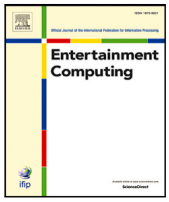
Entertainment Computing 52 (2025) 100826

Contents lists available at ScienceDirect

Entertainment Computing

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



CyberFamily: A collaborative family game to increase children's cybersecurity awareness

Farzana Quayyum *, Letizia Jaccheri

Department of Computer Science, Norwegian university of Science and Technology, Trondheim, Norway

ARTICLE INFO

Keywords:
Cybersecurity awareness
Human factors in cybersecurity
Parent–child collaboration
Game-based learning
Storytelling

ABSTRACT

Parental involvement is an essential factor that influences a child's learning, behavior, and every other aspect of life, including online interactions. While holding parents responsible for the consequences of children's online actions and overall well-being, we often overlook the importance of and need for means that can effectively support parents in interacting and engaging in activities with their children. In the present study, we describe and evaluate a collaborative family game called "CyberFamily" to facilitate parent–child collaboration and leverage family communication, intending to increase cybersecurity awareness among children aged 9–12. We also present the results of two user studies: one conducted with four parent–child dyads to test the feasibility of the game and a second user study conducted with 11 parent–child dyads focusing on evaluating the usability of CyberFamily. Our findings yielded positive feedback and showed that a collaborative family game like CyberFamily can help parents engage with their children's online activities, leading to discussions and the potential for collaborative learning for both groups. We suggest that future researchers and designers consider and provide an active, engaging role for parents when developing solutions to raise cybersecurity awareness among children, rather than just having parents monitor and control children's online access and activities.

1. Introduction

Today's children are global citizens. In a hyper-digitized world, people of all ages routinely use the internet for education, entertainment, communication, and virtually every aspect of life. Online settings are now a meaningful social context for children. While technology in general and online applications in particular can have significant positive impacts on users, there are risks associated with both, particularly for children who lack the maturity to fully comprehend online dangers. Along with technological countermeasures, security awareness and safe practices can help prevent or mitigate the damage done by cybersecurity threats. One of the several aspects of security practices is how well people are aware of and able to assess risks and apply knowledge to mitigate them [1]. Considering the importance of human-related vulnerabilities, the present study focuses on raising cybersecurity awareness as a personal practice from an early age.

Researchers have proposed different techniques to teach children about cybersecurity [2] and developed many educational tools to support that goal (e.g., [3–5]). While proposing awareness-raising approaches and developing tools, most existing research focuses solely on children. However, without proper support and guidance from adults, it is difficult for children to develop the necessary skills to understand online safety and threats, as they do not have the same maturity and cognitive ability as adults. Previous studies have identified the lack of meaningful roles for parents in designing interactions for children [6,7]. To provide better guidance to children, parents need opportunities to actively engage with their children's interactions without compromising their privacy. Therefore, the aim of our research is to explore the possibilities and opportunities for parents to play meaningful roles that can help them engage in cybersecurity actions and communications with their children, with the goal that children can learn about cybersecurity and build an understanding relationship with their parents so they can share knowledge and learn from one another.

The research community has acknowledged the important role of parents in shaping children's digital lives, including areas such as the need for parental education and concerns [6,7]. Children start to learn from their parents or caregivers even before starting school. Research has shown that security breaches like privacy violations can befall children even through the actions of others, notably their parents and other relatives [8,9]. Thus, parents must also possess cybersecurity knowledge and skills [7]. The digital competence of both children and parents needs to be improved. To help achieve that goal, we have

* Corresponding author.
E-mail addresses: farzana.quayyum@ntnu.no (F. Quayyum), letizia.jaccheri@ntnu.no (L. Jaccheri).

https://doi.org/10.1016/j.entcom.2024.100826
Received 23 January 2023; Received in revised form 13 February 2024; Accepted 12 July 2024
Available online 31 July 2024

explored the following research question: *How can we increase parent–child collaboration to raise cybersecurity awareness using a game-based learning approach?*

Game-based learning can facilitate a collaborative learning environment (e.g., [10]) and be fun and motivating for both adults and children (e.g., [11,12]). Our study uses that approach to create a collaborative family game, "CyberFamily," to raise cybersecurity awareness. In this game, parents and children can play together, learn about cybersecurity topics like online privacy, password security, cyberbullying, phishing, and online etiquette, and help one another increase overall cybersecurity awareness. The primary target age group of children for this game is 9–12. Our aim with this proposed game is to raise cybersecurity awareness while giving parents the opportunity to actively engage with children in online scenarios and play essential roles in assisting children in learning what they need to know.

The primary contributions of this research include the design of a collaborative cybersecurity awareness game for children and their parents, the development of a prototype, and empirical evidence demonstrating the game's effectiveness. The design of our proposed game is based on two key assumptions: (i) a collaborative family game can facilitate collaborative learning between parents and children, and (ii) the collaborative aspect of the game shall foster dialogue between parents and children. To the best of our knowledge, our work is one of the first to propose a collaborative family game to raise children's cybersecurity awareness and emphasize the need for active parental involvement in educational children's games about cybersecurity. Our study also offers a mechanism to enhance family communication and understanding of cybersecurity and how to deal with the consequences of risk. It outlines our game concept and pertinent research on the evaluation of the game. In order to determine whether our proposed game successfully boosts parent–child collaboration, leading to cybersecurity awareness and whether it is a useful instrument to foster collaborative learning in a family context, we first conducted a feasibility study with four parent–child dyads. Later, we extended our work with a user study of 11 pairs of parents and children, where we evaluated CyberFamily in terms of usability and in relation to our assumptions.

The background of this study is presented in Section 2, followed by a description of our proposed game design in Section 3. Our research methodology is detailed in Section 4. The outcomes of the user studies and the CyberFamily game evaluation are presented in Section 5. Section 6 addresses our findings, the study's limitations and avenues for future work. Finally, in Section 7, we summarize our findings and conclude the paper.

2. Background

In this section, we discuss the relevant literature on cybersecurity awareness and the intersection of cybersecurity awareness with game-based learning (Section 2.1), parents' role in children's cybersecurity awareness with a focus on parent–child collaboration (Section 2.2), and collaborative learning in Section 2.3.

2.1. Cybersecurity awareness and game-based learning

The number of people using the internet is constantly growing; consequently, so are risks and online attacks. As more and more of our daily lives revolve around being online, people have a growing need to deal with the online risks that accompany the many opportunities offered by the digital sphere. People of all ages need awareness to deal with online threats and their consequences. Awareness comprises knowledge, self-perception of skills, actual skills and behavior, attitudes, and the relationships among these elements [13]. 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" [14]. Thus, cybersecurity awareness involves alerting users of online dangers and threats and enhancing their understanding of those threats so that they can be fully committed to embracing security in their online lives [15].

A literature review by Quayyum et al. [2] shows a list of cybersecurity risks that are relevant for children, teenagers, and young adults. Another literature review was carried out by Svabensky et al. [16] to determine which cybersecurity-related topics are commonly explored by the research community and which are not. The results from these studies indicate that privacy, password security, online strangers, cyberbullying, phishing, identity theft, and financial scams are among the most common cybersecurity risks that children and young people now face. Along with identifying the risks, researchers have proposed many different approaches to raise and assess cybersecurity awareness among adults and children [2,15], including the game-based learning approach. Game-based learning has been identified as effective in making learning attractive and motivating people to engage in a topic [5]. Given the high and persistent levels of popularity of video games, online and otherwise, among today's young people, the game-based learning approach can play an essential role in promoting cybersecurity awareness and online etiquette among children. Although game-based learning has received attention, particularly regarding children, it has also proven effective for other users, including (young) adults [17].

Various studies have demonstrated that using game-based alternatives to teach academic skills leads to higher motivation and better learning outcomes (e.g., [18,19]). Game-based learning has also been shown to be effective in teaching social and emotional skills, including in the context of teaching and raising cybersecurity awareness among children. Examples of using games to raise cybersecurity awareness include "SecurityEmpire" by Olano et al. [4], "Wolf, Hyena, and Fox" by J. Allers et al. [20], "The Adventures of ScriptKitty" by Baciu-Ureche et al. [21], "CyberAware" by Giannakas et al. [5], and "CyberSIEGE" by Irvine and Thompson [22]. These games and others have addressed cybersecurity issues ranging from privacy, phishing, and password practices to basic internet etiquette, and research has shown that games can be an effective training tool and encourage behavioral change [17, 23]. All the studies cited above that propose using games to raise cybersecurity awareness have reported positive outcomes.

2.2. Parent-child collaboration for cybersecurity awareness

Parent-child interactions are unquestionably important for children's spontaneous mental, behavioral, and literacy development [24]. Many studies have demonstrated the essential role of parents in mediating children's online behaviors and shaping their attitudes towards risks (e.g., [6,25]). Parents implement a variety of strategies to mediate children's online behavior, including active mediation (e.g., co-use and interactions) and technical restrictions like filters, monitoring software, and parental controls [26].

Researchers from different fields have recently explored parent–child interactions to investigate their impact and benefits and highlight implications for design. For example, Alevar et al. [24] explore how the interactions between parents and children affect emotions and physiological arousal during shared but independent e-book reading. Lauricella et al. [27] also explore parent–child interactions during traditional and digital book reading and suggest implications for designing storybooks. Beheshti et al. [28] show how haptic feedback displays can facilitate collaborative parent–child learning. Many other studies have also explored parent–child interactions from different dimensions, such as collaboration for learning computer programming [29] and how tangible interfaces can enhance intergenerational collaboration [30]. All the research studies noted above have reported a favorable impact on children's learning and development from various forms of parent–child interactions.

