study did not specify the target group, the researchers read the paper to assess whether it would be applicable to children. If it looked relevant, the study was included (for example Maurer, De Luca, & Kempe, 2011); otherwise, it was excluded. The other exclusion criteria were as follows:

- Written in any language other than English.
- "Lessons learned" papers without any empirical evidence or papers based solely on expert opinion.
- Editorials, article summaries, panels, posters, and so on.
- The full text was not available.

3.4. Citation management, retrieval, and inclusion decisions

All the relevant citations (N = 1862) were entered into and stored using EndNote reference management software, after which duplicate citations were removed, with 1544 citations remaining. Fig. 1 shows the systematic review process and the number of papers identified at each stage.

In stage 1, the first author went through all the citations to determine their relevance to this systematic review by checking their titles and abstracts and removing those that were not relevant. As the focus of this review is cybersecurity and children,

Table 1
Quality assessment criteria and considered questions.

Quality criteria	Assessment questions
Empirical research	– Is the paper based on research (or is it merely a "lessons learned" report based on expert opinion)?
Clear statement of the aim	– Is there a rationale for why the study was undertaken? – Is the study's main or secondary focus on cybersecurity risks and awareness for children? – Does the study present empirical data? – Is there a clear statement of the study's primary outcome in terms of its impact on awareness or knowledge or identified risks)?
Description of the context	– Who is the target audience? – In which environment the research was carried out? – The type of software products or materials used in the research. – The being used to raise awareness or address risks.
Research design	– Has the researcher described or justified the research design by, for example, discussing how they decided which methods to use)?
Data collection	– Is it clear how data were collected (e.g. semi-structured interviews, focus groups, etc.)? – Has the researcher made the methods explicit; for example, is there an indication of how interviews were conducted? Did they use an interview guide?
Data analysis	– Was there an in-depth description of the process of analysis? – Have sufficient data been presented to support the findings?
Findings	– Are the findings explicit (e.g., magnitude of effect)? – Has an adequate discussion of the evidence, both for and against the researcher's arguments, been demonstrated? – Are the study's limitations explicitly discussed? – Are the findings discussed in relation to the original research questions? – Are the conclusions justified by the results?
Value of the research	– Does the researcher discuss the contribution the study makes to existing knowledge or understanding, as by considering the findings in relation to current practice or relevant research-based literature)? – Does the study identify new areas in which further research is necessary?

studies addressing other kinds of security, such as infrastructure security or cyber–physical systems security, were excluded. If the first author had any doubt about the relevance of any study and thus the inclusion–exclusion decision, the third author was consulted; both researchers checked the title and abstract again and made the final decision to include or exclude it. Sometimes, study titles and even abstracts do not give a clear indication of their subjects. In such cases, the articles were included for review at the next stage. At the end of stage 1, 110 studies were selected for an in-depth (full text) study (Fig. 1).

In stage 2, the first two authors read the full text of all studies selected in stage 1. It was not always obvious whether a study was empirical by examining its abstract, so, after the full text was read, a study was excluded if it did not provide any empirical evidence or was otherwise not relevant to our review (e.g., not focused on children or not suitable for answering the research questions). Again, in the event of any doubt, all the authors discussed the study, and a final decision to include or exclude was made jointly. After stage 2, a total of 60 studies remained for the quality assessment step of this review.

3.5. Quality assessment

A number of quality assessment questions were devised to assess study quality. For quality assessment, we have considered three quality criteria: rigorousness, credibility, and relevance. These criteria and quality assessment questions were adapted from Dybå and Dingsøyr's (2008) checklist. The quality assessment questions we used are presented in Table 1. A detailed quality analysis of the studies was carried out by the first author and is presented found in Appendix B.

For each criterion a study met, it received one point; if a criterion was not met, no points were awarded. The maximum score a study could obtain was eight. If a study received fewer than four points, it was excluded. In addition, if either question 1 or both questions 2 (aim) and 3 (context) received a "No" response for a given study, the study was excluded before quality assessment was concluded. After the quality assessment, four more papers were excluded. Thus, after stage 3, 56 studies were selected for data synthesis. A list of the selected studies appears in Appendix A, and a brief overview of the studies can be found at Quayyum (2020).

3.6. Data extraction

We extracted data from each of the 56 studies according to a predefined extraction form (Table 2) that enabled us to record the full details of the studies for review and to be specific about how each addressed our research questions. The data extraction process was carried out by the first and second authors. For half the studies, two of the authors extracted data separately and then discussed them to clarify any disagreements. For the rest of the papers, the first author extracted the data, and the second author cross-checked the extracted data to ensure the consistency of the data extraction process.

After extracting the study details, research settings, research methods descriptions, findings, and implications reported by study authors, the data files were copied into MaxQDA, a specialized software package for the qualitative analysis of textual data for further data analysis.

3.7. Synthesis of findings

We used thematic synthesis to synthesize the results, following the steps recommended by Cruzes and Dybå (2011). We took an integrated approach to the synthesis process. Keeping the research questions in mind, we first coded the data using the original authors' terms. Those codes were then reviewed, and similar codes were merged. Afterward, the codes were categorized into themes based on our research questions, keeping the concepts unchanged from the studies' original authors. Finally, we prepared using maps and tables to present the synthesized findings. The findings are described in the following section.

Table 2
Template of the data extraction form.

1. Study overview	
Study identifier	Unique ID for the study
Extraction date	
Bibliographic reference	Author, Title, Year, Publication Source
2. Design of the study	
Study type	Qualitative, Quantitative or Mixed
Research methodology	Case study, Experiment, Action research, Interview, Survey, Other methods
Research Questions/Hypothesis	
Research context	What are the aims of the study? What are the objectives?
Target audience (age)	
Theory/Model/Framework used	
3. Cybersecurity risks	
What risks have been addressed and focused on?	
4. Approach to raise awareness	
What approach has been used to raise cybersecurity and privacy awareness?	
Description of "How the approach has been used"	What kind of activities has been used? What was the effect of the approach (success/failure and effective or not)?
5. Measuring cybersecurity awareness	
How has cybersecurity and privacy awareness been measured?	What type of awareness has been measured? What parameters have been used to measure?
6. Variables used in the study	
Dependent variables	Name, Definition, and Data Collection Procedure
Independent variables	Name, Definition, and Data Collection Procedure
7. Data collection and analysis	
Data analysis (qualitative or quantitative)	
Data collection instrument	
Sample size and age	
Data analysis method	
8. Evaluation	
Evaluation method	Has the study evaluated its approach and solution? What method was used?
Factors	What factors have been considered for evaluation?
9. Results and findings	
Findings	What are the results and findings?
Implications	What are the implications of the research?
Threats to validity and limitations	

4. Results

4.1. Overview of studies

Methods. Table 3 presents an overview of the methods used by the studies along with the references of the studies from each method category.

Publication channels. The distribution of the studies between journals and conferences was almost equal; 29 studies were published in conference proceedings, 27 in journals. A detailed list of the publication channels and occurrences appears in Appendix C.

Six studies included in this review were published in the journal *Computers in Human Behavior* and two in the *International Journal of Child–Computer Interaction*. As to conferences, four studies were published in proceedings of the ACM Conference on Human Factors in Computing Systems and three in proceedings of the ACM Computer Supported Cooperative Work and Social Computing. The International Symposium on Human Aspects of Information Security and Assurance and Symposium on Usable Privacy and Security (SOUPS) included two studies each. Other than these journals and conferences, all publication channels had one occurrence each.

Publication frequency. As to publication year, as we noted in Section 3.3, we included studies published in 2011 and afterward. Five studies from this review were published in 2020, nine in 2019, six in 2018, eight in 2017, seven in 2016, ten in 2015, three in 2014, five in 2013, one in 2012, and two in 2011.

4.2. RQ1. Cybersecurity risks

Through our first research question (Which cybersecurity risks are addressed in current research for children?), we aimed to identify the common cybersecurity risks to children explored by researchers, and we have indeed identified various risks and categorized them into groups. Fig. 2 presents an overview of the risks. However, before the risks are presented, it is essential to note that some studies also focused on topics not directly tied to cybersecurity, examining instead topics related to internet use and the fundamentals of networking. For example, Giannakas et al. (2016) developed a mobile app called *CyberAware* that is designed for cybersecurity education and awareness for children. With *CyberAware*, the researchers aim to familiarize students with the fundamental cybersecurity topics required to use the internet safely and keep internet-connected devices protected against threats. The topics include firewall technologies, antivirus software, security patches and updates, email spam filters, legacy threats, malware, cyberattacks, and spam. Baciu-Ureche et al. (2019) developed an online learning aid called *The Adventures of ScriptKitty*, which aims to teach children about different internet safety topics, including internet fundamentals, networking, packet sniffers, password management, and social engineering. Amo et al. (2019) propose instructional interventions for teens to learn about cybersecurity concepts like networking, phishing, cryptography, system administration, and web design. Reid and

Table 3
Methods used by the studies. *Bioglio et al. (2019) has used two methods.

Method	Study reference
Survey	Ahmad, Arifin, Mokhtar, Hood, Tiun, and Jambari (2019), Bernadas and Soriano (2019), Choong, Theofanos, Renaud, and Prior (2019), Clemons and Wilson (2015), Dempsey, Sim, and Cassidy (2018), Hamdan et al. (2013), Hofstra, Corten, and van Tubergen (2016), Maoneke, Shava, Gamundani, Bere-Chitauro, and Nhamu (2018), Martin, Wang, Petty, Wang, and Wilkins (2018), Moreno, Egan, and Bare (2013), Sezer, Yilmaz, and Yilmaz (2015), Shin and Kang (2016), Teimouri, Benrazavi, Griffiths, and Salleh Hassan (2018), Türker and Çakmak (2019) and Wisniewski et al. (2015)
Experiment	Alemany, del Val, Alberola, and García-Fornes (2019), Amo, Liao, Frank, Rao, and Upadhyaya (2019), Baciu-Ureche et al. (2019), Bioglio et al. (2019), Desimpelaere et al. (2020), Lastdrager et al. (2017), Maurer et al. (2011), Zhang-Kennedy, Abdelaziz et al. (2017) and Zhang-Kennedy, Baig and Chiasson (2017)
Case study	Agarwal and Singhal (2017), Baracaldo, López, Anwar, and Lewis (2011), Hung, Iqbal, Huang, Melaisi, and Pang (2016), Reid and Van Niekerk (2014) and Valente and Cardenas (2017)
Literature review	Alotaibi et al. (2016), Aponte and Richards (2013), de Paula Albuquerque et al. (2020) and Tsirtsis et al. (2016)
Interview	Amancio, Fantinato, Hung, Coutinho, and Roa (2018), Kumar et al. (2017), Muir and Joinson (2020) and Staksrud et al. (2013)
Document analysis	Cullinane et al. (2015), Prior and Renaud (2020) and Von Solms and Von Solms (2014, 2015)
Focus group	Bannon, McGlynn, McKenzie, and Quayle (2015), Just and Berg (2017) and Zhao et al. (2019)
Secondary analysis	Feng and Xie (2014), Jia, Wisniewski, Xu, Rosson, and Carroll (2015) and Wisniewski, Jia, Xu, Rosson and Carroll (2015)
Proof of concept with survey	Giannakas et al. (2016), Meng, Zakaria, Bindahman, Alias, and Husain (2012) and Salazar, Gaviria, Laorden, and Bringas (2013)
Diary study	Wisniewski, Xu, Rosson, and Carroll (2017) and Wisniewski, Xu, Rosson, Perkins, and Carroll (2016)
Participatory design	Bioglio et al. (2019) and Kumar et al. (2018)
Hazard matching	Jeong and Chiasson (2020)
Meta-analysis	Kritzinger (2015)
Quasi-experimental study	Vanderhoven, Willems, Van Hove, All, and Schellens (2015)

Van Niekerk (2014) report on a study of a cybersecurity educational campaign that aims to foster a cybersecure culture among youth in South Africa. The topics covered in this campaign include browsing and downloading, cyber citizenship, cybercrime, social networking, password and hardware security, and cyber identity management. In addition to these topics, two studies mention online etiquette (Kritzinger, 2015; Türker & Çakmak, 2019). Kritzinger (2015) searched online resources to identify cybersecurity issues and found digital footprints, digital reputation, chatrooms, the trustworthiness of online materials, issues with free downloads, plagiarism, and online consequences. However, all these studies have a similar aim as the rest of the research in this review: increasing cybersecurity awareness among children and ensuring their safe internet use.

4.2.1. Online privacy

The studies address many issues related to online privacy; some studies examine online privacy risks in general, while others investigate those risks in specific contexts such as social media or smart toys. Other topics include third-party data tracking (Clemons & Wilson, 2015; Desimpelaere et al., 2020; Zhao et al., 2019), the influence of different factors on privacy behavior (Bernadas & Soriano, 2019; Shin & Kang, 2016), children's level of privacy knowledge and awareness (Dempsey et al., 2018), and how different approaches can increase children's privacy literacy and awareness (Desimpelaere et al., 2020; Zhang-Kennedy, Abdelaziz et al., 2017; Zhang-Kennedy, Baig et al., 2017). A more detailed breakdown of privacy-related risks is presented in Fig. 3.

Privacy in social networks

Some studies investigate privacy-related risks in the context of social networks. Several examine privacy risks and different aspects of teens' privacy behavior on Facebook, including teens' privacy concerns and peer influences (Hofstra et al., 2016), the relationship between teens' level of online privacy concern and their privacy-protecting behaviors (Feng & Xie, 2014), and the cognitive mechanisms behind privacy behaviors on Facebook (Jia et al., 2015). The studies propose a multitude of educational interventions and tools to raise privacy risk awareness on social networks (Baracaldo et al., 2011; Meng et al., 2012; Vanderhoven et al., 2015).

Some studies also discuss specific privacy risks that children can encounter on social networks. One is the geo-tagging of photos taken with smartphones and uploaded online (Zhang-Kennedy, Baig et al., 2017). This study illustrates how geo-tagged photos threaten online privacy and discusses the possible consequences of photo sharing. Though this study (Zhang-Kennedy, Baig et al., 2017) does not explicitly mention the risk on social media, the researchers do use social media as a context for their privacy test. Thus, we have included this risk in this category. Another privacy risk in social networks is oversharing of information (Salazar et al., 2013; Zhao et al., 2019). Salazar et al. (2013) designed a presentation model aimed to teach cybersecurity measures to teenagers; these researchers categorized over-sharing as one of the main ways in which high school students can have their information security compromised. Wisniewski et al. (2017, 2016) asked teens and parents to report potential types of online risks and use information breaches as one of their four predefined categories of risk. In their study, the authors define information breaches as "personal information or photos being shared or used online without teens' permission or those shared by teen and later regretted". Martin et al. (2018) surveyed teenagers about their social media use; the teens reported their concern about social media accounts being hacked as a safety or privacy issue. Thus, hacking of social media accounts is also categorized as a privacy risk related to social networks.