However, in the domain of children's cybersecurity awareness and education, there is a scarcity of research exploring the dimensions of parent–child interaction and collaboration. While some researchers

have examined the perceptions of parents, teachers, and other stakeholders regarding children's cybersecurity awareness [31–33], there are very few studies that explore the role of parents in children's online interactions (e.g., [6]) and how parent–child interactions influence children's cybersecurity awareness and attitudes. Some research has highlighted the challenges in parent–child relationships and using parental controls regarding children's online attitudes and activities [34,35]. While parents naturally wish to safeguard their children from threats or simply unpleasant digital experiences, they need to balance monitoring and control with trust [31]. Building a trusting relationship with their children can sometimes be challenging for parents; a lack of communication and active interactions between parents and children is one of the main factors in such challenges. Children may be reluctant to discuss their online experiences with their parents if the matter is not handled correctly. In order to foster such understanding and communication, it is crucial to investigate and comprehend how we can design cybersecurity solutions that are transparent and facilitate building trust by interacting and collaborating [34].

Furthermore, in order to enhance parent–child interactions and collaborations for children's cybersecurity education, parents need a role that allows them to actively engage in interactions with their children. However, as highlighted by Nouwen and Zaman, while designing interactions for children, we often overlook design opportunities that can support a meaningful role for parents [6]. Without such a role, it is hard for parents to know about and participate in their children's online activities. As a result, further study is needed to investigate and propose design opportunities for parents to participate in activities and discussions connected to children's online security experiences and learning. These opportunities can also encourage and facilitate the development of trust and transparent relationships within the family.

2.3. Collaborative learning

Gokhale [36] refers to collaborative learning as "an instruction method in which students at various performance levels work together in small groups towards a common goal." In collaborative learning, the participants are responsible for their own and one another's learning; thus, the success of one participant helps other participants succeed [36]. Although collaborative learning has received attention in academic learning environments (e.g., [37,38]), in the present study, we explore collaborative learning in the social context of the family.

According to social cognitive theory [39], human learning also occurs in social environments by observing or interacting with others. Children tend to imitate behavior and activities that they see people around them doing. Research shows that interacting with parents in learning activities (such as book reading and computer use for education) complements children's cognitive skill development [24,27]. In today's digital age, children begin using electronics and accessing online resources at a young age. As a result, children's collaboration with other family members and social contact within the family context provide the chance to observe, learn, and lay the foundation for learning about online safety and safe online behavior. As stated by J. P. Hourcade [40], adults can play a significant part in teaching children problem-solving skills. Problem solving influences children's attitudes towards challenges and the problem-solving approaches that they have already observed or been taught. Researchers have recently started exploring ways to increase parent–child collaboration in terms of, for example, using technologies [41] and jointly managing parental control tools [42,43]. These studies have demonstrated the benefit of involving parents in increasing children's awareness and improving their behavior. Greater collaboration between parents and children can help build a trust-based relationship; that is, one where children can feel free to share all their experiences and problems with their parents and families.

3. The concept and design of CyberFamily

3.1. The design rationales

Designing education tools for children entails several distinctive demands, one of which is that educational tools for children need to be visually and cognitively appealing. To perceive a learning activity as fun and attractive, children need to have motivation, attention, and concentration regarding the tasks involved [19]. Researchers suggest that interaction design for children should have three related high-level requirements: perceivability, operability, and developmental fit [3,40]. The first requirement means that it should be easy for children to understand what they can do with a technology; the user interface should be simplified according to the targeted child users' developmental stage and needs [3]. Children have limited physical and motor skills when compared to adults; thus, the second requirement is that the technology user interface is easy for children to operate, while the third requirement is that the user interface should meet children's abilities and experience in understanding how to use a technology [3,40].

3.2. Our game design

Keeping the requirements noted above in mind, we have designed a simple maze game (Fig. 1) using an online maze generator[1] for our paper prototype. A maze is defined as "a kind of game where a player moves in pathways with many branches to find a way out/certain targets" [44,45] and is well known to teach users problem-solving skills, critical thinking, patience, and persistence. Researchers have used maze games for various educational purposes (e.g., [46–48]). We have chosen the maze approach for our game to help our target users handle online threats and increase their awareness by triggering their critical thinking and problem-solving skills. Additionally, we modified the automatically created maze to make it a two-player game, as we sought to create a collaborative game that parents and children could play together.

To comply with operability requirements and make the game easy for children, we optimized the maze with an outer diameter of 20 cells and a small number of challenges (5 per player). When designing the game scenarios and questions, we carefully chose the wording so that children could perceive the given challenges without difficulty. We used simple, child-friendly language to ensure that children in our target age group could understand the meaning and context of each challenge. We presented only one cybersecurity topic for each challenge and asked only one question related to that topic. We applied this segmenting principle so that children could process one topic at a time and avoid cognitive overload. In addition, in consideration of the developmental fit, we used colorful illustrations throughout the game (Fig. 1).

3.2.1. The challenge scenarios

To design these challenges, we used a combination of storytelling and a quiz approach. Storytelling has proven effective in increasing children's awareness of cybersecurity issues such as privacy, online personal identity, and content appropriateness [49]. Using a storytelling approach to visualize cybersecurity scenarios and collect inputs from children has been effectively employed by many researchers (e.g., [3,49–51]). Thus, we have designed the scenarios and challenges for our study by taking inspiration from existing studies, including [21,52–55]. We had five such challenges for each player, covering the topics of basic internet etiquette, privacy on social media, phishing, password management, and cyberbullying. We included only five cybersecurity risks in the game to keep it simple and neither overwhelming nor time-consuming for the participants.

[1] https://mazegenerator.net

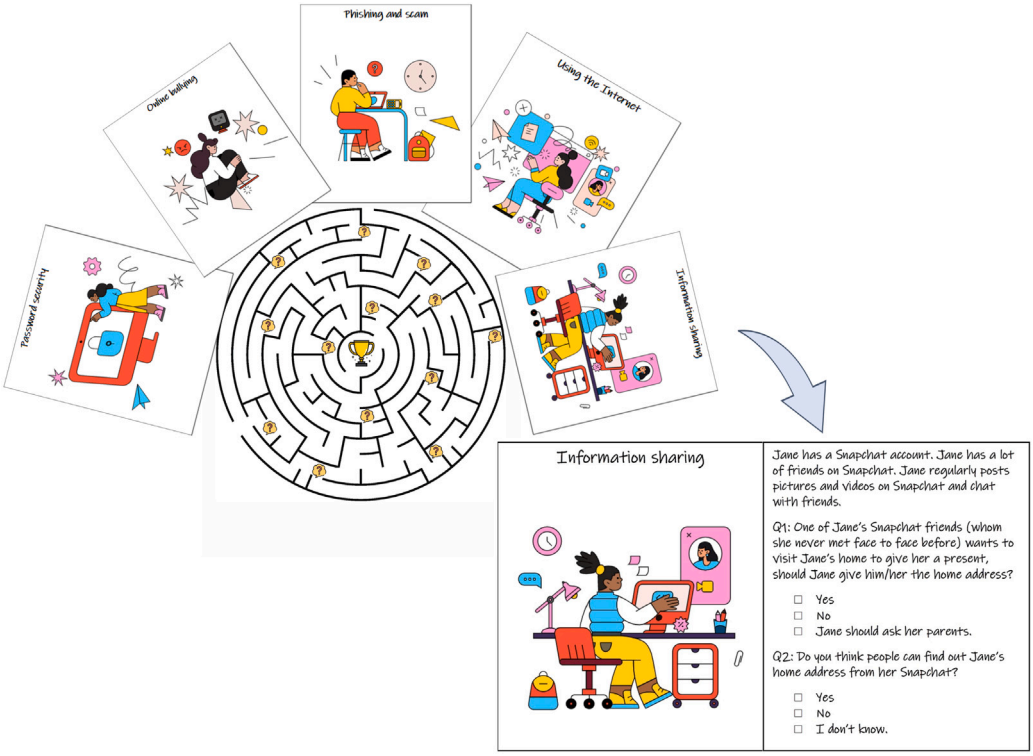


Fig. 1. The maze game and an example of a challenge card.

In each challenge, the player was given a scenario. We also included a few questions connected to the situations that each story presents and asked how the player would react in the given situation or what suggestion the player would give to the imaginary character in the story. These questions aimed to reveal the participants' behavior regarding risks and similar online situations. Each challenge ends with a question about a particular cybersecurity topic and provides several options from which players can choose. Some challenges also have the option of giving more than one answer. This combined approach has two goals: for parents to guide children to a particular scenario and to prompt reflection on how they would behave in similar circumstances, while for children we aimed to understand how much they know about online risks and how they handle them in real life.

However, instead of using precisely the same scenarios from the existing literature [3,49–51], we customized the scenarios to match the context of our maze game with a quiz approach. In our study, the challenges were customized depending on the age of the player, as noted above, so there is one set of child-specific challenges and another of parent-specific challenges, although the topics were the same for both parents and children. The children's challenges center on how much they knew about online risks and how they would react if presented with similar problems. On the other hand, the parent-specific challenges focus on caregiver perspectives and how they react or would react in comparable situations involving their children. An overview of all the challenges can be found online [56].