Privacy in smart toys

Our review found four studies addressing privacy issues related to smart toys. de Paula Albuquerque et al. (2020) conducted a literature review on smart toy-related children's privacy risks and the major strategies to mitigate such risks. They identify various privacy risks that can be caused by smart toys, such as exposing sensitive information, dataveillance, and advertisement. Amancio et al. (2018) evaluate the perceptions of potential Brazilian consumers about issues involving children's privacy and the use of smart toys. Hung et al. (2016) discuss privacy requirements for smart toys in a toy computing environment through a case study on *Hello Barbie*, a commercial smart toy from Mattel. They also explore various scenarios and illustrate how a child can unintentionally reveal sensitive information when communicating with a smart toy, leading to a serous privacy risk. Finally, Valente and Cardenas (2017) analyze the security practices and possible vulnerabilities of three smart toys that communicate with children through voice commands. They focus on weaknesses in the encryption scheme in the smart toys and note that weak encryption can expose children's voice contents to eavesdroppers and risk audio injection attacks using the device (Valente & Cardenas, 2017).

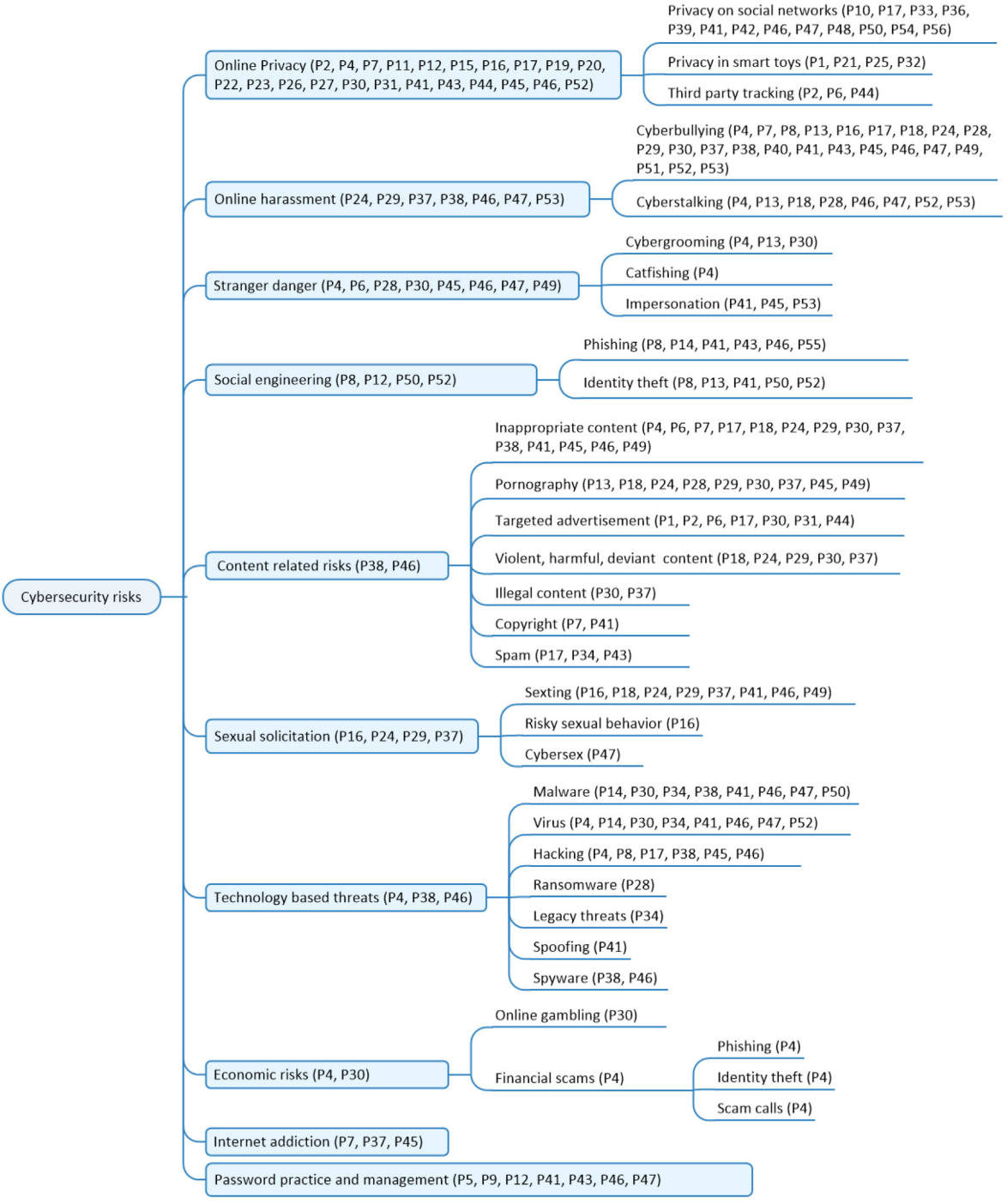

Fig. 2. Cybersecurity risks.

4.2.2. Online harassment

Harassment-related risks result from different forms of unwanted online contact. Cyberbullying and cyberstalking are the two most common forms of online harassment found in the literature (see Fig. 4).

Cyberbullying

Cyberbullying is one of the most frequently cited cybersecurity risks in the literature. Cyberbullying involves bullying through the use of technology such as the internet and cellular phones (Aponte & Richards, 2013). Studies have addressed multiple issues related to cyberbullying, such as determining awareness levels of teachers concerning cyberbullying (Sezer et al., 2015), how cyberbullying may affect teenagers and proposed countermeasures to support them (Hamdan et al., 2013), and so on. Several studies explore the cybersecurity risks to which children and teens can be exposed and identify cyberbullying as one of the main cybersecurity risks (Maoneke et al., 2018; Wisniewski et al., 2017, 2016). Aponte and Richards (2013) categorize different kinds of cyberbullying and explore a variety of behavioral and psychological issues relating to cyberbullying.

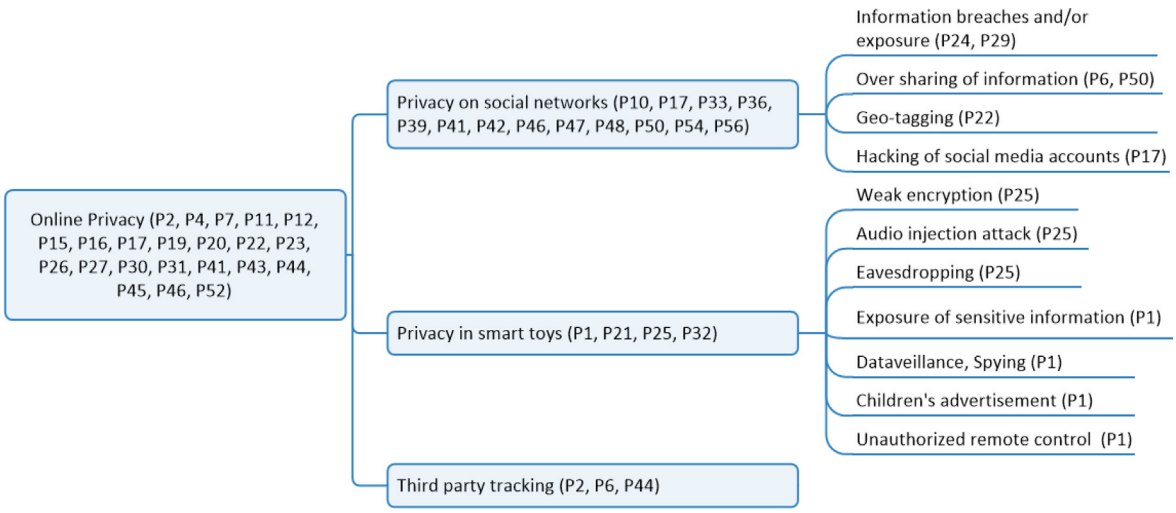

Fig. 3. Privacy-related risks.

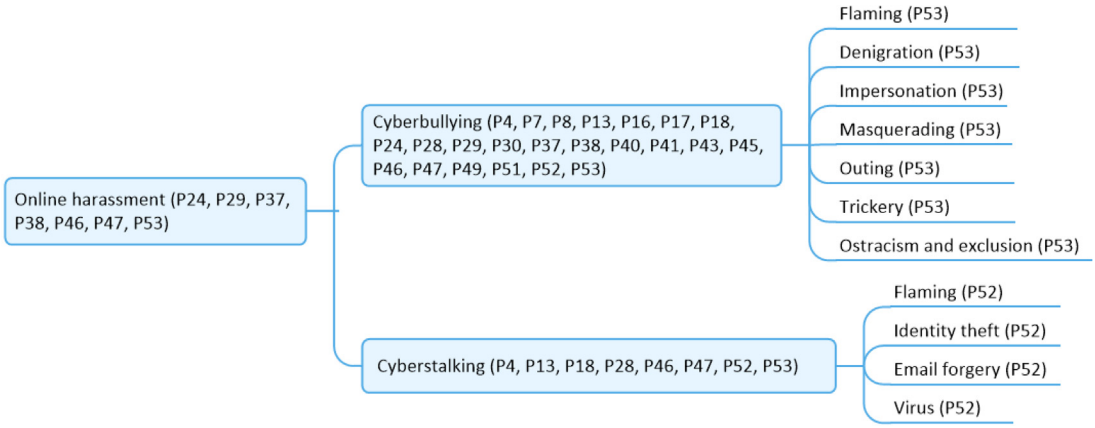

Fig. 4. Cyberharassment and cyberbullying.

Cyberstalking

Cyberstalking refers to harassing someone through unwanted communication using technology including computers, global positioning systems (GPS), cell phones, cameras, and the like (Hamdan et al., 2013). Hamdan et al. (2013) surveyed teenagers to investigate and identify the various cybersecurity threats they experience and identified cyberstalking as one of the most commonly encountered. Aponte and Richards (2013) conducted a literature review to identify cybersecurity risks for children; cyberstalking is one of them.

4.2.3. Stranger danger

"Stranger danger" is the idea that potential physical and emotional ramifications of children can occur by interacting with strangers online and forming relationships with people that they have not met in person. Muir and Joinson (2020) report concerns around online stranger danger, which covers a range of issues like catfishing, online grooming, and cyberstalking. Online grooming risks can result from the online interaction between a child and an adult (Ahmad et al., 2019; Muir & Joinson, 2020; Tsirtsis et al., 2016); the adult befriends a child online and builds an emotional connection with (undisclosed) harmful intentions. For online grooming purposes, people often impersonate others; impersonation is also used to steal confidential information (Aponte & Richards, 2013).

4.2.4. Social engineering attacks

With social engineering, attackers usually try to trick computer users into giving them sensitive information. Our review reveals two types of social engineering attacks that researchers have explored to raise awareness among children.

Phishing

Phishing is commonly thought to be equivalent to theft of credentials of financial institutions (Lastdrager et al., 2017), but the researchers in study (Lastdrager et al., 2017) discuss why children are also vulnerable to phishing attacks. They carried out an experiment to test children's ability to recognize phishing and measured the effect of that intervention. Maurer et al. (2011) implemented a warning concept as a Firefox plugin that can help users identify fraudulent (or phishing) websites and evaluated it in a series of studies. Amo et al. (2019) conducted two interventions for children in which participants could learn about different cybersecurity concepts, including phishing.

Identity theft

Like phishing attacks, identity theft has been recognized in many studies as a relevant cybersecurity risk for children. With the amount of personal information shared on multiple web services and social networks, it can be difficult for anyone to maintain appropriate control in this area (Salazar et al., 2013), and losing control over personal information can lead to that information being compromised through identity theft. Studies including (Ahmad et al., 2019; Hamdan et al., 2013; Kritzinger,

2015; Lastdrager et al., 2017; Salazar et al., 2013) discuss identity theft risks for children and offer several recommendation to help children recognize online misbehavior and take the necessary actions to avoid risks.

4.2.5. Content-related risks

Content-related risks involve being subjected to harmful or offensive content or being influenced to produce or distribute such content (Von Solms & Von Solms, 2015). Many kinds of content that can be risky for a child to be exposed to; the most commonly mentioned form is exposure to inappropriate content; that is, content that is inappropriate for children's age and experience level (Türker & Çakmak, 2019). Many studies, including (Maoneke et al., 2018; Martin et al., 2018; Muir & Joinson, 2020; Türker & Çakmak, 2019; Wisniewski et al., 2016; Zhao et al., 2019), mention this risk. Another common form of content-related risk is exposure to pornographic content (Maoneke et al., 2018; Wisniewski et al., 2017, 2016). Unwanted or targeted advertisements (de Paula Albuquerque et al., 2020; Desimpelaere et al., 2020; Martin et al., 2018; Shin & Kang, 2016; Tsirtsis et al., 2016; Zhao et al., 2019), violent, harmful or illegal content (Maoneke et al., 2018; Tsirtsis et al., 2016; Wisniewski, Jia, Wang et al., 2015; Wisniewski et al., 2017, 2016), and spam (Cullinane et al., 2015; Giannakas et al., 2016; Martin et al., 2018) are some of the other major content-related risks. Beyond risks, copyright violation can be also an issue with online content (Kritzinger, 2015; Türker & Çakmak, 2019).

4.2.6. Sexual solicitation

Sexual solicitation refers to sexting or any requests received by a stranger, acquaintance, or friend that are sexual in nature (Wisniewski et al., 2017, 2016). Studies (Wisniewski et al., 2017, 2016) have explored teens' online risk experiences and categorized certain risks as related to sexual solicitation. Sexting, which means sending or receiving sexual images, videos, or texts online, is a common form of sexual solicitation that many research studies have discussed (Kritzinger, 2015; Maoneke et al., 2018; Staksrud et al., 2013; Teimouri et al., 2018; Von Solms & Von Solms, 2014; Wisniewski, Jia, Wang et al., 2015; Wisniewski et al., 2017, 2016). Sexual solicitation can also lead children to engage in risky sexual behavior online (Reid & Van Niekerk, 2014; Teimouri et al., 2018).

4.2.7. Technology based threats

Technology-based threats include attacks on devices that can result in data loss or loss of functionality. Among the most frequently cited threats of this kind are malware, viruses, and hacking. Malicious software with sophisticated malware, spyware, or viruses can lead to serious risks of exposing sensitive information, hacking of accounts or devices, and so on (Salazar et al., 2013). Amo et al. (2019) reports on an intervention for children, in which the researchers arranged a workshop focused on viruses and malware; the students learned how they are employed by hackers or attackers to cause damage to important data and obtain private information and how to guard themselves against such attacks. Other technology-based threats include legacy threats (Giannakas et al., 2016), spoofing (Kritzinger, 2015), and ransomware attacks (Agarwal & Singhal, 2017).

4.2.8. Economic risks

It has become common for children to spend exorbitantly online if they obtain access to online payment methods through internet-connected devices like mobile phones or online services (Tsirtsis et al., 2016). The most widespread form of economic risks are online gambling (Tsirtsis et al., 2016) and financial scams (Muir & Joinson, 2020). Children can become victims of financial scams in different ways, such as phishing, identity theft, or scam calls (Muir & Joinson, 2020). Tsirtsis et al. (2016) also mention online games, which can carry economic risks. Though such games are not cybersecurity risks themselves, sometimes children engage in online purchases intentionally or unintentionally by buying different features or premium functionalities in them. The authors note that such events usually happen when services do not clarify that there could be additional charges in the course of using a product or service. As a result, enormous amounts of money can be lost through fraudulent transactions.

4.2.9. Internet addiction

Though internet addiction is not a security risk in itself, it is an important dimension in safe and responsible internet use. We have included internet addiction in the list of risks as it can be a significant predictor for risky cybersecurity behaviors; it can have similar negative physical and behavioral consequences as other cybersecurity risks. In Türker and Çakmak (2019), the researchers investigated students' and teachers' awareness of the safe and responsible use of the internet, using internet addiction as one of the dimensions to measure cyberwellness and awareness. Two other studies also address the issue of internet addiction (Bannon et al., 2015; Wisniewski, Jia, Wang et al., 2015). Wisniewski, Jia, Wang et al. (2015) investigate whether resilience can reduce online risk exposure and the negative effects of internet addiction. Bannon et al. (2015) examine the understanding of online risks among young people with additional support needs; some of the participants expressed concern over spending a large amount of time online, which they felt may have an impact on them in their offline environment.

4.2.10. Password practices and management

As children are increasingly engaging in an online world without the necessary knowledge and skills to use passwords wisely, they are prone to cybersecurity risks. Thus, researchers have identified this issue as one of the most important topics in cybersecurity (Cullinane et al., 2015; Kritzinger, 2015; Reid & Van Niekerk, 2014; Von Solms & Von Solms, 2014). Some researchers have also explored children's practices, perceptions, and knowledge regarding passwords (Choong et al., 2019) and derived an ontology of best-practice password principles for children (Prior & Renaud, 2020). Baciu-Ureche et al. (2019) have developed a free online, story-based educational aid that aims to improve cyber-awareness among children through practical exercises. In their learning aid, the researchers have included a separate chapter on password security and addressed the dangers of weak passwords.

4.2.11. Findings regarding the risks

Multiple studies in this review conducted surveys to identify different risks but have not performed in-depth research focusing on specific risks. In Fig. 5, we have presented the findings from studies that are devoted to specific cybersecurity risks. However, not all the risks or all findings from the studies in this review are listed in the figure.

4.3. RQ2. Approaches to raise cybersecurity awareness

We have divided this section into two parts. In the first, we present the relevant theories in cybersecurity awareness research involving children on which some studies in this review are grounded; the second presents the approaches researchers have used to raising cybersecurity awareness.

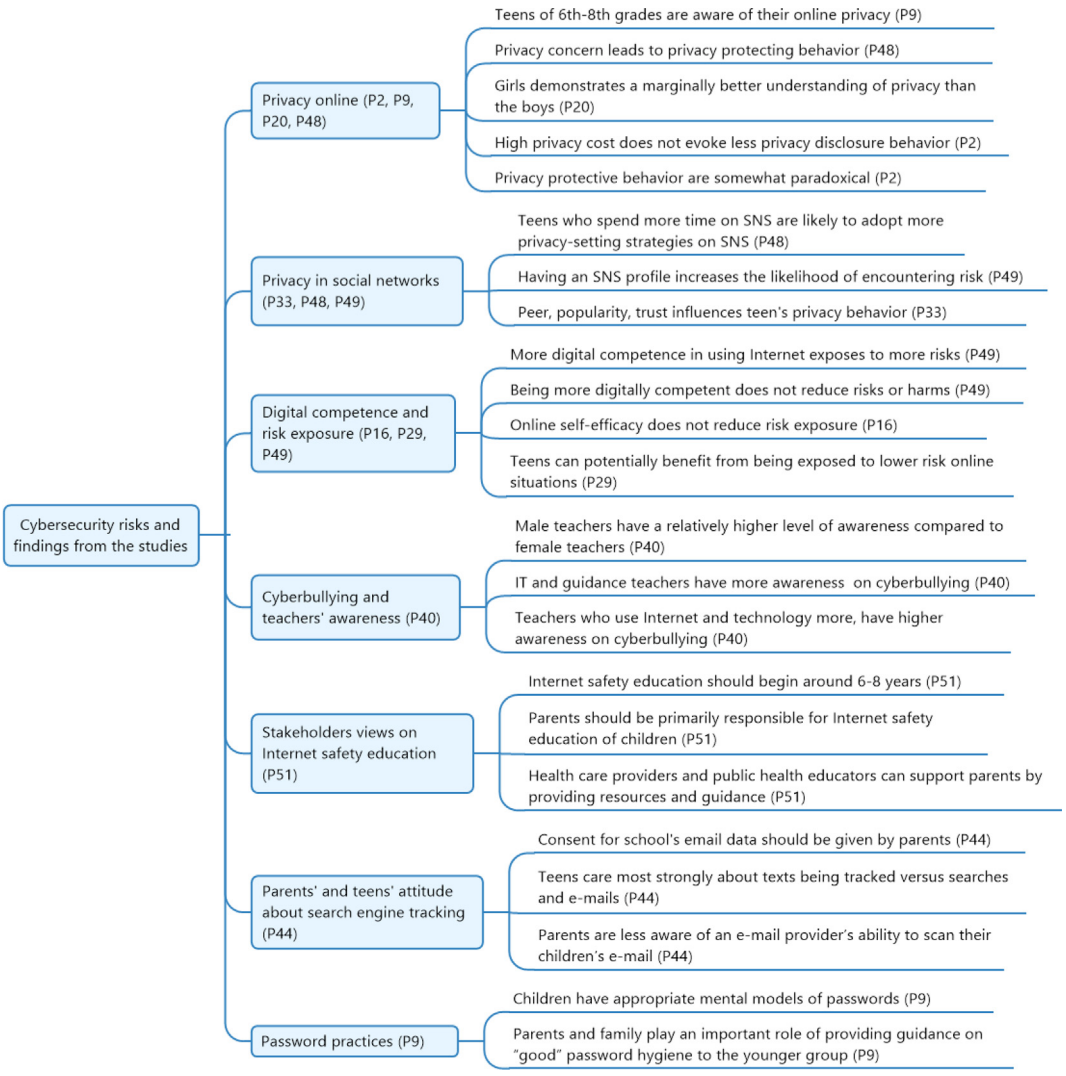

Fig. 5. Findings related to cybersecurity risks from the studies.

4.3.1. Relevant theories and models behind the studies

Knowing the relevant theories is essential to guide the research work and give meaning to what we see and do as researchers. Given that, we have reviewed which theories are relevant in this research area and how different researchers have used their chosen methods in their studies. Some articles in this review have included such theories in their research to facilitate the development of learning materials and improve children's learning processes. Table 4 presents an overview of the theories and models; in the following section, we briefly describe how the studies use these theories.

Piaget's *theory of cognitive development* is a well-known learning theory in child education research that suggests that children in their concrete operational stage (from roughly 7 to 11 years old) can "work things out in their heads" (Lee, 2000). Dempsey et al. (2018) designed an activity workbook using Piaget's theory of cognitive development. Kumar et al. (2017) and Zhao et al. (2019) both ground their work on Vygotsky's *zone of proximal development (ZPD)* theory (Brown et al., 2003), and Nissenbaum's *theory of contextual integrity (CI)* (Nissenbaum, 2010). ZPD is a well-established learning theory that relates the difference between what learners can do independently to what can be achieved through guidance by a skilled partner (Zhao et al., 2019). Nissenbaum's CI is a theory of privacy that can be used to interpret people's perceptions of privacy. Both Kumar et al. (2017) and Zhao et al. (2019) use the CI framework to understand children's mental models concerning privacy and security. Other studies have also grounded their work on privacy-related theories, such as the *privacy calculus theory* (Zhang et al., 2018) and the *Antecedents-Privacy Concerns-Outcome (APCO) Macro Model* (Smith et al., 2011). Privacy calculus theory is often used to explain the underlying cognitive processes that occur when individuals are asked to share personal data (Desimpelaere et al., 2020; Zhang et al., 2018). Desimpelaere et al. (2020) used it to investigate how privacy literacy training can increase children's privacy awareness, influence their online disclosure behavior, and heighten their understanding of different levels of privacy costs. The APCO Macro Model is another privacy-focused model, which Jia et al. (2015) use to investigate teens' privacy behaviors in online information privacy management. Another important theory found in the studies is *resilience theory* (Fergus & Zimmerman, 2005). It was originally derived and validated by researchers in developmental psychology, which is useful in explaining outcomes related to adolescents' online risk exposure and a number of risky teen behaviors. Wisniewski, Jia, Wang et al. (2015) and Wisniewski et al. (2016) use this adolescent resilience theory (Fergus & Zimmerman, 2005) to study the role of resilience in protecting teens from online risk exposure and the negative effects of internet addiction.

Table 4
Theories and models the studies have used.

Theory	Description	Ref.
Privacy calculus theory	Privacy calculus theory is often used to explain the underlying cognitive processes that take place when individuals are requested to share personal data (Zhang et al., 2018). This theory proposes that individuals first perform a cost–benefit analysis when they are asked to share their personal details.	Desimpelaere et al. (2020)
Vygotsky's ZPD theory	ZPD relates the difference between what learners can do independently and what can be achieved by through guidance by a skilled partner (Brown, Heath, & Pea, 2003). An individual's ZPD is the distance between what he or she can do without help and what he or she is capable of doing with help.	Kumar et al. (2017) and Zhao et al. (2019)
Nissenbaum's CI theory	The CI theory states that information flows according to the norms that govern a given situation. These norms vary based on the context of the situation and are shaped by cultural, ethical, moral, and legal factors (Nissenbaum, 2010). The framework has four components: context, attributes, actors and transmission principles.	Kumar et al. (2017) and Zhao et al. (2019)
Piaget's theory of cognitive development	This theory suggests that children in their concrete operational stage (roughly 7 to 11 years old) are able to "work things out in their heads" (Lee, 2000). At this age children should be competent enough to use digital devices on their own and may risk revealing private information.	Dempsey et al. (2018)
ARCS motivational model	The ARCS Model is a method for improving the motivational appeal of instructional materials (Keller, 1987). Its main purpose is to inform the design of a learning app so as to be more intrinsically interesting to learners. ARCS consists of four major components for promoting and sustaining motivation during the learning process; namely, attention, relevance, confidence, and satisfaction.	Giannakas et al. (2016)
APCO macro model	The APCO model (Smith, Dinev, & Xu, 2011) is versatile as it includes information privacy-related factors ranging from the individual level through group and organizational levels to the societal level. At the center of the APCO model, privacy concern functions as a "proxy" for information privacy and represents the beliefs, attitudes, and perceptions of privacy at the individual level of analysis. APCO then abstracts a variety of antecedents and outcomes of privacy concerns across several research streams in the literature.	Jia et al. (2015)
Resilience theory	Resilience is the ability to overcome negative effects associated with risk exposure; it helps an individual cope with traumatic experiences (Fergus & Zimmerman, 2005). The theoretical framework of adolescent resilience was derived and validated by researchers in developmental psychology (Fergus & Zimmerman, 2005). The outcomes associated with resilience theory are not simply whether or not teens are exposed to risk, but rather whether they are able to thrive in spite of it (Fergus & Zimmerman, 2005).	Wisniewski, Jia, Wang et al. (2015) and Wisniewski et al. (2016)
PMT and HBM	HBM is one of the primary theories of health behavior, while the PMT (Rogers, 1975) is widely employed as a model for safe decision-making and taking actions regarding health behavior. The PMT originated as an extension and reworking of the HBM intended to protect individuals from risky health behaviors by educating them about threat appraisal (severity and susceptibility) and coping (response efficacy, self-efficacy) (Rosenstock, Strecher, & Becker, 1988)	Teimouri et al. (2018)
Family systems theory	A family system is portrayed as a dynamic process in which parents and children iteratively and bidirectionally influence one another over time (Cummings, Bergman, & Kuznicki, 2014). The three main tenets of family systems theory are a focus on transactional and bi-directional processes, longitudinal effects, and multi-level analysis (individual, dyadic, etc.) (Cummings et al., 2014).	Wisniewski et al. (2017) and Wisniewski et al. (2016)
Parental mediation theory	Parental mediation refers to strategies that parents employ to control and supervise their children's media use (Warren, 2001). Parental mediation theory acknowledges that children can be affected by their exposure to media but holds that such media effects can be mediated or mitigated by the extent to which parents are involved in monitoring and supervising their children's media use (Mesch, 2009).	Shin and Kang (2016)

Giannakas et al. (2016) use the *Attention, Relevance, Confidence, and Satisfaction (ARCS) motivational model* to design instructional material for children that sustains motivation. The main purpose of the ARCS model is to make the design of a learning app more intrinsically interesting to learners (Giannakas et al., 2016). Teimouri et al. (2018) develop the theoretical framework of their study based on aspects of the *protection motivation theory (PMT)* (Rogers, 1975) and *the health belief model (HBM)* (Janz & Becker, 1984). HBM is a widely known theory of health behavior of which PMT is an extension intended to protect individuals from risky health behaviors (Teimouri et al., 2018). Teimouri et al. (2018) use the PMT and HBM to study children's level of privacy concerns, children's perceptions of exposure to online risks, safety in adopting online protection behavior, and online self-efficacy.

Other than these theories, the studies in the review also employ theories that focus on children's relationships and communication with their parents and families. For example, *the family systems theory* (Cummings et al., 2014) posits that a family is a complex system and dynamic process in which parents and children iteratively and bidirectionally influence one another over time. Wisniewski et al. (2017, 2016) use the family system theory in their research on the context of understanding adolescent online risk experiences and how they communicate with their parents regarding those experiences. Another important theory that involves parents is *parental mediation theory* (Mesch, 2009). Shin and Kang (2016) ground their study on parental mediation theory, using it to help their investigation of the role of parents and parental mediation in adolescents' online privacy concerns and information-disclosing behaviors.