3.2.2. The gameplay

To conduct user studies for our research, we employed a paper prototype of CyberFamily and asked participants to play the game following the steps below.

1. The players will alternate turns.
2. Player 1 (either parent or child) starts first from one entry point and moves forward in the maze.
3. When Player 1 reaches a challenge, he or she will pick up one of the question cards and answer the question(s) on that card.
4. Once Player 1 answers the first challenge, Player 2 will start the game from another entry point.
5. When one player plays, the other player will wait for that player to answer a challenge.
6. Once Player 2 answers one challenge, Player 1 will continue to proceed in the maze.
7. The game continues until both players reach the destination point in the maze.
8. If needed, the players can discuss and help each other answer the challenges at any time during gameplay.

4. Methodology

According to Druin [57], participants can play four different roles in a technology design process: user, tester, informant, and design partner. Depending on the participant's role, the degree of involvement in the design process and thus the stage at which stage children become involved differ. In both our user studies, all participants (children and parents) played the roles of users and informants. Details about the user studies are provided below.

4.1. User study 1: Feasibility test

We conducted our first user study to test the feasibility of CyberFamily; this study was divided into three sections, each of which is explained in greater detail later in this section.

1. Pre-survey: Collect users' demographic data (age and gender of both parent and child, occupation of the parent).
2. Game playing activity: Participants play the game.
3. Focus group: Participants provide feedback regarding their experiences in using CyberFamily.

This article primarily reports the findings from the focus group discussions for this user study (see Section 5.1). As we aimed to test the feasibility of the game concept and understand the participants'

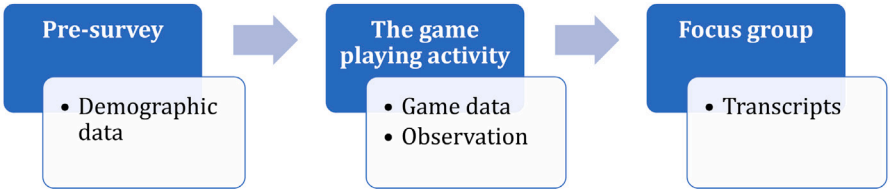


Fig. 2. Study process and data collected (feasibility test).

Table 1
Breakdown of the feasibility study timetable.

Task	Estimated time
Welcome and settle down	10 min
Introduction, filling out consent and demographic forms	15 min
Playing the game	45 min
Snack break	10 min
Focus group discussion and conclusion	35 min

Table 2
Breakdown of the usability study timetable.

Task	Estimated time
Welcome and settle down	10 min
Introduction, filling out consent and pre-survey forms	15 min
Playing the game	40 min
Snack break	20 min
Post-survey	35 min

opinions of the game, we have focused mainly on the in-depth understanding of the participants' feedback and thus not included any analysis of the game-playing activity and observation data from the feasibility test.

4.1.1. Participants and recruitment

A total of eight participants (four pairs of children and parents) participated in the feasibility test. We employed a self-selection technique to find participants by contacting people who might know parents who had children in the target age range. Ultimately, the age of the child participants ranged from 9 to 13. Though our targeted age range was 9–12, one of the children turned 13 just a week before our session date, and as both the parent and child were interested in taking part in the activity, we included them in the study. Among the four children, two were boys, and two were girls. The parents were diverse in terms of occupation; all had higher education; there were three fathers and one mother.

4.1.2. The game session

At the beginning of the session, we introduced ourselves to the participants. We presented a brief overview of the session plan and asked participants to fill out demographic and consent forms. An overview of the session plan is presented in Table 1. We briefed the participants about the game rules and steps before asking them to begin playing. The main game task was allotted 45 min, followed by a short break, while the discussion and conclusion were allocated a total of 35 min. We chose 45 min for the game task so that all the participants would have ample time to understand and play the game to completion. However, participants could finish the game within 30 min.

As the prototype was a low-fidelity paper version of the game, there was no automated functionality to verify whether players' answers in the game were right or wrong. However, after all the participants finished playing, we asked them if they had any questions or were confused about the topics or scenarios presented in the game and briefly discussed them. In addition, as there was no automated or instant feedback on the answers, we allowed the participants to answer the questions (challenge cards) and move forward in the game regardless of whether their answers were correct. This was to ensure that participants felt motivated to continue playing the game even if they answered incorrectly; stopping or interrupting the participants while playing might have had an influence on their engagement with playing. However, for future iterations of game development and in moving towards a digital version, we plan to implement mechanisms to provide instant feedback on the answers and their impact on game progression, along with guidelines about appropriate solutions and recommended actions regarding the online scenarios and activities.

4.1.3. Focus group

After finishing the game task and a short snack break, we continued the feasibility test with a focus group discussion [58]. We performed focus groups separately but simultaneously with parents and children to ensure that each group could express their thoughts freely without feeling conscious about how their family members would react. During the focus group discussion, we dealt with three main questions:

- What was good about this game? What did you like the most?
- Is there anything you did not like and/or found challenging in the game?
- What would you change in this game if you could?

We asked open-ended questions so as not to guide respondents and to allow them to express themselves freely. In addition to the three questions and related discussions during the focus group, we also considered correct or recommended behaviors in the challenge scenarios if a participant had further questions regarding the answers. After the focus group discussion, we concluded our session and handed out cinema gift cards to all the participants to express our gratitude for their time, participation, and input.

4.2. User study 2: Evaluation of CyberFamily

In our second user study, we focused on the usability evaluation of the CyberFamily game and verified our assumptions. To conduct the usability evaluation, we followed the steps in Rubin and Chisnell [59]. We first developed the evaluation plan, followed by the evaluation environment, participant recruitment, and the evaluation questionnaires. Before the user study began, we introduced ourselves to the participants and briefly described our work and the objectives of the activities. In order to better understand the participants' demographics and general game-playing habits (such as whether they play games at home and the kinds of games they play), we conducted a brief pre-survey before the CyberFamily game play began. Afterward, the players were asked what they thought of the game in a post-survey. Details of the study sessions and our data collection are illustrated in Fig. 3 and Table 2.

4.2.1. Participant recruitment

A total of 11 pairs of children and parents participated in this study. The participants were recruited through a local technology club for children, a voluntary organization run primarily by the parents of the participating children. In this club, the children (aged 9 to 12) practice various activities, including making robots using Scratch and building Lego structures. The children also had the experience of participating in robotics competitions and Lego leagues at the national and international levels. As our game is a collaborative game for children and

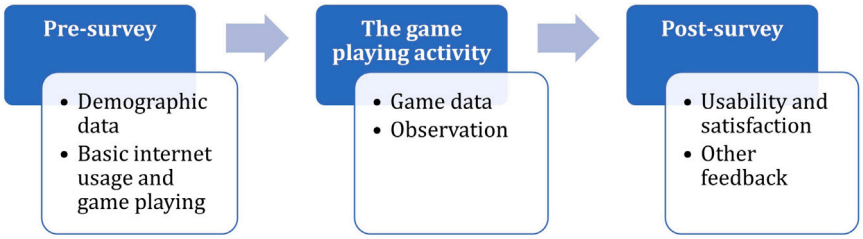


Fig. 3. Study process and data collection (usability evaluation).

parents, the children from the club participated with their parents. The parents' educational qualifications varied from bachelor's to doctoral degrees; all the adults had higher education. The gender distribution of the children was three girls and eight boys; among the parents, there were five mothers and six fathers.

4.2.2. Child and parent usability questionnaires

The child questionnaire contained seven five-point Likert-type scale questions covering three constructs to evaluate the usability of CyberFamily: ease of use (Q1, Q2), ease of learning (Q3, Q4), and engagement (Q5–Q7). The questions for the children were as follows:

- (Q1) Was the game easy for you to understand and play?
- (Q2) Did you and your parent play the game well?
- (Q3) Has the game helped you improve your online security knowledge?
- (Q4) Did the game help you talk about online security with your parent?
- (Q5) Will you play the game again to learn about other security topics?
- (Q6) Will you play the game with your brother or sister?
- (Q7) Will you tell your friends about this game?

The questions were coded from one *least positive* to five *most positive*. The survey continued with some open-ended questions that asked the children if they had learned something new about online security by playing the game and how they had learned it (from the game questions or in discussions with a parent or other children), what other topics they would add to the game, and what they liked and disliked about the game.

The parent questionnaire was based on the same three constructs: ease of use (Q1, Q2), ease of learning (Q3, Q4), and engagement (Q5–Q7). It contained seven five-point Likert-type scale questions:

- (Q1) How age-appropriate was the game for the children?
- (Q2) How well did you and your child interact during the game?
- (Q3) How effective was the game as a learning tool for children?
- (Q4) How well did the game facilitate discussions about online security between you and your child?
- (Q5) Will you play the game again with your child?
- (Q6) Will you recommend this game to other parents?
- (Q7) Will you use the game to teach your child about other security topics?

The parent questionnaire also had open-ended questions similar to the children's questionnaire.

4.3. Data analysis

The feasibility test yielded a range of data: demographic information, observation notes the researchers took during the game-playing session, and transcripts from the focus group discussions (Fig. 2). All the data were anonymized before we conducted the analysis (in both studies). We used thematic analysis for the focus group transcripts and synthesized the results following the steps recommended by Cruzes and Dybå [60]. We took an inductive approach to the analysis. The transcripts were reviewed line by line; as a concept became apparent, a code was assigned. Later, we merged similar codes and categorized them into themes. After analyzing the transcripts of the focus group discussions with parents and children, we identified six main themes, which are presented in Section 5.1. We did not perform any analysis on the observation data; the purpose of observing the participants as they engaged with CyberFamily was to see if our game was easy for them to understand and if they needed help playing it.

The data from the usability evaluation were analyzed using a mixed methodology. We gathered both qualitative and quantitative data from the game evaluation. The participants' responses to the open-ended survey questions from the post-survey, observational notes, and game-playing activity outcomes made up the qualitative data that we used to verify our assumptions, while we conducted a quantitative analysis of the data from the five-point Likert-type scale questions from the usability evaluation. We present our quantitative analysis results using simple descriptive statistics and qualitative results in detail in Section 5.2.

To ensure the reliability of the scales, we utilized Cronbach's alpha indicators for the items of the individual constructs and evaluated the reliability of each item by measuring its factor loading onto the underlying construct (Tables 3 and 4). Manly [61] suggested that a factor loading of 0.6 is a good indicator of item-level validity. For Cronbach's alpha, values between 0.50 and 0.80 are generally considered to indicate moderate reliability, whereas values above 0.8 are considered high reliability [62,63]. However, in our study, Cronbach's alpha values ranged from 0.448 to 0.902. The alpha values were comparatively low for the constructs ease of use and ease of learning, which could be explained by the fact that each of these constructs comprised only two items.

Table 3
Summary of the measurement values (children's questionnaire).

Construct	Item	Mean	SD	Load	Cronbach alpha
Ease of use	Q1	4.55	0.522	0.838	0.775
	Q2	4.45	0.688	0.849	
Ease of learning	Q3	3.64	0.809	0.752	0.515
	Q4	3.82	1.168	0.788	
Engagement	Q5	2.77	0.833	0.855	0.833
	Q6	2.50	1.619	0.911	
	Q7	3.00	0.816	0.614	

Table 4
Summary of the measurement values (parent's questionnaire)

Constructs	Item	Mean	SD	Load	Cronbach alpha
Ease of use	Q1	4.09	0.539	0.859	0.586
	Q2	4.00	0.447	0.867	
Ease of learning	Q3	3.27	0.467	0.698	0.448
	Q4	3.82	0.405	0.861	
Engagement	Q5	2.89	1.167	0.896	0.902
	Q6	3.44	1.130	0.861	
	Q7	3.33	1.118	0.949	

4.4. Ethics

Before conducting the study, we obtained approval from the Norwegian Agency for Shared Services in Education and Research[2] for data collection and child participation. We collected signed informed consent from each participant before starting a study. The parents signed the consent forms for themselves and on behalf of their children. Additionally, before beginning the data collection, we fully disclosed to the participants the purpose of the study, the types of data we would collect from them, and their right to withdraw from the study at any point.

5. Results

In this section, we present the results from both our user studies: the results from the feasibility study in Section 5.1 and the usability evaluation results in Section 5.2.

5.1. Results of the feasibility study

We obtained valuable feedback about the game and its feasibility during the focus group discussions with parents and children. As described above, we asked participants to give feedback on three main topics: what was good about the game, what was not, and whether they had any suggestions to improve it. All the participants gave positive feedback about the game; indeed, none mentioned disliking anything. Below, we present the six key themes that emerged from the discussions.

5.1.1. An opportunity to think and reflect

One goal of CyberFamily was to help parents and children reflect on the security issues they face in their daily lives. We designed the questions with relevant scenarios to help players connect their own experiences with those scenarios. As intended, all four parents indicated that this game was a good opportunity for them to reflect on how they think about and handle online security issues at home. The game's scenario-based questions thus helped them relate to their real-life situations. When asked about their opinion of the game, one parent replied,

"We do not sit together (at home) for things like this. It gave us the opportunity to go through this and see. I mean, there were some questions that we had never thought about before. Or, you can say 'I never thought [about that.' So that is very good about this game. And yes, even my daughter was sometimes like, "'Ah!' [an expression of surprise]. So, these kinds of expressions and questions will make us think and do something about this." (T2-parent).

This quotation indicates that even the child was able to think about online risk and was prompted to ask the parent questions. This observation was supported by the statement of another child who said that *"The questions were pretty good. There was a story behind each question, which made me think about it"* (T3-child).

5.1.2. An environment for learning

Another important theme that emerged in the discussions was the environment for learning about online security-related issues at home. During the focus group, we asked the children if they talked about online security and cyber risks at home with their parents. All four said that they usually do not have this kind of discussion with their parents. However, one mentioned that his elder sister discusses her experiences with him:

"Not with my parents; I talk about this with my sister [who is 16 years old]. She shares her experiences with me. For example, she met some people online, but those people who were not as polite or nice as they seemed to be. She shared her experience with me and said that I should not meet or trust people like that." (T3-child).

As pointed out by the parents, the game helped create an environment in which parents and children could discuss online security issues and learn together, even when playing a game: *"To create awareness on the topic, it was a good exercise. Absolutely"* (T4-parent).

5.1.3. Promotes collaboration

Along with raising children's awareness, one of the game's main goals is to increase parent–child collaboration and give parents a role in which they can engage with their children's online interactions. From the discussions with the participants, it seemed that the game could promote and enhance parents' collaboration with their children, as is reflected in this statement by a parent:

"I think it is a good opportunity to talk about these things, and you can also learn from each other. Children know many things that we do not necessarily know that they know. So, it is a good way to work together and talk about these things." (T3-parent).

In addition, from the discussion with the children, we found that sometimes parents may not be able to play the typical entertaining games with their children, perhaps due to a lack of time or interest. One child mentioned that,

"My parents are not interested in playing games. They think playing video games is not fun; they do not like or understand the games. Once, I tried to teach my dad to play a game, but he thought it was boring. I showed him a hunting game, and he got bored after 15 min." (T3-child).

Unlike a regular entertainment game, we observed that all the participants, whether children or parents, were very focused and engaged in the game while they were playing. Both parents and children asked each other questions regarding the game challenges and had conversations about the topics presented in those challenges.

5.1.4. Awareness for both parents and children

Supporting the findings from previous research [7,31], our results again show the need for parental awareness of cybersecurity issues. Multiple parents from this study indicated that they also need training and awareness to help their children with cybersecurity issues. As this parent said,

"I think at the transition point, like me, we started with very basic technology but now moving towards very advanced technology, so probably we cannot cope with this as much as the kids. They are smart with this [technology]. [...] I am not really equipped with enough knowledge in this regard. So, if I say something, I say it from an everyday ground, not like a technical ground. So, I probably need more training than my kid." (T2-parent).

From the focus group discussions, we could see that participants agreed that our game contributes to increasing awareness for both parents and children. While traditional learning games usually focus on a specific target group, CyberFamily focuses on raising awareness for both parents and children, fulfilling the needs of both groups: *"And that is what I think is good about your game here. Because it raises awareness on both parts and creates a dialogue; that is good. And yeah, parents need to be taught about this as well, because we are barely hanging on."* (T3-parent).

5.1.5. A combination of learning alone and learning with parents

In addition to the themes noted above, we found another interesting theme: the combination of learning alone and learning with a parent. Two parents mentioned that a cybersecurity awareness game should allow children to play both alone and with their parents. The rationale behind this opinion is the boundary between respecting children's privacy and parental control. One parents stated that,

"Children do not like to sit with their parents all the time. And they just like to do it alone sometimes, or they feel comfortable doing it alone. And they may sometimes feel that parents are doing too much parenting." (T1-parent).

[2] https://sikt.no/en/about-sikt

Another parent had a similar concern: *"The environment you have created here cannot be created at home. Because as he [T1-parent] said, they sometimes like to play games by themselves. They think we are not really cool enough to play with them."* (T2-parent).

Nevertheless, when asked about preferences about what type of games (i.e., a single-player game for children or a collaborative game for multiplayer) we should design for children on the topic of cybersecurity, the same parents highlighted the need for collaborative games:

"I think a collaborative game would be the best for the kids, so that if they do something wrong, we can know that, and then we can teach them. Sometimes the kids are quite good, even with their parents. So yeah, I think collaborative is the best [approach]." (T1-parent).

5.1.6. Suggestions for improvement

During the focus group discussion, we asked participants if they had ideas for improving our game. We received some interesting suggestions from both parents and children. One child said that in his opinion, the maze game could be more interesting and motivating for the players. He suggested that there should be a goal behind each of the challenges in the maze, like mini-games, rather than just the one final goal of reaching the final destination. A player will feel motivated to keep playing if there are mini-goals with each of the challenges. The child added that,

"I think it should be like if you go through the maze, probably like the TV series 'The Maze,' that you find some checkpoints where you have to find different things to build up towards the end or like a password or something that you can find hints all over the maze." (T3-child).

However, not all the suggestions were directly relevant to our game; parents also had ideas for games in general and raising cybersecurity awareness. For example, one parent suggested that using demos in games can also help players learn, citing Fortnite as an example:

"They [Fortnite] have a small demo that every kid must go through and then say, 'OK, I have read it.' Not just like we do with a PDF reader, not reading like that. But you play like a small demo, and then you learn a little about what can be done in the game and what the responses can be. And then you can go for the game. So this kind of demo before you can play the Fortnite game, for example [would be helpful]." T2-parent.