4.3.2. Approaches

In reviewing the studies, we found multiple approaches to raise cybersecurity awareness, as presented in Fig. 6. This section discusses those approaches, the techniques associated with them, and the findings they enabled. Here, we note that we have used the terms that the papers' authors employ in the studies to define their approaches. For example, Lastdrager et al. (2017) use storytelling with video presentations as a method to share knowledge

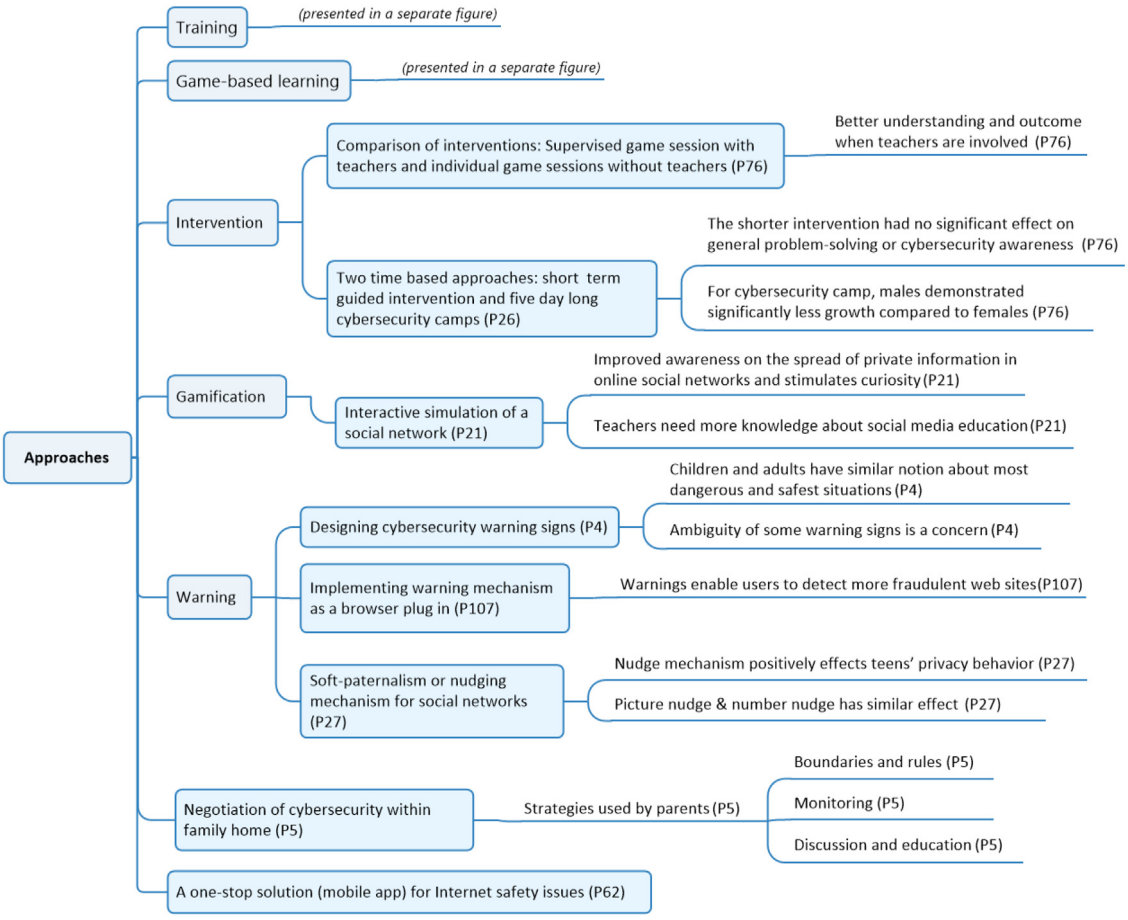

Fig. 6. Approaches to raising cybersecurity awareness found in the review.

and to attract children's attention; Vanderhoven et al. (2015) use a serious game in the interventions to study teachers' role and influence. The authors of these papers have not called their approach gamified or game-based; they call their approaches training and intervention, respectively.

Training

The most commonly used awareness approach was training (Fig. 7). We found six techniques that researchers use to train children about cybersecurity risks and concepts: informative video (Desimpelaere et al., 2020), interactive presentation with storytelling (Lastdrager et al., 2017), digital comics (Baciu-Ureche et al., 2019; Zhang-Kennedy, Abdelaziz et al., 2017; Zhang-Kennedy, Baig et al., 2017), making a school curriculum (Von Solms & Von Solms, 2015), developing and using tools (Meng et al., 2012), and proposing a best-practice ontology for passwords (Prior & Renaud, 2020).

All the techniques showed positive outcomes and proved effective at raising awareness of various cybersecurity risks. Though all the techniques had positive outcomes, one study (Meng et al., 2012) does report ineffectiveness among some users. In Meng et al. (2012), the authors discuss users who were not satisfied with the tools for at least two reasons: its simple user interface made it hard for the users to believe the recommendations provided by the tool, and some believed that their privacy on social networks was already protected by those networks' privacy rules and regulations, making an additional privacy management tool unnecessary.

Game-based learning

Three studies use games and game-based learning as their approach to raise cybersecurity awareness (Giannakas et al., 2016; Kumar et al., 2018; Salazar et al., 2013)(see Fig. 8). The researchers in Kumar et al. (2018) conducted three sessions with children using existing resources (games, game prototypes, and interactive stories); based on the results, they offer recommendations for designing privacy-related educational resources for children. Study (Giannakas et al., 2016) reports that playing the serious game increased knowledge acquisition among students, but study (Salazar et al., 2013) indicates that using a serious game did not have a significant impact on students' knowledge acquisition when compared to their knowledge acquisition after an information presentation, since it did not introduce any new concepts. However, it greatly affected the students' self-awareness of cybersecurity while significantly decreasing their confidence in technology, which was an intended effect of the study.

Warning

Warnings are a type of communication designed to prevent people from harm; they can alert users of threats, remind users, or trigger changes in user behavior. As Fig. 6 shows, we found three studies that use warning as an approach to make users aware of cybersecurity risks (Alemany et al., 2019; Jeong & Chiasson, 2020; Maurer et al., 2011). Jeong and Chiasson (2020) explores children's perceptions of warning messages and found that both children and adults had similar notions about which signal items indicated the safest and the most dangerous situations; they expressed similar concepts shaping their risk perceptions of warnings. The researchers also identified ambiguity and mixed interpretations about some cybersecurity warning symbols, including the "open lock" and "police officer" symbol (Jeong & Chiasson, 2020). The other two studies use warnings to alert

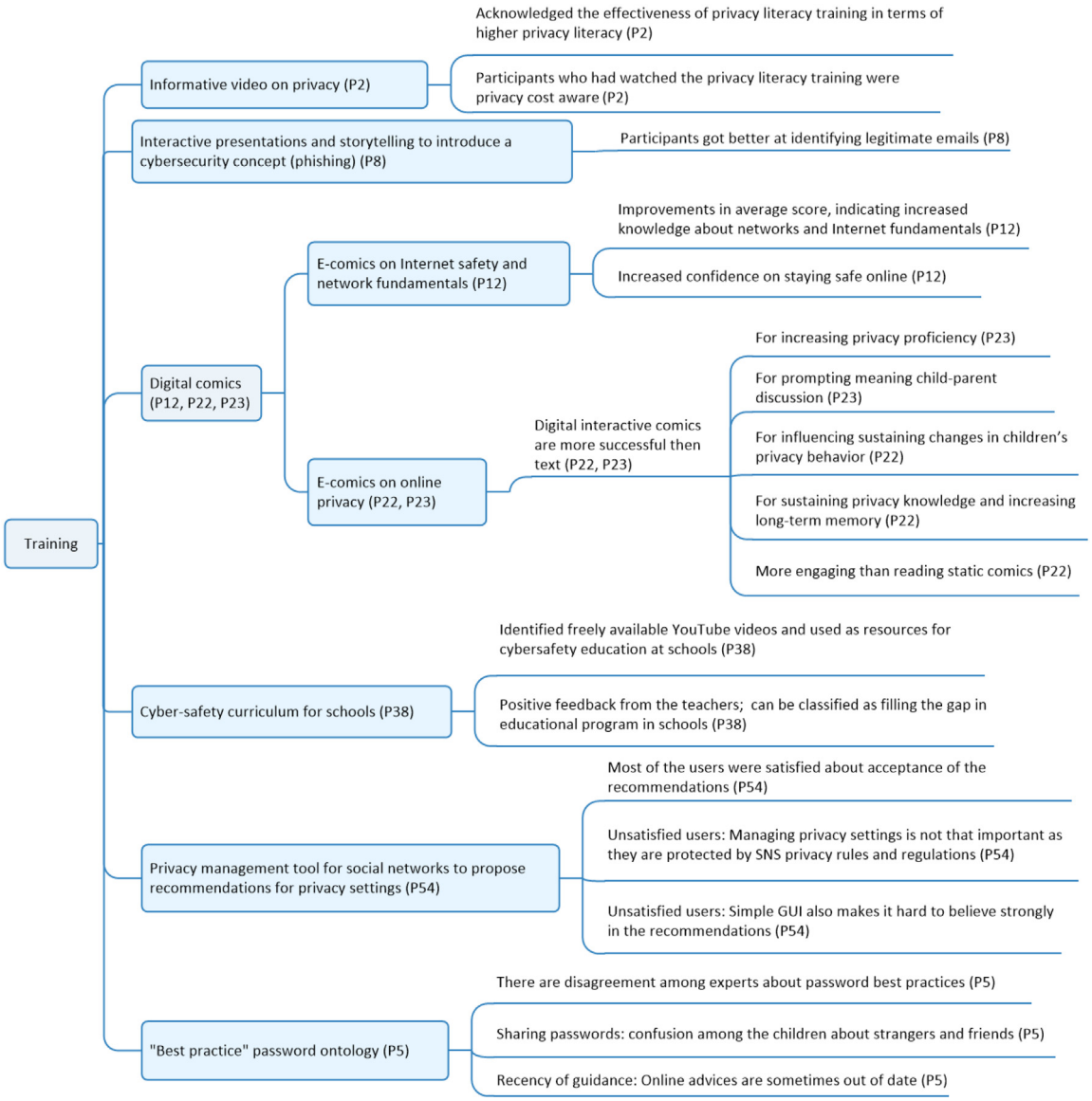

Fig. 7. Training as an approach to raise cybersecurity awareness.

users about possible phishing risks (Maurer et al., 2011) and to nudge users to reconsider their privacy disclosure actions before performing them in social networks (Alemany et al., 2019). Both studies (Alemany et al., 2019; Maurer et al., 2011) show positive results and the effectiveness of warning mechanisms to make users aware of risks.

Intervention

This review includes two studies that use interventions (Fig. 6) as their approach to raise cybersecurity awareness (Amo et al., 2019; Vanderhoven et al., 2015). Both studies also compare different types of interventions. Amo et al. (2019) adopts two time-based approaches, one a short (60-min) workshop and the other a long (5-day) cybersecurity camp. The researchers compared the results of the two interventions and conclude that the long intervention demonstrated very promising results, whereas in the shorter, less intensive intervention, the students did not demonstrate growth in cyberawareness. The authors also state that "the results from this study seem to suggest that in order for interventions to positively affect the relative outcomes, the intensity and type of the intervention matter" (Amo et al., 2019). The other study (Vanderhoven et al., 2015) involved a quasi-experimental study with four short-term interventions in which pupils (1) played a serious game on a tablet computer without teacher involvement, (2) played a serious game on a tablet computer while the teacher summarized the learned content every five minutes, (3) received a traditional course on privacy risks, and (4) received a course on a different topic (as a control condition). The results of this study showed that pupils' awareness of privacy risks increased under all three intervention conditions compared to the control condition, thus proving the effectiveness of the interventions. This study also compare the different forms of interventions as to teacher involvement, finding that pupils were more aware of the topic of the game or course when a teacher was involved in the intervention process.

Gamification

One paper in the review reports using gamification as its approach (Fig. 6) to raising awareness about information sharing in social networks and possible privacy risks. Bioglio et al. (2019) employ a web application that allows children and teenagers to experience the typical dynamics of information spread across an online social network through a realistic interactive simulation. This study shows the effectiveness of the interactive gamification

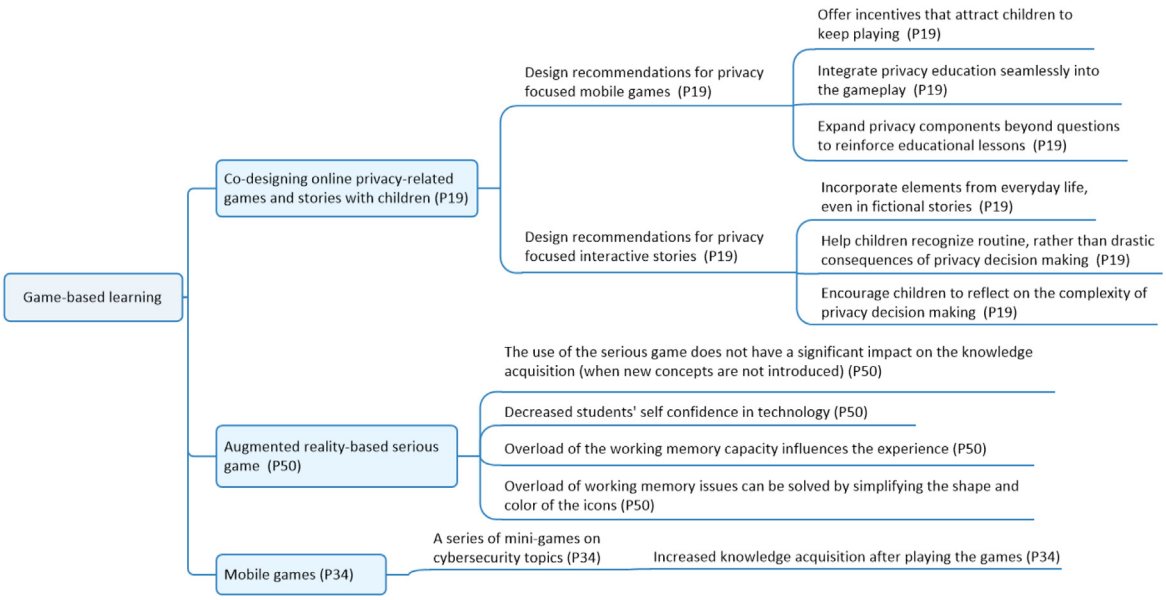

Fig. 8. Game-based learning as an approach to raising cybersecurity awareness.

approach in stimulating students' curiosity and improving their awareness of the spread of private information in online social networks. This study's outcomes also highlight the lack of training and material on social media and privacy-related problems for teachers.

Family negotiation

In addition to the five approaches discussed above, we found two other approaches used to raise cybersecurity awareness. One is family negotiation, which differs from the approaches discussed above by eschewing a formal environment in favor of an informal approach carried out inside a family context. Muir and Joinson (2020) investigate how parents and their children jointly negotiate processes at home in terms of cybersecurity concerns and managing cybersecurity threats. They report that parents and children balance the costs and benefits of using technology. The researchers also describe the cybersecurity risks about which parents and children are concerned and various strategies used by parents to cope with cybersecurity threats and manage cybersecurity within the household.

Mobile app as a one-stop solution

The last approach we found uses a mobile app as a one-stop solution. This approach differs from other mobile application-based awareness-raising approaches found in our review. Agarwal and Singhal (2017) report that this approach is not only for raising awareness but also for providing expert help and consultation to the victim or any individual who asks for help using the app. It can also be used to guide children, parents, and educators about cybersecurity and to provide awareness about their own victimization.

4.4. RQ3. Evaluating cybersecurity awareness

With our third research question (How do researchers evaluate cybersecurity awareness in children?), we sought to understand how researchers evaluate children's cybersecurity awareness; we have also tried to see what factors and techniques researchers have used for their evaluation. After reviewing the papers, we conclude that researchers use two primary techniques to evaluate children's awareness; (i) directly measuring their level of awareness or knowledge and (ii) measuring the effectiveness of their approaches to raise cybersecurity awareness.

4.4.1. Measuring awareness

Zhao et al. (2019) measured the online privacy risk awareness of children in terms of (i) their ability to recognize privacy-related contexts and (ii) their responses to different types of explicit and implicit threats to online personal data privacy. They report that the *"children in our study had a good understanding of risks related to inappropriate content, the approach of strangers, and oversharing of personal information online. However, they struggled to fully understand and describe risks related to online game/video promotions and personal data tracking. Moreover, children's risk coping strategies depended on their understanding of the risks and their previous experiences: effective risk strategies were applied only if children recognized certain risks or when they felt something untoward"*. Desimpelaere et al. (2020) measured children's level of privacy literacy, using the following three self-composed multiple response questions: (i) What would you do if a website requested your personal details? (ii) How can companies collect your personal data? (iii) What kind of information would companies like to have about you? Türker and Çakmak (2019) developed a cyberwellness scale form consisting of seven sub-scales: internet addiction, cyberbullying, netiquette, online privacy, inappropriate online content, copyright, and cybersecurity. Using this form and a survey, they investigated the cyberwellness awareness of secondary school students and teachers. Choong et al. (2019) measure children's knowledge of password by assessing their use of computers, passwords, password practices, and knowledge of and feelings about passwords. Dempsey et al. (2018) test whether children understand privacy concepts by asking them questions that relate to privacy issues in an online setting where children must make decisions about their "control over personal information". Other than these five studies, we have not found any other study that clearly measures any form of awareness related to cybersecurity or privacy.

From all the studies discussed above, we observe a process that researchers follow to measure children's awareness. They generally do so in two steps (Fig. 9). First, they try to gauge children's ability to recognize a risk or a risky context and their existing concepts about privacy and security. Then, researchers examine children's responses to or behavior toward the risks or risky contexts. We observe this two-step process both in studies that implement an approach to raise awareness and studies that simply measure awareness. The former group of studies generally

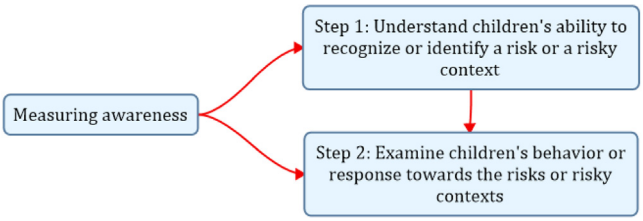

Fig. 9. Process of measuring cybersecurity awareness.

measure awareness after implementing the awareness-raising approaches.

4.4.2. Evaluating effectiveness of the approaches

As we have already mentioned, some studies have evaluated children's cybersecurity awareness by measuring the effectiveness of their proposed approaches and solutions. Fig. 10 presents an overview of the studies that evaluate approaches and the factors each study considers. We found ten such studies (Amo et al., 2019; Baciu-Ureche et al., 2019; Bioglio et al., 2019; Desimpelaere et al., 2020; Giannakas et al., 2016; Lastdrager et al., 2017; Meng et al., 2012; Reid & Van Niekerk, 2014; Zhang-Kennedy, Abdelaziz et al., 2017; Zhang-Kennedy, Baig et al., 2017).

For privacy-focused studies, the impact on users' privacy knowledge and concern, privacy behavior, and related disclosure intention or disclosure behavior appear to be the important factors for measuring effectiveness (Desimpelaere et al.,

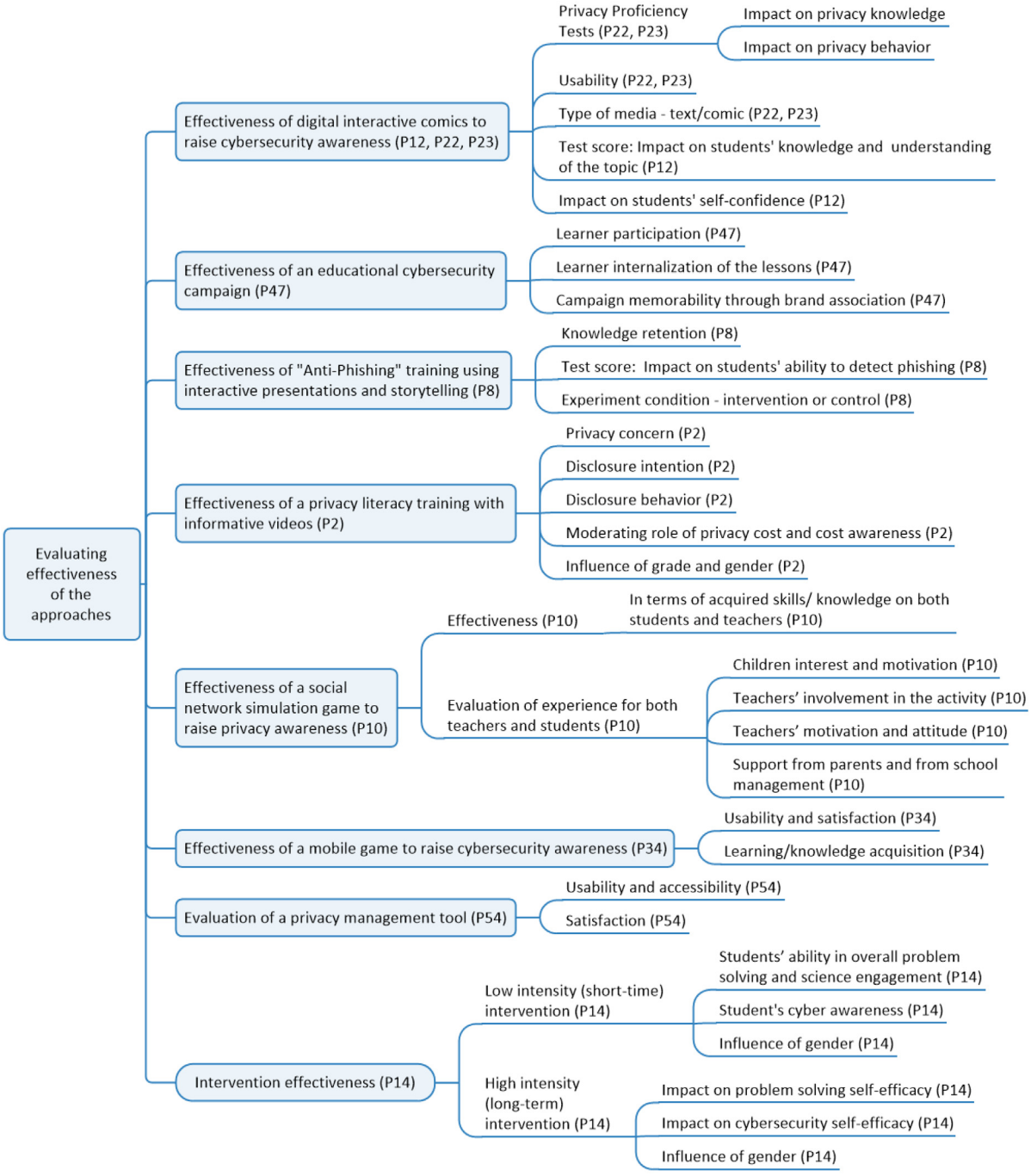

Fig. 10. Evaluating effectiveness of the approaches and the considered factors.

2020; Zhang-Kennedy, Abdelaziz et al., 2017; Zhang-Kennedy, Baig et al., 2017). Another important factor to show the effectiveness of an approach is increased learning and knowledge acquisition (Amo et al., 2019; Bioglio et al., 2019; Giannakas et al., 2016). Two other studies use learning as a factor to measure effectiveness through test scores (Baciu-Ureche et al., 2019; Lastdrager et al., 2017). For cybersecurity campaigns, effectiveness is measured in terms of learner participation, learners' internalization of the lessons, and campaign memorability through brand association (Reid & Van Niekerk, 2014). Studies that developed any kind of products or solutions employ usability as an important factors in measuring effectiveness (Giannakas et al., 2016; Meng et al., 2012; Zhang-Kennedy, Abdelaziz et al., 2017; Zhang-Kennedy, Baig et al., 2017). The satisfaction level of users is also an important factor (Giannakas et al., 2016; Meng et al., 2012). Students' awareness, self-efficacy of cybersecurity, and problem solving were all used as factors to measure the effectiveness of interventions (Amo et al., 2019). Two studies evaluate how the effectiveness of approaches differ based on gender (Amo et al., 2019; Desimpelaere et al., 2020). Besides effectiveness, one study (Bioglio et al., 2019), evaluates the experience of teachers and students, using factors like motivation, engagement, interest, and attitude to evaluate the participants' experience of their gamified approach to raising awareness of online privacy.

5. Discussion

As we identified a large number of papers (1544) through certain relevant search terms, it is clear that research into cybersecurity awareness for children has received a substantial amount of interest from the research community. The present review focuses on cybersecurity risks, the approaches used to raise awareness of those risks, and an evaluation of cybersecurity awareness and approaches to it. After applying our inclusion, exclusion, and quality criteria, we selected the most relevant high-quality papers to answer our research questions. Ultimately, we included 56 papers that were diverse in nature and focus on different risks and approaches.

5.1. Lack of focus on awareness of some specific cybersecurity risks

If we compare our findings with Tsirtsis et al. (2016), we see that the risks we have found are mostly similar to theirs; invasion of privacy, online harassment, content-related dangers, social engineering, and technology-based threats are still significant cybersecurity risks for children. The most commonly addressed risks for children are privacy, cyberbullying, and exposure to inappropriate content and pornography, as a significant number of studies acknowledge these risks for children. At the same time, it is evident that many risks have not been addressed in detail by the research community, such as stranger danger. Though many studies refer to the phenomenon but have not studied the risks that come from strangers (such as catfishing, impersonation, and cybergrooming) in full depth. Similarly, only two studies discuss economic risks (Muir & Joinson, 2020; Tsirtsis et al., 2016). With advances in technology and the growth of e-commerce, more and more children now have access to online payment methods, making them vulnerable to risks like financial scams and online gambling. Unfortunately, this kind of risk to children has not been studied in sufficient depth.

The findings from privacy-focused studies show that children have a reasonable understanding of and concern about online privacy (Choong et al., 2019; Zhao et al., 2019) and apply various privacy-protective strategies when online (Feng & Xie, 2014; Kumar et al., 2017). This suggests that privacy awareness has been addressed to a significant extent by the research community and society as a whole. Children, especially teenagers or adolescents, are aware of online privacy and know some privacy-protecting techniques. However, as to the other several cybersecurity risks found in the literature, we have not seen studies that measure children's level of awareness of any other specific risks. The lack of in-depth studies on these other risks means that we do not yet understand the level of awareness children may or may not have about those risks.

In summary, we observe that by focusing only on few specific risks, researchers have missed other significant risks to children's well-being, safety, and security. Thus, we argue that there is a need for more robust and in-depth studies on these other cybersecurity risks. Researchers can investigate the causes and consequences of the risks, social or behavioral factors, influences, mitigation mechanisms, attack detection techniques, and so on for all the relevant risks to children.

5.2. Theories identified in the studies

Learning and motivational theories can assist the development of learning materials and a learning environment for children. Giannakas et al. (2016) state that *"motivation is considered as a theoretical construct for explaining learner's behavior"*. Of the 56 studies, only 11 refer to one or more theories. In this review, we observe that only a few studies consider factors like motivation and engagement as a theoretical construct when designing or developing tools or approaches. A limited number of studies, including (Bioglio et al., 2019; Lastdrager et al., 2017; Zhang-Kennedy, Baig et al., 2017), have considered children's engagement and motivation in their research processes but not as a theoretical construct, while (Giannakas et al., 2016) uses motivation as a theoretical construct for developing an awareness game. Thus, we emphasize the need to connect the cybersecurity awareness research more closely with motivational and learning theories to achieve better effectiveness.

5.3. Approaches to raising cybersecurity awareness

All the approaches found in this review showed positive results, proving their effectiveness and positive impact on children. Training has been found to be the most commonly used approach, with studies using different techniques to implement their training efforts. We highlight that it is unusual to always have positive results when this many studies are involved; our explanation is that researchers tend not to publish negative results; rather, they are more likely to refine their approaches before publishing them. At the same time, the evaluations are limited by the context, aligning with the findings of Alotaibi et al. (2016).