The parent from Team 1 also talked about parental awareness and suggested ways for other parents to ensure a safe environment at home, emphasizing the need to be aware of sharing Wi-Fi passwords with outsiders, such as guests or neighbors, and the need to monitor the children's online activities.

5.2. Results of the usability evaluation

In this section, we present the results of our evaluation study in two phases. First, we provide an overview of the results of the game-playing activities and our participants' cybersecurity awareness level based on those results. We then present the results of the usability measurement of CyberFamily and our findings in regard to our two assumptions.

5.2.1. Participants' demonstrated cybersecurity awareness

Before getting into the game's usability evaluation outcomes, we analyzed the participants' cybersecurity knowledge and awareness to better understand their expertise and contextualize our data for the game evaluation (i.e., their responses in terms of learning). A general understanding of the participants' knowledge will also help us in future iterations of game creation and content; we can stress cybersecurity issues or concentrate on areas where children and/or parents are uninformed or need a deeper understanding of core ideas.

Children's cybersecurity awareness: Of the five cybersecurity themes in the game, the children demonstrated the most awareness of cyberbullying. They all felt that Sara (the character in the scenario), in the bullying situation depicted on a card, should take appropriate action, including reporting the bullying to her teachers and parents and documenting it with screenshots. However, whereas all the children said that Sara should inform her parents, three children did not select the option of informing teachers. Regarding phishing and scams, none of the children considered clicking a link to reveal a prize, as presented on the card scenario. However, only two children were confident enough to choose "No" as the response to the phishing attempt. The remaining nine children chose to ask parents about how Timmy (the character in the scenario) should respond, which may indicate that even though the children were suspicious about the whole prize-winning scenario, they were not sure enough to decide on their own and thus preferred to seek help from their parents. In terms of information sharing and GPS location sharing in Snapchat, nine children indicated that they knew that Snapchat could reveal their home address, and eight said that Jane should not share her address; the remaining three said she should ask her parents. The children displayed a limited amount of awareness when it came to online etiquette and password security. In these two scenarios, we listed a number of recommended practices and asked the children to select which ones they thought should be suggested to the character in the scenario on the card. All the children selected a few of the better internet usage habits from the list, but only two could identify every single good practice. Similarly, every child named more than one best practice for password management, but none chose all the best practices to recommend to the scenario's character.

Parent's cybersecurity awareness: The parents showed a good level of understanding of the cybersecurity topics presented in the game and how they would deal with such scenarios with their children. They all indicated that they would suggest that their children choose a random password when asked about suggestions they would give to their children about passwords. Regarding phishing and scams, all the parents mentioned that they would show the scenario to their children and explain those risks. As for cyberbullying, 10 of 11 parents said the scenario on the card could be considered bullying. However, four thought that it was a normal thing to happen among children, even though they identified the scenario as bullying and inappropriate behavior. Interestingly, most parents (7 of 11) did not choose to inform their children's teachers about the bullying, even though the cyberbullying scenario referred to a school environment. All the parents were well aware of the risks of bullying and the correct age limit for Snapchat, though two did not know that Snapchat could reveal the user's home location through map sharing. Finally, parents had the least level of awareness when it came to understanding the fundamentals of online etiquette. For instance, six parents did not consider "checking privacy settings regularly," and five did not consider "safety issues of open/free Wi-Fi." Three parents did not consider "GPS and risks of location sharing" to be crucial lessons they should teach their children.

5.2.2. Usability of CyberFamily

Here, we present the usability evaluation of CyberFamily in relation to our assumptions and the game's usability scores. As indicated in Section 4.2.2, CyberFamily's usability was evaluated in terms of ease of use, ease of learning, and engagement. Fig. 4 presents an overview of the means for each construct based on the ratings participants gave in the five-point Likert-type scale questions.

The children rated the CyberFamily game highly regarding ease of use (4.49/5) and learning (3.72/5). However, the ratings for engagement and intent to play the game again were slightly lower than the other two constructs; the engagement score was only 2.6/5. The results from the parents were somewhat similar; the parents rated the game more highly in terms of ease of use (4.05/5) and learning (3.54/5) but lower in terms of engagement (3.21/5). However, the differences in average scores across the constructs were smaller for parents than for children. A more detailed breakdown of the average rating for each question can be found in Fig. 5.

It is important to note that two of the parents answered the engagement questions (Q5–Q7) in words rather than giving a numerical

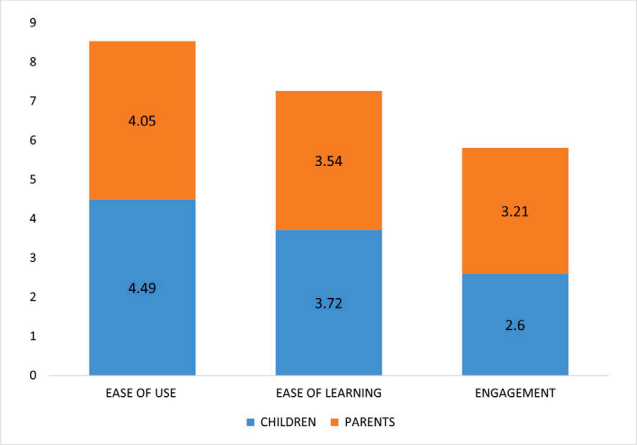


Fig. 4. Overview of the mean values for each construct.

score; hence, we removed their answers when calculating the mean values. In addition, one of the children did not answer Q6, which we removed when calculating the mean. We discovered some likely causes that may have influenced participants' perceptions and scores for the engagement criteria based on the open-ended questions in the usability questionnaire. We further discuss these potential reasons for lower scores for engagement in Section 6.3.2.

5.2.3. Knowledge acquisition and transfer

To verify our first assumption about collaborative learning, we asked our participants if they had learned anything new from playing the game or discussing any topics with their game partner while filling out the post-game questionnaire. Even though there were some gaps in knowledge of specific topics, as noted in Section 5.2.1, all the participants at least had a basic understanding of each topic.

Regarding learning and knowledge acquisition by the children, two child participants mentioned that phishing was new to them. Two other children reported learning outcomes, such as learning more about password practices and the security concerns with open Wi-Fi networks. Other than that, four children said that they had learned about online security and why it is important from the game, but they did not describe what they had learned in detail. The children who reported these learning outcomes indicated that they had learned from both playing the game itself and discussing the game questions with their parents.

Among the parents, two mentioned that they did not know how to identify secure networks and what the lock sign beside the URL means. One parent learned about this by playing the game, and the other parent learned it when her 12-year-old son explained it to her during the game (as in the right-hand photograph in Fig. 6). Another parent mentioned that she learned how Snapchat (especially the map feature) works from her child during the game. In addition, six parents said that although the game did not provide any new information or anything they did not know before, playing the game with their children helped them grasp their children's cybersecurity knowledge and behavior. Thus, from participating in our workshop and playing CyberFamily, parents learned about their children and what they should know more about to help them.

Overall, as stated above, some participants reported learning from one another, even if not all said they had learned in that way. Thus, we can state that our first assumption — that playing a collaborative family game can facilitate collaborative learning between parents and children — is supported to some extent.

5.2.4. Effect of collaboration

In order to verify our second assumption, we observed the participants' activities during game play and how they communicated with one another. We noticed that the game encouraged discussions between parents and children about cybersecurity that were motivated by CyberFamily and the subjects it covered. For example, we refer to the episode shown in Fig. 6, in which one child explains secure URLs and lock signs to his mother (and others). We observed similar conversations among the participants, with children or parents explaining topics from the game — the map feature in Snapchat, password practices, and so on — to one another. As a result, our second assumption concerning fostering communication between parents and children is supported, just as it is by both the observational data and the post-survey findings. In that questionnaire, we asked participants what they liked about the game; six parents responded that they appreciated the fact that it allowed them to engage and communicate with their children about cybersecurity.

5.2.5. Game evaluation results in summary

Overall, the usability evaluation of CyberFamily contained positive responses from both parent and child participants. The game scored above average in all three evaluation criteria but was better in ease of use and learning than in engagement. The results indicate that the proposed CyberFamily game does offer the prospect of helping children and parents with cybersecurity knowledge and awareness while facilitating communication and sharing knowledge and experiences in a family context.

Despite the fact that our study participants already had a good level of cybersecurity knowledge, playing the CyberFamily game resulted in learning new information for some participants. This result shows that a collaborative game like CyberFamily can facilitate collaborative learning between parents and children, as our first assumption proposed. However, any one individual's learning is a dynamic experience that can depend on and be influenced by a number of underlying and contextual factors. We further discuss our findings related to this result in Section 6.3.1.

The results of the post-survey and our observational data indicate that our second assumption is supported. We observed several episodes during the workshops in which the CyberFamily game led participants to discuss cybersecurity and related issues with one another. From our observations, we believe that these dialogues between parents and children fostered knowledge-sharing and understanding.

6. Discussion

As presented throughout this paper, we aimed to explore opportunities to leverage parent–child collaboration to raise cybersecurity awareness using a game-based learning approach. Our study thus provides valuable insights into how parents and children can collaborate to raise cybersecurity awareness using a game. Our preliminary findings from both user studies show that parents and children accepted the idea of a collaborative game to learn about cybersecurity and that the CyberFamily game facilitated knowledge sharing and collaboration between the parents and children. Additionally, the game helped the parents understand how their children might act in certain online situations and allowed them to participate in discussions about their children's digital activities. Similarly, it enabled the children to discuss their online experiences with their parents. This section further discusses the main takeaways from our feasibility and game evaluation studies.