One notable discovers is that the training approaches adopted by the researchers in this review differ from traditional training approaches. Researchers have used game elements like storytelling (Lastdrager et al., 2017), digital comics (Baciu-Ureche et al., 2019; Zhang-Kennedy, Abdelaziz et al., 2017; Zhang-Kennedy, Baig et al., 2017), and social media (Meng et al., 2012; Von Solms & Von Solms, 2015) for training purposes. As children are usually more interested in games and media, using such techniques for training appears to be an effective technique for training children. However, compared to training, the other awareness approaches we observed (such as interventions, warning, gamification, and game-based learning) are not explored in great detail. We believe there is a broad scope to investigate all approaches to increasing security awareness. Future research could investigate the approaches that have not been explored in depth more fully and compare them with traditional approaches like training to see which are more effective for children. It is generally assumed that children like games more than adults; thus, we expected more

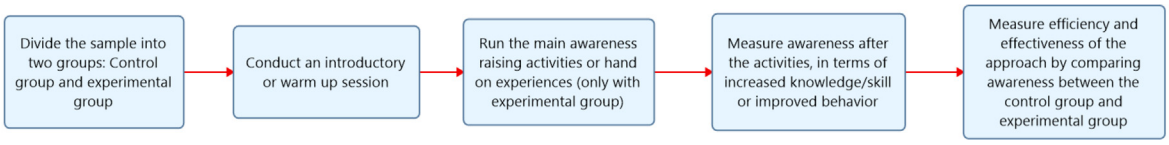

Fig. 11. Process of implementing an awareness-raising approach.

studies to use a game-based learning approach or a gamified approach to raise awareness, given the target audience of children. Gamification and game-based learning have shown proven to be promising in many research areas; research studies like Alotaibi et al. (2016) have also reported the potential of gaming to help create cybersecurity awareness. Warning or nudging mechanisms have also shown promising results as an approach to raising cybersecurity awareness among children (Alemany et al., 2019; Maurer et al., 2011).

We did observe certain similarities in the processes researchers followed when conducting their studies. Based on these similarities and common steps, we have developed an overview of the process (Fig. 11) that can serve as a recommended structure for future studies to raise cybersecurity awareness. We note that not every study followed the same process.

Most studies that implement an approach, including (Alemany et al., 2019; Bioglio et al., 2019; Choong et al., 2019; Desimpelaere et al., 2020; Lastdrager et al., 2017; Maurer et al., 2011; Vanderhoven et al., 2015; Zhang-Kennedy, Baig et al., 2017), divided their samples into two groups: control and experimental. Dividing the sample helped researchers see the impact of the awareness activities. Before starting the main activities of the study, some researchers, for example Zhao et al. (2019), preferred to have an introductory or warm-up session where they could introduce themselves and the tasks to the children so that the children would relax and feel more comfortable to engage in the subsequent tasks. After running the main activities of the study, researchers measured the impact of the activities on children in terms of increased awareness, skills, knowledge, or improved behavior. Finally, the effectiveness and efficiency of the approach can be evaluated by comparing the results between experimental and control groups.

5.4. Evaluating cybersecurity awareness

In this review, we have identified a few studies where researchers evaluate their approaches and solutions using different factors or measure awareness related to cybersecurity or privacy. But it is important to mention that studies that clearly presented their evaluation processes and criteria were very limited in number. Some mentioned evaluating their solutions but did not present an adequate description of the process or the factors. However, based on the findings from those few studies, we have identified a process of measuring awareness (Fig. 9) which could be useful for future research studies.

Regarding the effectiveness of the approaches, in Fig. 10 we present the factors that researchers considered when evaluating effectiveness. Most studies that offered an evaluation of effectiveness focus on the impact of the awareness activities on children's knowledge, knowledge retention, and effects of behavior. Motivation is a crucial factor in increasing knowledge and awareness and bringing about changes in children's behavior. For example, Giannakas et al. (2016) developed a game based on the ARCS motivational model, Teimouri et al. (2018) grounded their work on PMT, and Bioglio et al. (2019) considered children's interest and motivation when evaluating their proposed method. Unfortunately, very few studies consider or even mention children's motivational aspects. We argue that researchers need to focus more on increasing motivation and engagement when developing awareness-raising solutions for children. Connecting research work with the relevant theories and using motivational and learning theories can be beneficial for children's knowledge retention and satisfaction.

After conducting this review, we conclude that, compared to other fields of study (e.g., the social sciences), the evaluation frameworks and factors in this area remain underdeveloped. Though all the approaches showed positive results, in order to implement the right approach, researchers need to know which factors and conditions led to successful solutions and increased awareness. Alotaibi et al. (2016) also point out multiple issues regarding the evaluation of cybersecurity awareness using gaming technologies: small sample populations, a lack of robust evaluation approaches, early indications of positive impacts, and so on. Though Alotaibi et al. (2016) focused on evaluation in a specific context, after analyzing the findings from our review, we believe these issues are persistent in contexts beyond the gaming approach. To clearly understand the impact and progress of research, we as a research community need to focus on this gap and develop structured frameworks to effectively evaluate cybersecurity awareness.

5.5. Limitations of this review

To mitigate the possible bias, we followed some rules. We developed a research protocol in advance that defined the research questions. Based on these research questions, we identified the keywords and search terms to search the relevant literature. However, due to our choice of keywords, there is a risk of omitting relevant literature. The risk of omitting relevant literature can also be caused by selecting a limited bibliographic database. This risk was mitigated by performing an additional manual search on Google Scholar.

To reduce the bias in the data extraction process, two authors jointly extracted data for half of the studies; and for the rest of the studies, the first author extracted the data, and then the extracted data were reviewed by the second author. However, it is important to note that some studies lacked sufficient and exact details about the design and findings; we frequently found that methods were not described adequately. These issues made it difficult for us to identify the research methods for some studies and to extract the data in a satisfactory manner.

5.6. Implications for research and practice

This research contributes to both practice and research by identifying trends, practices, and opportunities for future work. The review has clearly shown the importance of and need for more research on this topic. It shows the areas that need more attention from researchers, who can study specific cybersecurity risks that have not been fully explored as yet, and they can look more into the effectiveness of a variety of approaches, along with conventional training or classroom teaching, to raising cybersecurity awareness. Another important need identified in this review is for structured and more developed models and frameworks to measure and evaluate cybersecurity awareness approaches to increase and ideally maximize their effectiveness.

The trends and needs identified by this research will also help professionals better plan their future products and solutions. Companies developing educational applications on cybersecurity can focus on the risks that need more attention. They can also examine the approaches reported here and adopt the best ones in their solutions. We also recommend that researchers and practitioners also consider the negative effects of approaches for creating awareness about children's online security and privacy issues when designing interactions and products for them. Our search did not find even one paper that focused solely on negative outcomes of awareness-raising approaches. In 2011, Yarosh, Radu, Hunter, and Rosenbaum (2011) analyzed the explicitly expressed values of 137 papers published at Interaction Design for Children (IDC) conferences from 2002 to 2010. They report that only five percent of the analyzed papers discussed possible negatives of the technologies such as concerns about online safety.

6. Conclusion

This review analyzed 56 peer-reviewed articles selected from a systematic literature search spanning 2011 to mid of 2020. This review aimed to investigate the current research status and practices in cybersecurity awareness for children. We have identified the commonly addressed risks, the approaches implemented to raise awareness, the effectiveness and evaluation of the approaches, and how researchers have evaluated their own cybersecurity awareness approach.

Some scholars have investigated one risk exclusively, such as privacy, cyberbullying, and inappropriate content, and there are other risks that need more research and attention. Among the approaches, many studies used training approaches with a variety of techniques, whereas other approaches have not been as much in focus. All the studies address cybersecurity risks, and several propose tools and awareness programs but have not measured their effects on awareness or have not rigorously evaluated children's cybersecurity awareness. Thus, the evidence from this research suggests that, although cybersecurity awareness research for children has received significant attention from researchers, there remain gaps, and intensified research in this field is needed to fill them. Building on previous research studies dealing with raising children's cybersecurity awareness, we aim to develop a framework for children to help them with cybersecurity awareness. The findings from this study will support us in the design and development of that framework such that it will also help address the gaps in existing research.

For this review, we have exploited the method proposed by Kitchenham (2004) that is a central method in our research group and research infrastructure (Papavlasopoulou, Giannakos, & Jaccheri, 2017; Trifonova, Jaccheri, & Bergaust, 2008). We acknowledge that the Kitchenham method has been criticized (Dyba, Dingsoyr, & Hanssen, 2007; Staples & Niazi, 2007) and suggestions have been made to extend it with Cochrane Collaboration initiative[4] and with the PRISMA[5] guidelines for presentation. We will explore how to use extended methods for performing and presenting systematic literature reviews in future work.

7. Selection and participation

There were no participants involved.

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.

Appendix A. Studies included in the review

See Table 5.

Appendix B. Quality assessment of the studies

See Table 6.

[4] https://www.cochrane.org/about-us.
[5] http://www.prisma-statement.org/.

Table 5
Studies included in this review.

Study ID	Authors	Title	Publication source	Year	Ref.
P1	Albuquerque et al.	Privacy in smart toys: Risks and proposed solutions	Electronic Commerce Research and Applications	2020	de Paula Albuquerque et al. (2020)
P2	Desimpelaere et al.	Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior.	Computers in Human Behavior	2020	Desimpelaere et al. (2020)
P3	Jeong and Chiasson	"Lime", "open lock", and "blocked": Children's perception of colors, symbols, and words in cybersecurity warnings	Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems	2020	Jeong and Chiasson (2020)
P4	Muir and Joinson	An exploratory study into the negotiation of cyber-security within the family home	Frontiers in Psychology	2020	Muir and Joinson (2020)
P5	Prior and Renaud	Age-appropriate password "best practice" ontologies for early educators and parents	International Journal of Child–Computer Interaction	2020	Prior and Renaud (2020)
P6	Zhao et al.	'I make up a silly name': Understanding children's perception of privacy risks online	Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems	2019	Zhao et al. (2019)
P7	Türker and Çakmak	An investigation of cyberwellness awareness: Turkey secondary school students, teachers, and parents	Computers in the Schools	2019	Türker and Çakmak (2019)

(continued on next page)

Table 5 (*continued*).

Study ID	Authors	Title	Publication source	Year	Ref.
P8	Lastdrager et al.	How effective is anti-phishing training for children?	13th Symposium on Usable Privacy and Security, SOUPS 2017	2017	Lastdrager et al. (2017)
P9	Choong et al.	"Passwords protect my stuff"— A study of children's password practices	Journal of Cybersecurity, Vol 5	2019	Choong et al. (2019)
P10	Bioglio et al.	A social network simulation game to raise awareness of privacy among school children	IEEE Transactions on Learning Technologies	2019	Bioglio et al. (2019)
P11	Bernadas and Soriano	Online privacy behavior among youth in the Global South: A closer look at diversity of connectivity and information literacy	Journal of Information Communication & Ethics in Society, Vol 17, issue 1	2019	Bernadas and Soriano (2019)
P12	Baciu-Ureche et al.	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	2019	Baciu-Ureche et al. (2019)
P13	N. Ahmad et al.	Parental awareness on cyber threats using social media	Jurnal Komunikasi — Malaysian Journal of Communication, Vol 35	2019	Ahmad et al. (2019)
P14	L.C. Amo et al.	Cybersecurity interventions for teens: Two time-based approaches	IEEE Transactions on Education, Vol 62	2019	Amo et al. (2019)
P15	J. Alemany et al.	Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms	International Journal of Human Computer Studies, vol 129	2019	Alemany et al. (2019)
P16	Teimouri et al.	A model of online protection to reduce children's online risk exposure: Empirical evidence From Asia	Sexuality and Culture, Vol 22, Issue 4	2018	Teimouri et al. (2018)
P17	Martin et al.	Middle school students' social media use	Educational Technology & Society, Vol 21, Issue 1	2018	Martin et al. (2018)
P18	Maoneke et al.	ICTs use and cyberspace risks faced by adolescents in Namibia	2nd African Conference for Human–Computer Interaction, AfriCHI	2018	Maoneke et al. (2018)
P19	Kumar et al.	Co-designing online privacy-related games and stories with children	Proceedings of the 17th ACM Conference on Interaction Design and Children (IDC)	2018	Kumar et al. (2018)
P20	Dempsey et al.	Designing for GDPR — Investigating children's understanding of privacy: A survey approach	Proceedings of the 32nd International BCS Human–Computer Interaction Conference (HCI)	2018	Dempsey et al. (2018)
P21	Amancio et al.	Evaluation of the perception of Brazilians about smart toys and children's privacy	2018 XLIV Latin American Computer Conference (CLEI)	2018	Amancio et al. (2018)
P22	Zhang-Kennedy et al.	Engaging children about online privacy through storytelling in an interactive comic	HCI '17: Proceedings of the 31st British Computer Society Human–Computer Interaction Conference	2017	Zhang-Kennedy, Baig et al. (2017)
P23	Zhang-Kennedy et al.	Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy	International Journal of Child–Computer Interaction	2017	Zhang-Kennedy, Abdelaziz et al. (2017)
P24	Wisniewski et al.	Parents just do not understand: Why teens do not talk to parents about their online risk experiences	Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing	2017	Wisniewski et al. (2017)
P25	Valente and Cardenas	Security & privacy in smart toys	Proceedings of the 2017 Workshop on Internet of Things Security and Privacy; ACM SIGSAC Conference on Computer and Communications Security	2017	Valente and Cardenas (2017)
P26	Kumar et al.	'No telling passcodes out because they are private': Understanding children's mental models of privacy and security online	Proceedings of the ACM on Human–Computer Interaction, Vol 1	2017	Kumar et al. (2017)
P27	Just and Berg	Keeping children safe online: Understanding the concerns of carers of children with autism	IFIP Conference on Human–Computer Interaction, INTERACT 2017: Human–Computer Interaction — INTERACT 2017	2017	Just and Berg (2017)

(*continued on next page*)

Table 5 (*continued*).

Study ID	Authors	Title	Publication source	Year	Ref.
P28	Agarwal and Singhal	Securing our digital natives: A study of commonly experience internet safety issues and a one-stop solution	10th International Conference on Theory and Practice of Electronic Governance, ICEGOV	2017	Agarwal and Singhal (2017)
P29	Wisniewski et al.	Dear Diary: Teens reflect on their weekly online risk experiences	Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems	2016	Wisniewski et al. (2016)
P30	Tsirtsis et al.	Cyber security risks for minors: A taxonomy and a software architecture	11th International Workshop on Semantic and Social Media Adaptation and Personalization, SMAP	2016	Tsirtsis et al. (2016)
P31	Shin and Kang	Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet	Computers in Human Behavior	2016	Shin and Kang (2016)
P32	Hung et al.	A glance of child's play privacy in smart toys	International Conference on Cloud Computing and Security, ICCCS	2016	Hung et al. (2016)
P33	Hofstra et al.	Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust	Computers in Human Behavior	2016	Hofstra et al. (2016)
P34	Giannakas et al.	Security education and awareness for K-6 going mobile	International Journal of Interactive Mobile Technologies	2016	Giannakas et al. (2016)
P35	Alotaibi et al.	A review of using gaming technology for cyber-security awareness	International Journal for Information Security Research (IJISR)	2016	Alotaibi et al. (2016)
P36	Wisniewski et al.	"Preventative" vs. "reactive": How parental mediation influences teens' social media privacy behaviors	Proceedings of the 2015 ACM International Conference on Computer-Supported Cooperative Work and Social Computing	2015	Wisniewski, Jia, Xu et al. (2015)
P37	Wisniewski et al.	Resilience mitigates the negative effects of adolescent internet addiction and online risk exposure	In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)	2015	Wisniewski, Jia, Wang et al. (2015)
P38	Von Solms and Von Solms	Cyber safety education in developing countries	9th International Multi-Conference on Society, Cybernetics and Informatics, IMSCI 2015	2015	Von Solms and Von Solms (2015)
P39	Vanderhoven et al.	Wait and see? Studying the teacher's role during in-class educational gaming	Proceedings of the European Conference on Games-based Learning	2015	Vanderhoven et al. (2015)
P40	Sezer et al.	Cyber bullying and teachers' awareness	Internet Research	2015	Sezer et al. (2015)
P41	E. Kritzinger	Enhancing cyber safety awareness among school children in South Africa through gaming	2015 Science and Information Conference (SAI)	2015	Kritzinger (2015)
P42	H. Jia et al.	Risk-taking as a learning process for shaping teen's online information privacy behaviors	Proceedings of the 2015 ACM International Conference on Computer-Supported Cooperative Work and Social Computing	2015	Jia et al. (2015)
P43	Cullinane et al.	Cyber security education through gaming cybersecurity games can be interactive, fun, educational and engaging	Journal of Computing Sciences in Colleges	2015	Cullinane et al. (2015)
P44	Clemons and Wilson	Family preferences concerning online privacy, data mining, and targeted ads: Regulatory implications	Journal of Management Information Systems	2015	Clemons and Wilson (2015)
P45	Bannon et al.	The internet and young people with Additional Support Needs (ASN): Risk and safety	Computers in Human Behavior	2015	Bannon et al. (2015)
P46	Von Solms and Von Solms	Toward cyber safety education in primary schools in Africa	8th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2014	2014	Von Solms and Von Solms (2014)
P47	Reid and Niekerk	Toward an education campaign for fostering a societal, cyber security culture	Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA)	2014	Reid and Van Niekerk (2014)

(*continued on next page*)

Table 5 (*continued*).

Study ID	Authors	Title	Publication source	Year	Ref.
P48	Feng and Xie	Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors	Computers in Human Behavior	2014	Feng and Xie (2014)
P49	Staksrud et al.	Does the use of social networking sites increase children's risk of harm?	Computers in Human Behavior	2013	Staksrud et al. (2013)
P50	Salazar et al.	Enhancing cybersecurity learning through an augmented reality-based serious game	2013 IEEE Global Engineering Education Conference, EDUCON	2013	Salazar et al. (2013)
P51	Moreno et al.	Internet safety education for youth: stakeholder perspectives	BMC Public Health 2013, 13:543	2013	Moreno et al. (2013)
P52	Hamdan et al.	Protecting teenagers from potential internet security threats	2013 International Conference on Current Trends in Information Technology (CTIT)	2013	Hamdan et al. (2013)
P53	Aponte and Richards	Managing cyber-bullying in online educational virtual worlds	Proceedings of The 9th Australasian Conference on Interactive Entertainment: Matters of Life and Death	2013	Aponte and Richards (2013)
P54	Meng et al.	PrivacyDoc: A study on privacy protection tools for children in SNS	International Journal of Smart Home	2012	Meng et al. (2012)
P55	Maurer et al.	Using data type based security alert dialogs to raise online security awareness	Proceedings of the Seventh Symposium on Usable Privacy and Security	2011	Maurer et al. (2011)
P56	Baracaldo et al.	Simulating the effect of privacy concerns in online social networks	2011 IEEE International Conference on Information Reuse and Integration	2011	Baracaldo et al. (2011)

Table 6
Quality assessment of the studies.

Study ID	Research	Aim	Context	Research design	Data collection	Data analysis	Finding	Value	Total score
P1	1	1	1	1	1	1	1	1	8
P2	1	1	1	1	1	1	1	1	8
P3	1	1	1	1	1	1	1	1	8
P4	1	1	1	1	1	1	1	1	8
P5	1	1	1	1	1	1	1	1	8
P6	1	1	1	1	1	1	1	1	8
P7	1	1	1	1	1	1	1	1	8
P8	1	1	1	1	1	1	1	1	8
P9	1	1	1	1	1	1	1	0	7
P10	1	1	1	1	1	1	1	0	7
P11	1	1	1	1	1	1	1	1	8
P12	1	1	0	1	0	1	1	1	6
P13	1	1	0	1	0	1	1	0	5
P14	1	1	1	1	1	1	1	1	8
P15	1	1	1	1	1	1	1	1	8
P16	1	1	1	1	1	1	1	1	8
P17	1	1	1	1	1	1	1	1	8
P18	1	1	1	1	1	1	1	1	8
P19	1	1	1	1	1	1	1	1	8
P20	1	1	1	1	1	1	1	1	8
P21	1	1	1	1	1	1	1	1	8
P22	1	1	1	1	1	1	1	1	8
P23	1	1	1	1	1	1	1	1	8
P24	1	1	1	1	1	1	1	1	8
P25	1	1	1	1	1	1	1	1	8
P26	1	1	1	1	1	1	1	1	8
P27	1	1	1	1	1	1	1	1	8
P28	1	1	1	0	0	0	1	1	5
P29	1	1	1	1	1	1	1	1	8
P30	1	1	1	0	0	1	1	1	6
P31	1	1	1	1	1	1	1	1	8
P32	1	1	1	0	1	1	0	1	6
P33	1	1	1	1	1	1	1	1	8
P34	1	1	1	1	1	1	1	1	8
P35	1	1	1	1	1	1	1	1	8
P36	1	1	1	1	1	1	1	1	8

(*continued on next page*)

Table 6 (*continued*).

Study ID	Research	Aim	Context	Research design	Data collection	Data analysis	Finding	Value	Total score
P37	1	1	1	1	1	1	1	1	8
P38	1	1	1	1	0	0	0	1	5
P39	1	1	1	1	0	1	1	0	6
P40	1	1	1	1	1	1	1	1	8
P41	1	0	1	0	0	1	1	1	5
P42	1	1	1	1	1	1	1	1	8
P43	1	1	0	0	0	1	1	1	5
P44	1	1	1	1	0	0	1	1	6
P45	1	1	1	1	1	1	1	1	8
P46	1	1	1	1	1	1	1	1	8
P47	1	1	1	1	0	0	1	1	6
P48	1	1	1	1	1	1	1	1	8
P49	1	1	1	1	1	1	1	1	8
P50	1	1	1	0	1	0	0	1	5
P51	1	1	1	1	1	1	1	1	8
P52	1	1	1	0	0	1	1	1	6
P53	1	1	0	0	0	1	1	1	5
P54	1	1	0	1	1	1	1	1	7
P55	1	1	1	0	1	1	1	1	7
P56	1	1	1	0	1	1	1	1	7

Table 7
Publication channels.

Journals	No. of papers
Computers in Human Behavior	6
International Journal of Child–Computer Interaction (ijCCI)	2
International Journal of Smart Home	1
BMC Public Health	1
Journal of Management Information Systems	1
Journal of Computing Sciences in Colleges	1
Internet Research	1
International Journal for Information Security Research (IJISR)	1
International Journal of Interactive Mobile Technologies	1
ACM Transactions on Computer–Human Interaction	1
Educational Technology and Society	1
Sexuality and Culture	1
International Journal of Human Computer Studies	1
IEEE Transactions on Education	1
Jurnal Komunikasi — Malaysian Journal of Communication	1
Journal of Information Communication and Ethics in Society	1
Journal of Cybersecurity	1
Computers in the Schools	1
Frontiers in Psychology	1
Electronic Commerce Research and Applications	1
IEEE Transactions on Learning Technologies	1
Conferences	
ACM Conference on Human Factors in Computing Systems	4
ACM Computer Supported Cooperative Work and Social computing	3
Symposium on Usable Privacy and Security, SOUPS	2
International Symposium on Human Aspects of Information Security and Assurance	2
Annual SIG Conference on Information Technology Education	1
ACM Conference on Interaction Design and Children (IDC)	1
IEEE International Conference on Information Reuse and Integration	1
Australasian Conference on Interactive Entertainment: Matters of life and death	1
International Conference on Current Trends in Information Technology	1
IEEE Global Engineering Education Conference, EDUCON	1
Science and Information Conference (SAI)	1
European Conference on Games-based Learning	1
International Multi-Conference on Society, Cybernetics and Informatics	1
International Conference on Cloud Computing and security ICCCS	1
Workshop on Semantic and Social Media Adaptation and Personalization	1
Conference on Theory and Practice of Electronic governance	1
IFIP Conference on Human–Computer Interaction, INTERACT	1
ACM SIGSAC Conference on Computer and Communications Security	1
British Computer Society Human–Computer Interaction Conference	1
Latin American Computer Conference (CLEI)	1
African Conference for Human–Computer Interaction, AfriCHI	1
International BCS Human–Computer Interaction Conference (HCI)	1

Appendix C. Publication channels

See Table 7.

References

Abd Rahim, Noor Hayani, Hamid, Suraya, Kiah, Miss Laiha Mat, Shamshirband, Shahaboddin, & Furnell, Steven (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*.

Agarwal, Chandni, & Singhal, Akshath (2017). Securing our digital natives: A study of commonly experience internet safety issues and a one-stop solution. In *ICEGOV '17, Proceedings of the 10th international conference on theory and practice of electronic governance* (pp. 178–186). New York, NY, USA: Association for Computing Machinery.

Ahmad, Nazilah, Arifin, Ahmad, Mokhtar, Umi Asma, Hood, Zaihosnita, Tiun, Sabrina, & Jambari, Dian Indrayani (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi: Malaysian Journal of Communication*, *35*(2), 485–498.

Alemany, J., del Val, E., Alberola, J., & García-Fornes, A. (2019). Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. *International Journal of Human-Computer Studies*, *129*, 27–40.

Alotaibi, Faisal, Furnell, Steven, Stengel, Ingo, & Papadaki, Maria (2016). A review of using gaming technology for cyber-security awareness. *International Journal for Information Security Research (IJISR)*, *6*(2), 660–666.

Amancio, F., Fantinato, M., Hung, P., Coutinho, G., & Roa, J. (2018). Evaluation of the perception of Brazilians about smart toys and children's privacy. In *2018 XLIV Latin American computer conference (CLEI)* (pp. 318–327).

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.

Aponte, Diego Fernando Gutierrez, & Richards, Deborah (2013). Managing cyberbullying in online educational virtual worlds. In *IE '13, Proceedings of the 9th Australasian conference on interactive entertainment: Matters of life and death*. New York, NY, USA: Association for Computing Machinery.

Baciu-Ureche, Ovidiu-Gabriel, Sleeman, Carlie, Moody, William C., & Matthews, Suzanne J. (2019). The adventures of scriptkitty: Using the raspberry pi to teach adolescents about internet safety. In *SIGITE '19, Proceedings of the 20th annual SIG conference on information technology education* (pp. 118–123). New York, NY, USA: Association for Computing Machinery.

Bannon, Stephanie, McGlynn, Tracy, McKenzie, Karen, & Quayle, Ethel (2015). The internet and young people with additional support needs (ASN): Risk and safety. *Computers in Human Behavior*, *53*, 495–503.

Baracaldo, N., López, C., Anwar, M., & Lewis, M. (2011). Simulating the effect of privacy concerns in online social networks. In *2011 IEEE international conference on information reuse integration* (pp. 519–524).

Bernadas, J. M. A. C., & Soriano, C. R. (2019). Online privacy behavior among youth in the Global South: A closer look at diversity of connectivity and information literacy. *Journal of Information, Communication and Ethics in Society*, *17*(1), 17–30.

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.

Brown, John Seely, Heath, Christian, & Pea, Roy (2003). *Vygotsky's educational theory in cultural context*. Cambridge University Press.

Choong, Yee-Yin, Theofanos, Mary F., Renaud, Karen, & Prior, Suzanne (2019). "Passwords protect my stuff"—a study of children's password practices. *Journal of Cybersecurity*, *5*(1).

Clemons, Eric K., & Wilson, Joshua S. (2015). Family preferences concerning online privacy, data mining, and targeted ads: Regulatory implications. *Journal of Management Information Systems*, *32*(2), 40–70.

Cruzes, Daniela. S., & Dybå, Tore (2011). Recommended steps for thematic synthesis in software engineering. In *2011 international symposium on empirical software engineering and measurement* (pp. 275–284).

Cullinane, Ian, Huang, Catherine, Sharkey, Thomas, & Moussavi, Shamsi (2015). Cyber security education through gaming cybersecurity games can be interactive, fun, educational and engaging. *Journal of Computing Sciences in Colleges*, *30*(6), 75–81.

Cummings, E. Mark, Bergman, Kathleen N., & Kuznicki, Kelly A. (2014). Emerging methods for studying families as systems. In *Emerging methods in family research* (pp. 95–108). Springer.

de Paula Albuquerque, Otávio, Fantinato, Marcelo, Kelner, Judith, & de Albuquerque, Anna Priscilla (2020). Privacy in smart toys: Risks and proposed solutions. *Electronic Commerce Research and Applications*, *39*, Article 100922.

Dempsey, John, Sim, Gavin, & Cassidy, Brendan (2018). Designing for GDPR - Investigating children's understanding of privacy: A survey approach. In *HCI '18, Proceedings of the 32nd international BCS human computer interaction conference*. Swindon, GBR: BCS Learning & Development Ltd..

Desimpelaere, Laurien, Hudders, Liselot, & Van de Sompel, Dieneke (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, *110*, Article 106382.

Dyba, Tore, Dingsoyr, Torgeir, & Hanssen, Geir K. (2007). Applying systematic reviews to diverse study types: An experience report. In *First international symposium on empirical software engineering and measurement (ESEM 2007)* (pp. 225–234). IEEE.

Dybå, Tore, & Dingsøyr, T. (2008). Empirical studies of agile software development: A systematic review. *Information and Software Technology*, *50*(9–10), 833–859.

Feng, Yang, & Xie, Wenjing (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior*, *33*, 153–162.

Fergus, Stevenson, & Zimmerman, Marc A. (2005). Adolescent resilience: A framework for understanding healthy development in the face of risk. *Annual Review of Public Health*, *26*, 399–419.