6.1. Knowledge sharing and awareness

One of our key assumptions of the CyberFamily game design was that communication between parents and children would facilitate knowledge sharing about cybersecurity. The results of both user studies

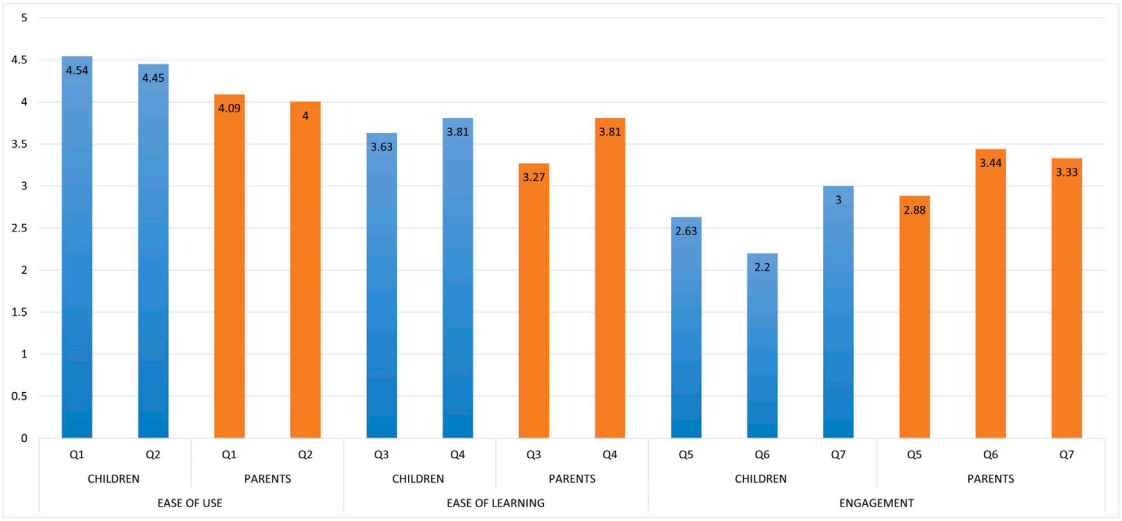


Fig. 5. Mean values for each question.

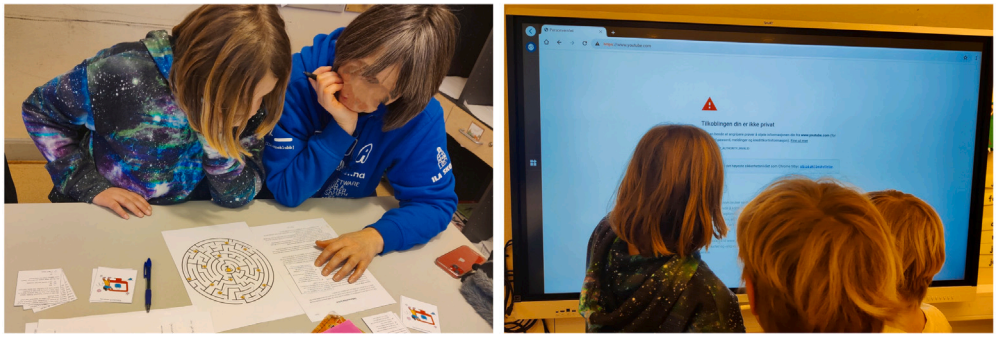


Fig. 6. Photographs from the user study (left: a parent–child duo playing the CyberFamily game; right: a child explains secure URLs).

show that the CyberFamily game did, in fact, promote dialogue between parents and children and eventually led to knowledge sharing on multiple occasions. One episode from the feasibility study serves as an example: while playing the game, the parent from Team 1 answered the question about Snapchat incorrectly, and his 12-year-old daughter immediately pointed that out and explained why his answer was not the right one. Later on, observing the same team, we saw that the daughter chose the incorrect answer to one of the password security questions; her father noticed and explained to her why had erred. This episode clearly shows how the game facilitated knowledge transfer between parents and children, who helped one another to learn about cybersecurity and create awareness. We also saw the same kinds of conversations and knowledge-sharing in other teams. During the usability evaluation study, we observed episodes in which children and parents helped one another learn about cybersecurity (see Section 5.2.3). Therefore, we argue that collaborative games on cybersecurity awareness, such as CyberFamily, have significant potential to improve cybersecurity knowledge and understanding for both parents and children. If parents have sufficient cybersecurity proficiency, they can better contribute to their children's cybersecurity knowledge and behavior development, as other researchers have suggested (e.g., [6,64]). Researchers and practitioners from this domain should focus more on engaging other stakeholders — and not only children — when designing cybersecurity games or training materials. Such games can also improve the measures parents and children take to ensure children's online safety and improve behavior from an early age by working together at home.

6.2. Improving family communication

It is sometimes challenging for parents to understand how their children act in the digital realm and to acquire cybersecurity-related knowledge without directly engaging with them, as indicated by earlier research (e.g., [31]). Hartikainen et al. [34] highlight the need to build technical mediation for children's online safety that is transparent and facilitates the building of trust. The challenge scenarios in this game allowed the parents to see how their children are likely to behave in certain real-life situations. Based on the children's responses, the parents could explain and offer relevant suggestions about how to handle risky situations in real life. We also observed children asking questions of their parents about the game scenarios when they needed clarification. Therefore, the findings of our studies suggest that a collaborative game like CyberFamily can help parents play an active and engaged role in their children's digital lives while also improving parent–child communication and family collaboration.

In both studies we conducted, we observed occasions on which either a parent or child had limited knowledge of a specific cybersecurity topic and were thus prompted to ask questions. Nevertheless, we acknowledge that there could be scenarios where a child or parent had all the knowledge required to answer all the questions of the game correctly and would not need help from the other player. In addition, there could be a scenario where neither the parent nor the child knows the correct answer. Either way, we believe this game can still be an effective tool in providing an environment for discussion and joint learning, allowing parents and children to sit together and talk about cybersecurity topics and build understanding and trust, which is a goal of CyberFamily and our research more broadly. Moreover, as stated

in Section 5.2.3, we observed an episode where one child knew about secure URLs and what the lock sign beside a URL meant and explained it to both a parent and other children. Thus, the game resulted in communication not only between a parent–child pair but also among the children and other parents.

6.3. Key findings from CyberFamily usability evaluation

In the following section, we discuss our findings and note takeaways specifically related to the evaluation study of CyberFamily and its usability.

6.3.1. Impact of CyberFamily on participants' learning

The results of the CyberFamily game-playing activity in our second user study showed that participants (especially the parents) had good proficiency in various cybersecurity concepts and were familiar with many of the topics presented in our game, at least to some extent. This means that there may have been only a few new things for them to learn for the first time. Another possible explanation might be the background of the participants. We recruited the children from a technology club whose goal is to learn about technology and make innovative things using technology (such as programming LEGO robots). Thus, our sample of children may well have had higher technology and cybersecurity proficiency than other groups of children in the same age cohort. In addition, all the parents who participated were well educated, with university degrees in a range of disciplines. Conducting this study with a different sample with more diverse educational backgrounds and qualifications might have produced different results. Nevertheless, as presented in Section 5.2.3, there was some knowledge that a few participants reported learning from the game.

6.3.2. Opportunities to improve engagement of CyberFamily

We have identified a number of aspects to improve CyberFamily in our future work based on participant comments from the user studies. In addition to the participants' feedback during the feasibility test presented in Section 5.1.6, in the usability questionnaire, we again asked the participants for feedback on what they thought should be improved about the game and received some promising suggestions. We believe these suggestions are also related to why they rated the game less highly than the other constructs in terms of engagement. Two key pieces of feedback involved the game's replayability and its limited content. Both parents and children reported that they wanted more topics and challenges to be added to the game so that it could be played again with new challenges. One parent also responded that she would love to play the game again if there were new challenges and content each time. Thus, we believe the content limitation influenced participants' answers when asked about their intention to participate in the future. This is understandable, and expanding the content was already one of the goals for our future work. Another common item of feedback was to make the game interface more fun by using more game elements and animations, as people usually experience when playing mobile or online games in their daily lives. This suggestion is also not surprising to us as we used a low-fidelity paper prototype for the study, which is markedly different than the digital games the participants were used to playing. We believe this issue also influenced the responses for the engagement score.

6.3.3. Cybersecurity concepts and the need for real-life examples

Overall, the children and adults in our evaluation study demonstrated a good level of understanding of the cybersecurity topics covered in CyberFamily. However, we have discovered that while children may have some fundamental netiquette when engaging in online activities, they are not always acquainted with the relevant cybersecurity concepts and challenges. In our study, for example, we found that all the children said they would not agree to click any link in a suspicious email. However, two children stated that phishing was something they learned from the game, so there are some common cybersecurity issues that they were not able to identify, even though they knew enough not to fall prey to a suspicious link. This finding emphasizes the significance of embedding real-life components and examples in cybersecurity instructional tools that children can easily relate to and understand, as was suggested by Kumar et al. [50].