Giannakas, Filippos, Kambourakis, Georgios, Papasalouros, Andreas, & Gritzalis, Stefanos (2016). Security education and awareness for K-6 going mobile. *International Journal of Interactive Mobile Technologies (IJIM)*, *10*(2), 41–48.

Giannakas, Filippos, Papasalouros, Andreas, Kambourakis, Georgios, & Gritzalis, Stefanos (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective*, *28*(3), 81–106.

Gjertsen, Eyvind Garder B., Gjære, Erlend Andreas, Bartnes, Maria, & Flores, Waldo Rocha (2017). Gamification of information security awareness and training. In *Proceedings of the 3rd international conference on information systems security and privacy - Volume 1: ICISSP* (pp. 59–70). INSTICC, SciTePress.

Hamdan, Z., Obaid, I., Ali, A., Hussain, H., Rajan, A. V., & Ahamed, J. (2013). Protecting teenagers from potential internet security threats. In *2013 international conference on current trends in information technology (CTIT)* (pp. 143–152).

Hofstra, Bas, Corten, Rense, & van Tubergen, Frank (2016). Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior*, *60*, 611–621.

Hourcade, Juan Pablo (2015). *Child-computer interaction*. CreateSpace Independent Publishing Platform.

Hung, Patrick C. K., Iqbal, Farkhund, Huang, Shih-Chia, Melaisi, Mohammed, & Pang, Kevin (2016). A glance of child's play privacy in smart toys. In Xingming Sun, Alex Liu, Han-Chieh Chao, & Elisa Bertino (Eds.), *Cloud computing and security* (pp. 217–231). Cham: Springer International Publishing.

Janz, Nancy K., & Becker, Marshall H. (1984). The health belief model: A decade later. *Health Education Quarterly*, *11*(1), 1–47, PMID: 6392204.

Jeong, Rebecca, & Chiasson, Sonia (2020). 'Lime', 'Open Lock', and 'Blocked': Children's perception of colors, symbols, and words in cybersecurity warnings. In *CHI '20, Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1–13). New York, NY, USA: Association for Computing Machinery.

Jia, Haiyan, Wisniewski, Pamela J., Xu, Heng, Rosson, Mary Beth, & Carroll, John M. (2015). Risk-taking as a learning process for shaping teen's online information privacy behaviors. In *CSCW '15, Proceedings of the 18th ACM conference on computer supported cooperative work & social computing* (pp. 583–599). New York, NY, USA: Association for Computing Machinery.

Just, Mike, & Berg, Tessa (2017). Keeping children safe online: Understanding the concerns of carers of children with autism. In Regina Bernhaupt, Girish Dalvi, Anirudha Joshi, Devanuj K. Balkrishan, Jacki O'Neill, & Marco Winckler (Eds.), *Human-computer interaction – INTERACT 2017* (pp. 34–53). Cham: Springer International Publishing.

Keller, John M. (1987). Development and use of the ARCS model of instructional design. *Journal of Instructional Development*, *10*(3), 2–10.

Kitchenham, B. A. (2004). *Procedures for undertaking systematic reviews*. Joint Technical Report, Computer Science Department, Keele University (TR/SE-0401) and National ICT Australia Ltd. (0400011T.1).

Kritzinger, E. (2015). Enhancing cyber safety awareness among school children in South Africa through gaming. In *2015 science and information conference (SAI)* (pp. 1243–1248).

Kumar, Priya, Naik, Shalmali Milind, Devkar, Utkarsha Ramesh, Chetty, Marshini, Clegg, Tamara L., & Vitak, Jessica (2017). No telling passcodes out because they're private: Understanding children's mental models of privacy and security online. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW).

Kumar, Priya, Vitak, Jessica, Chetty, Marshini, Clegg, Tamara L., Yang, Jonathan, McNally, Brenna, et al. (2018). Co-designing online privacy-related games and stories with children. In *IDC '18, Proceedings of the 17th ACM conference on interaction design and children* (pp. 67–79). New York, NY, USA: Association for Computing Machinery.

Lastdrager, Elmer, Gallardo, Inés Carvajal, Hartel, Pieter, & Junger, Marianne (2017). How effective is anti-phishing training for children? In *Thirteenth symposium on usable privacy and security (SOUPS 2017)* (pp. 229–239). Santa Clara, CA: USENIX Association.

Lee, Kang (2000). *Childhood cognitive development: The essential readings*. Wiley-Blackwell.

Livingstone, Sonia, Hasebrink, Uwe, & Görzig, Anke (2012). Towards a general model of determinants of risk and safety. In Sonia Livingstone, Leslie Haddon, & Anke Görzig (Eds.), *Children, risk and safety on the internet: Research and policy challenges in comparative perspective* (pp. 323–337). Bristol, UK: Policy Press.

Maoneke, Pardon Blessings, Shava, Fungai Bhunu, Gamundani, Attlee Munyaradzi, Bere-Chitauro, Mercy, & Nhamu, Isaac (2018). ICT use and cyberspace risks faced by adolescents in Namibia. In *AfriCHI '18*, *Proceedings of the second African conference for human computer interaction: Thriving communities*. New York, NY, USA: Association for Computing Machinery.

Martin, Florence, Wang, Chuang, Petty, Teresa, Wang, Weichao, & Wilkins, Patti (2018). Middle school students' social media use. *Journal of Educational Technology & Society*, *21*(1), 213–224.

Maurer, Max-Emanuel, De Luca, Alexander, & Kempe, Sylvia (2011). Using data type based security alert dialogs to raise online security awareness. In *SOUPS '11*, *Proceedings of the seventh symposium on usable privacy and security*. New York, NY, USA: Association for Computing Machinery.

Meng, Ma, Zakaria, Nasriah, Bindahman, Salah, Alias, Nik Mohd Asrol, & Husain, Wahidah (2012). "PrivacyDoc" : A study on privacy protection tools for children in SNS. *International Journal of Smart Home*, *6*, 41–48.

Mesch, Gustavo S. (2009). Parental mediation, online activities, and cyberbullying. *CyberPsychology & Behavior*, *12*(4), 387–393.

Moreno, M. A., Egan, K. G., & Bare, K. (2013). Internet safety education for youth: stakeholder perspectives. *BMC Public Health*, *13*(543).

Muir, Kate, & Joinson, Adam (2020). An exploratory study into the negotiation of cyber-security within the family home. *Frontiers in Psychology*, *11*, 424.

Nissenbaum, Helen (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Notar, Charles E., Padgett, Sharon, & Roden, Jessica (2013). Cyberbullying: A review of the literature. *Universal Journal of Educational Research*, *1*(1), 1–9.

Owens, Eric W., Behun, Richard J., Manning, Jill C., & Reid, Rory C. (2012). The impact of internet pornography on adolescents: A review of the research. *Sexual Addiction & Compulsivity*, *19*(1–2), 99–122.

Papavlasopoulou, Sofia, Giannakos, Michail N., & Jaccheri, Letizia (2017). Empirical studies on the Maker Movement, a promising approach to learning: A literature review. *Entertainment Computing*, *18*, 57–78.

Pinter, Anthony T., Wisniewski, Pamela J., Xu, Heng, Rosson, Mary Beth, & Caroll, Jack M. (2017). Adolescent online safety: Moving beyond formative evaluations to designing solutions for the future. In *IDC '17*, *Proceedings of the 2017 conference on interaction design and children* (pp. 352–357). New York, NY, USA: Association for Computing Machinery.

Prior, Suzanne, & Renaud, Karen (2020). Age-appropriate password "best practice" ontologies for early educators and parents. *International Journal of Child-Computer Interaction*, *23–24*, Article 100169.

Quayyum, Farzana (2020). Dataset: Cybersecurity awareness for children - A systematic literature review. https://drive.google.com/file/d/1Bs7CyLsk-OqO8pwciannntr8ci1SkVfPX/view?usp=sharing, Uploaded 13.11.20.

Read, J. C., & Markopoulos, P. (2013). Child–computer interaction. *International Journal of Child-Computer Interaction*, *1*(1), 2–6.

Reed, Karen P., Cooper, R. Lyle, Nugent, William R., & Russell, Kathryn (2016). Cyberbullying: A literature review of its relationship to adolescent depression and current intervention strategies. *Journal of Human Behavior in the Social Environment*, *26*(1), 37–45.

Reid, R., & Van Niekerk, J. (2014). Towards an education campaign for fostering a societal, cyber security culture. In *Proceedings of the eighth international symposium on human aspects of information security & assurance (HAISA 2014)*.

Rogers, Ronald W. (1975). A protection motivation theory of fear appeals and attitude change1. *Journal of Psychology*, *91*(1), 93–114, PMID: 28136248.

Rosenstock, Irwin M., Strecher, Victor J., & Becker, Marshall H. (1988). Social learning theory and the health belief model. *Health Education Quarterly*, *15*(2), 175–183.

Salazar, M., Gaviria, J., Laorden, C., & Bringas, P. G. (2013). Enhancing cybersecurity learning through an augmented reality-based serious game. In *2013 IEEE global engineering education conference (EDUCON)* (pp. 602–607).

Sezer, Baris, Yilmaz, Ramazan, & Yilmaz, Fatma Gizem Karaoglan (2015). Cyber bullying and teachers' awareness. *Internet Research*, *25*, 674–687.

Shaw, R. S., Chen, Charlie C., Harris, Albert L., & Huang, Hui-Jou (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100.

Shin, Wonsun, & Kang, Hyunjin (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the internet. *Computers in Human Behavior*, *54*, 114–123.

Smith, H. Jeff, Dinev, Tamara, & Xu, Heng (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015.

Staksrud, Elisabeth, Ólafsson, Kjartan, & Livingstone, Sonia (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior*, *29*(1), 40–50.

Staples, Mark, & Niazi, Mahmood (2007). Experiences using systematic review guidelines. *Journal of Systems and Software*, *80*(9), 1425–1437.

Teimouri, Misha, Benrazavi, Seyed Rahim, Griffiths, Mark D., & Salleh Hassan, Md. (2018). A model of online protection to reduce children's online risk exposure: Empirical evidence from Asia. *Sexuality & Culture*, *22*, 1205–1229.

Trifonova, Anna, Jaccheri, Letizia, & Bergaust, Kristin (2008). Software engineering issues in interactive installation art. *International Journal of Arts and Technology*, *1*(1), 43–65.

Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., & Sirivianos, M. (2016). Cyber security risks for minors: A taxonomy and a software architecture. In *2016 11th international workshop on semantic and social media adaptation and personalization (SMAP)* (pp. 93–99).

Türker, Pınar Mıhcı, & Çakmak, Ebru Kılıç (2019). An investigation of cyber wellness awareness: Turkey secondary school students, teachers, and parents. *Computers in the Schools*, *36*(4), 293–318.

Valente, Junia, & Cardenas, Alvaro A. (2017). Security & privacy in smart toys. In *IoTS&P '17*, *Proceedings of the 2017 workshop on internet of things security and privacy* (pp. 19–24). New York, NY, USA: Association for Computing Machinery.

Vanderhoven, Ellen, Willems, Bart, Van Hove, Stephanie, All, Anissa, & Schellens, Tammy (2015). Wait and see? Studying the teacher's role during in-class educational gaming. In *European conference on games based learning* (pp. 540–547).

Von Solms, S., & Von Solms, R. (2014). Towards cyber safety education in primary schools in Africa. In *Proceedings of the eighth international symposium on human aspects of information security & assurance (HAISA 2014)*.

Von Solms, R., & Von Solms, S. (2015). Cyber safety education in developing countries. *Journal of Systemics, Cybernetics and Informatics*, *13*, 14–19.

Warren, Ron (2001). In words and deeds: Parental involvement and mediation of children's television viewing. *The Journal of Family Communication*, *1*(4), 211–231.

Watts, Lynette K., Wagner, Jessyca, Velasquez, Benito, & Behrens, Phyllis I. (2017). Cyberbullying in higher education: A literature review. *Computers in Human Behavior*, *69*, 268–274.

Wisniewski, Pamela, Jia, Haiyan, Wang, Na, Zheng, Saijing, Xu, Heng, Rosson, Mary Beth, et al. (2015). Resilience mitigates the negative effects of adolescent internet addiction and online risk exposure. In *CHI '15*, *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 4029–4038). New York, NY, USA: Association for Computing Machinery.

Wisniewski, Pamela, Jia, Haiyan, Xu, Heng, Rosson, Mary Beth, & Carroll, John M. (2015). "Preventative vs. Reactive": How parental mediation influences teens' social media privacy behaviors. In *CSCW '15*, *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing* (pp. 302–316). New York, NY, USA: Association for Computing Machinery.

Wisniewski, Pamela, Xu, Heng, Rosson, Mary Beth, & Carroll, John M. (2017). Parents just don't understand: Why teens don't talk to parents about their online risk experiences. In *CSCW '17*, *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing* (pp. 523–540). New York, NY, USA: Association for Computing Machinery, https://doi.org/10.1145/2998181.2998236.

Wisniewski, Pamela, Xu, Heng, Rosson, Mary Beth, Perkins, Daniel F., & Carroll, John M. (2016). Dear diary: Teens reflect on their weekly online risk experiences. In *CHI '16*, *Proceedings of the 2016 CHI conference on human factors in computing systems* (pp. 3919–3930). New York, NY, USA: Association for Computing Machinery.

Yarosh, Svetlana, Radu, Iulian, Hunter, Seth, & Rosenbaum, Eric (2011). Examining values: An analysis of nine years of IDC research. In *IDC '11*, *Proceedings of the 10th international conference on interaction design and children* (pp. 136–144). New York, NY, USA: Association for Computing Machinery.

Zhang, Xing, Liu, Shan, Chen, Xing, Wang, Lin, Gao, Baojun, & Zhu, Qing (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management*, *55*(4), 482–493.

Zhang-Kennedy, Leah, Abdelaziz, Yomna, & Chiasson, Sonia (2017). Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction*, *13*, 10–18.

Zhang-Kennedy, Leah, Baig, Khadija, & Chiasson, Sonia (2017). Engaging children about online privacy through storytelling in an interactive comic. In *HCI '17*, *Proceedings of the 31st British computer society human computer interaction conference*. Swindon, GBR: BCS Learning & Development Ltd..

Zhao, Jun, Wang, Ge, Dally, Carys, Slovak, Petr, Edbrooke-Childs, Julian, Van Kleek, Max, et al. (2019). 'I make up a silly name': Understanding children's perception of privacy risks online. In *CHI '19*, *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1–13). New York, NY, USA: Association for Computing Machinery.