6.4. Potential of implementation in other contexts

Although CyberFamily's primary target users are parents and children, it also has the potential for use in other contexts. As pointed out by one child in our study (see the first quote in Section 5.1.2), siblings can be a valuable source for learning. So, the game can also be played between siblings instead of with parents. Another potential use is in the classroom. Instead of parents and children, we could organize a learning session where children from primary grades can play with children from secondary grades in pairs. Setting up the game in the school context could also result in positive knowledge sharing when the teachers review the gameplay.

6.5. Implications for game design

The overall findings from the usability evaluation study provided us with valuable guidelines and implications for future research. As we have seen, limited content in a game can influence a player's perception of the game; in our case, this issue impacted the players' views on engagement and made them less interested in playing the game in the future. Therefore, incorporating features into the game design that will give players a sense of making progress and the opportunity to reflect on their achievements over time is essential to capture and sustain players' attention [65].

Learning is a subjective process and depends on a number of individual factors, so it is necessary to make the content of a cybersecurity educational game as diverse and adaptable as possible. To make the CyberFamily game (and cybersecurity games in general) more acceptable for a wide range of users, we can incorporate multiple levels in the game and design the gameplay incrementally. Thus, based on individual skills and knowledge, players can progress in the game at their own pace. To maximize the learning impact, the game's level of difficulty and complexity should increase with a player's improving skill level. Furthermore, by introducing the cybersecurity topics and challenges gradually and grouping related content into levels according to topic complexity and associated difficulties, the players will be able to process the information gradually. When a player acquires a foundational understanding of cybersecurity, further complex concepts and challenges can be introduced at higher levels. Applying levels and an incremental approach to the game can also make it easily adaptable and open to further development. The field of technological development and the security concerns that accompany it are constantly changing. As a result, cybersecurity educational tools and resources need continuous development and should be easily adaptable with time.

6.6. Limitations and future work

Like any research, ours has certain limitations. The first involves the samples. Neither study's sample size was very large. Future studies with larger and more diverse sample pools are needed to produce more nuanced and generalized results. Our work at this stage has mainly aimed to assess the feasibility of the game as a general concept and to understand target users' perceptions of the prototype's acceptability and usability before further development. The second limitation of this research also relates to the samples. We used self-selection sampling as our recruitment strategy, and there is always a risk of bias when using that approach. To avoid bias in participant selection, we emphasized only the children's age and relevance to our study when recruiting participants. However, the parents we recruited in both of our studies

were highly educated. As previously discussed in Section 6.3.1, the background and proficiency level of the participants may have also impacted the evaluation results; both the children and their parents in our study may have had higher proficiency levels in technology use and related knowledge than would be true of people in general. Therefore, future research could focus more on preliminary studies before a usability evaluation to determine the proficiency levels of the participants and ensure that the tool (or the game to be evaluated) fits the maturity level of the targeted audience. Moreover, although we had four children participate in the focus group discussion during our first user study, only one child was vocal enough to share his opinions and experiences freely. The other three children were too shy to initiate any conversation on their own, and they replied quickly to the questions they were asked. A larger sample could be helpful in obtaining more opinions and feedback from the children.

The final limitation of this study is the fidelity issue of our prototype. The fidelity effect connected to the prototype's form can impact findings when evaluating prototypes [66]. Thus, our study participants' feedback may have been influenced by the fact that our game was a low-fidelity, paper-based prototype with limited content and functionalities, as discussed in Section 6.3.2. Though it is feasible to evaluate initial game concepts and design ideas at the early stages of game development using paper prototypes [66], we aim to continue working on the prototype to make it a more high-fidelity product. Moreover, in this initial stage, we incorporated only face-to-face collaboration in the game. Future research could explore what other forms of collaboration could be implemented in the game design to leverage parent–child collaboration in cybersecurity games and how different forms of collaboration operate.

7. Conclusion

Parents are usually regarded as responsible for dealing with the consequences of children's security issues. With the growing amount of online time spent by today's children, it is increasingly important that parents and children work together to ensure safe online and offline environments for children. Yet, there have only been modest efforts to help parents play an active role in supporting and interacting with their children regarding their online presence and managing their digital lives. The present study is one of the few to date that has highlighted this need, and we hope to inspire more work in this area.

The findings from our studies suggest that parents and children were keen to play a game in which they were guided to communicate and discuss cybersecurity issues. While confirming our first assumption (about collaborative learning) only to some extent, the game does provide an environment for discussion and communication between parents and children, supporting our second assumption. As a result, we believe CyberFamily might be a helpful example for future academics and practitioners to study this domain of research further and develop cybersecurity awareness tools and educational resources for children while keeping the roles and involvement of parents in mind. Such tools must support collaboration and facilitate the building of trust, as other researchers have highlighted [6,34]. This research, along with the presented game, showed the benefits of encouraging parent–child collaboration at home. Future research can explore more ideas and ways to leverage such collaboration in a family context and in the context of formal educational institutions.

However, before we conclude, we also want to emphasize the need for children's individual development in terms of critical thinking and decision-making ability. Parental involvement and guidance should be carefully balanced so as not to hinder a child's natural development or invade their privacy. We aim to increase parents' and children's communication, knowledge sharing, and understanding to ensure a secure digital world without violating children's right to privacy.

CRediT authorship contribution statement

Farzana Quayyum: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Validation, Visualization, Writing – original draft. **Letizia Jaccheri:** Funding acquisition, Project administration, Supervision, Validation, Writing – review & editing.

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.

Data availability

Data will be made available on request.

Acknowledgments

We extend our gratitude to all participants in our studies for generously contributing their time and providing valuable feedback. We also acknowledge Aida Omerovic for her insightful suggestions that significantly improved the manuscript, as well as Sigurd Røstad Augdal, Rolf Erik Sesseng Aas, and Ana Carolina Moises de Souza for their assistance in organizing the workshops.

References

[1] E.G.B. Gjertsen, E.A. Gjære, M. Bartnes, W.R. Flores, Gamification of information security awareness and training, in: ICISSP, 2017, pp. 59–70.
[2] F. Quayyum, D.S. Cruzes, L. Jaccheri, Cybersecurity awareness for children: A systematic literature review, Int. J. Child-Comput. Interact. 30 (2021) 100343.
[3] L. Zhang-Kennedy, Y. Abdelaziz, S. Chiasson, Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy, Int. J. Child-Comput. Interact. 13 (2017) 10–18.
[4] M. Olano, A. Sherman, L. Oliva, R. Cox, D. Firestone, O. Kubik, M. Patil, J. Seymour, I. Sohn, D. Thomas, {SecurityEmpire}: Development and evaluation of a digital game to promote cybersecurity education, in: 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, 3GSE 14, 2014.
[5] F. Giannakas, G. Kambourakis, S. Gritzalis, CyberAware: A mobile game-based app for cybersecurity education and awareness, in: 2015 International Conference on Interactive Mobile Communication Technologies and Learning, IMCL, IEEE, 2015, pp. 54–58.
[6] M. Nouwen, B. Zaman, Redefining the role of parents in young children's online interactions. a value-sensitive design case study, Int. J. Child-Comput. Interact. 18 (2018) 22–26.
[7] N.W. Rahayu, S. Haningsih, Digital parenting competence of mother as informal educator is not inline with internet access, Int. J. Child-Comput. Interact. 29 (2021) 100291.
[8] T. Minkus, K. Liu, K.W. Ross, Children seen but not heard: When parents compromise children's online privacy, in: Proceedings of the 24th International Conference on World Wide Web, 2015, pp. 776–786.
[9] M. Duggan, A. Lenhart, C. Lampe, N.B. Ellison, Parents and social media, Pew Res. Center 16 (1) (2015) 2.
[10] H.-Y. Sung, G.-J. Hwang, A collaborative game-based learning approach to improving students' learning performance in science courses, Comput. Educ. 63 (2013) 43–51.
[11] C.-H. Chen, V. Law, Scaffolding individual and collaborative game-based learning in learning performance and intrinsic motivation, Comput. Hum. Behav. 55 (2016) 1201–1212.
[12] N. Charlier, M. Ott, B. Remmele, N. Whitton, Not just for children: game-based learning for older adults, in: 6th European Conference on Games Based Learning, Cork, Ireland, 2012, pp. 102–108.
[13] R. Chandarman, B. Van Niekerk, Students' cybersecurity awareness at a private tertiary educational institution, Afr. J. Inf. Commun. 20 (2017) 133–155.
[14] N.H.A. Rahim, S. Hamid, M.L.M. Kiah, S. Shamshirband, S. Furnell, A systematic review of approaches to assessing cybersecurity awareness, Kybernetes Int. J. Syst. Cybern. 44 (4) (2015) 606–622, http://dx.doi.org/10.1108/K-12-2014-0283.
[15] N.H. Abd Rahim, S. Hamid, M.L.M. Kiah, S. Shamshirband, S. Furnell, A systematic review of approaches to assessing cybersecurity awareness, Kybernetes (2015).

[16] V. Švábenskỳ, J. Vykopal, P. Čeleda, What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences, in: Proceedings of the 51st ACM Technical Symposium on Computer Science Education, 2020, pp. 2–8.
[17] F. Alotaibi, S. Furnell, I. Stengel, M. Papadaki, A review of using gaming technology for cyber-security awareness, Int. J. Inf. Secur. Res.(IJISR) 6 (2) (2016) 660–666.
[18] M. Papastergiou, Digital game-based learning in high school computer science education: Impact on educational effectiveness and student motivation, Comput. Educ. 52 (1) (2009) 1–12.
[19] R. Rosas, M. Nussbaum, P. Cumsille, V. Marianov, M. Correa, P. Flores, V. Grau, F. Lagos, X. López, V. López, et al., Beyond Nintendo: design and assessment of educational video games for first and second grade students, Comput. Educ. 40 (1) (2003) 71–94.
[20] J. Allers, G.R. Drevin, D.P. Snyman, H.A. Kruger, L. Drevin, Children's awareness of digital wellness: A serious games approach, in: IFIP World Conference on Information Security Education, Springer, 2021, pp. 95–110.
[21] O.-G. Baciu-Ureche, C. Sleeman, W.C. Moody, S.J. Matthews, The adventures of scriptkitty: Using the raspberry pi to teach adolescents about internet safety, in: Proceedings of the 20th Annual SIG Conference on Information Technology Education, 2019, pp. 118–123.
[22] C.E. Irvine, M.F. Thompson, K. Allen, Cyberciege: gaming for information assurance, IEEE Secur. Priv. 3 (3) (2005) 61–64.
[23] M. Hendrix, A. Al-Sherbaz, B. Victoria, Game based cyber security training: are serious games suitable for cyber security training? Int. J. Serious Games 3 (1) (2016).
[24] D. Avelar, R.A. Dore, A.J. Schwichtenberg, C.K. Roben, K. Hirsh-Pasek, R.M. Golinkoff, Children and parents' physiological arousal and emotions during shared and independent e-book reading: A preliminary study, Int. J. Child-Comput. Interact. 33 (2022) 100507.
[25] M.A. Moreno, K.G. Egan, K. Bare, H.N. Young, E.D. Cox, Internet safety education for youth: stakeholder perspectives, BMC Public Health 13 (1) (2013) 1–6.
[26] S. Livingstone, E.J. Helsper, Parental mediation of children's internet use, J. Broadcast. Electron. Media 52 (4) (2008) 581–599.
[27] A.R. Lauricella, R. Barr, S.L. Calvert, Parent–child interactions during traditional and computer storybook reading for children's comprehension: Implications for electronic storybook design, Int. J. Child-Comput. Interact. 2 (1) (2014) 17–25.
[28] E. Beheshti, K. Borgos-Rodriguez, A.M. Piper, Supporting parent-child collaborative learning through haptic feedback displays, in: Proceedings of the 18th ACM International Conference on Interaction Design and Children, 2019, pp. 58–70.
[29] J.M.-C. Lin, S.-F. Liu, An investigation into parent-child collaboration in learning computer programming, J. Educ. Technol. Soc. 15 (1) (2012) 162–173.
[30] O. Sadka, H. Erel, A. Grishko, O. Zuckerman, Tangible interaction in parent-child collaboration: Encouraging awareness and reflection, in: Proceedings of the 17th ACM Conference on Interaction Design and Children, 2018, pp. 157–169.
[31] F. Quayyum, J. Bueie, D.S. Cruzes, L. Jaccheri, J.C.T. Vidal, Understanding parents' perceptions of children's cybersecurity awareness in Norway, in: Proceedings of the Conference on Information Technology for Social Good, 2021, pp. 236–241.
[32] F. Tazi, S. Shrestha, D. Norton, K. Walsh, S. Das, Parents, educators, & caregivers cybersecurity & privacy concerns for remote learning during covid-19, in: Chi Greece 2021: 1st International Conference of the Acm Greek Sigchi Chapter, 2021, pp. 1–5.
[33] D. Boyd, E. Hargittai, Connected and concerned: Variation in parents' online safety concerns, Policy Internet 5 (3) (2013) 245–269.
[34] H. Hartikainen, N. Iivari, M. Kinnula, Should we design for control, trust or involvement? A discourses survey about children's online safety, in: Proceedings of the the 15th International Conference on Interaction Design and Children, 2016, pp. 367–378.
[35] K. Badillo-Urquiola, C. Chouhan, S. Chancellor, M. De Choudhary, P. Wisniewski, Beyond parental control: designing adolescent online safety apps using value sensitive design, J. Adolesc. Res. 35 (1) (2020) 147–175.
[36] A. Gokhale, Collaborative learning enhances critical thinking, J. Technol. Educ. 7 (1) (1995).
[37] P. Resta, T. Laferrière, Technology in support of collaborative learning, Educ. Psychol. Rev. 19 (1) (2007) 65–83.
[38] A.I. Rodríguez, B.G. Riaza, M.C.S. Gómez, Collaborative learning and mobile devices: An educational experience in Primary Education, Comput. Hum. Behav. 72 (2017) 664–677.
[39] D.H. Schunk, Learning Theories an Educational Perspective, sixth ed., Pearson, 2012.
[40] J.P. Hourcade, Interaction design and children, Found. Trends Hum.-Comput. Interact. 1 (4) (2008) 277–392.
[41] P.-C. Chen, M.-W. Hung, H.-S. Lu, C.W. Yuan, N. Bi, W.-C. Lee, M.-C. Huang, C.-W. You, This app is not for me: Using mobile and wearable technologies to improve adolescents' smartphone addiction through the sharing of personal data with parents, in: CHI Conference on Human Factors in Computing Systems, 2022, pp. 1–15.
[42] M. Akter, A.J. Godfrey, J. Kropczynski, H.R. Lipford, P.J. Wisniewski, From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals? Proc. ACM Hum.-Comput. Interact. 6 (CSCW1) (2022) 1–28.
[43] Y. Hashish, A. Bunt, J.E. Young, Involving children in content control: a collaborative and education-oriented content filtering approach, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2014, pp. 1797–1806.
[44] Y. Hendrawan, A maze game on android using growing tree method, in: Journal of Physics: Conference Series, vol. 953, IOP Publishing, 2018, 012148.
[45] W.H. Matthews, Mazes and Labyrinths: Their History and Development, Courier Corporation, 1970.
[46] B. Bontchev, A. Antonova, V. Terzieva, Y. Dankov, "Let us save venice"—An educational online maze game for climate resilience, Sustainability 14 (1) (2021) 7.
[47] B. Bontchev, R. Panayotova, Generation of educational 3D maze games for carpet handicraft in Bulgaria, Digit. Present. Preserv. Cult. Sci. Herit. 7 (2017) 41–52.
[48] V. Terzieva, B. Bontchev, Y. Dankov, E. Paunova-Hubenova, How to tailor educational maze games: The student's preferences, Sustainability 14 (11) (2022) 6794.
[49] J. Zhao, G. Wang, C. Dally, P. Slovak, J. Edbrooke-Childs, M. Van Kleek, N. Shadbolt, I make up a silly name' understanding children's perception of privacy risks online, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019, pp. 1–13.
[50] P. Kumar, J. Vitak, M. Chetty, T.L. Clegg, J. Yang, B. McNally, E. Bonsignore, Co-designing online privacy-related games and stories with children, in: Proceedings of the 17th ACM Conference on Interaction Design and Children, 2018, pp. 67–79.
[51] L. Zhang-Kennedy, K. Baig, S. Chiasson, Engaging children about online privacy through storytelling in an interactive comic, Electron. Visual. Arts (EVA 2017) (2017) 1–11.
[52] E. Moran, D. Warden, L. Macleod, G. Mayes, J. Gillies, Stranger-danger: What do children know? Child Abuse Rev. J. Br. Assoc. Study Prev. Child Abuse Negl. 6 (1) (1997) 11–23.
[53] Y.-Y. Choong, M.F. Theofanos, K. Renaud, S. Prior, Passwords protect my stuff — a study of children's password practices, J. Cybersecur. 5 (1) (2019) tyz015.
[54] S. Prior, K. Renaud, Age-appropriate password "best practice" ontologies for early educators and parents, Int. J. Child-Comput. Interact. 23 (2020) 100169.
[55] K. Duncan, H. Nikels, M. Aurand, G. Bardhoshi, Helping kids and families stay safe: Workshops on cyberbullying and on-line safety, in: VISTA 2008 Online, 2008.
[56] F. Quayyum, Supplementary data for cyberfamily, Mendeley Data, V1, 2023. http://dx.doi.org/10.17632/9zdxpy7vnt.1. URL https://data.mendeley.com/datasets/9zdxpy7vnt/1.
[57] A. Druin, The role of children in the design of new technology, Behav. Inf. Technol. 21 (1) (2002) 1–25.
[58] D.W. Stewart, P.N. Shamdasani, Focus Groups: Theory and Practice, vol. 20, Sage publications, 2014.
[59] J. Rubin, D. Chisnell, Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests, John Wiley & Sons, 2008.
[60] D.S. Cruzes, T. Dyba, Recommended steps for thematic synthesis in software engineering, in: 2011 International Symposium on Empirical Software Engineering and Measurement, 2011, pp. 275–284, http://dx.doi.org/10.1109/ESEM.2011.36.
[61] B.F.J. Manly, Multivariate Statistical Methods: A Primer, Chapman & Hall/CRC, 1994.
[62] Ş. Tan, Misuses of KR-20 and Cronbach's alpha reliability coefficients, Educ. Sci. 34 (152) (2009).
[63] S.O. Ekolu, H. Quainoo, Reliability of assessments in engineering education using Cronbach's alpha, KR and split-half methods, Global J. Eng. Educ. 21 (1) (2019) 24–29.
[64] N. Ahmad, U. Asma'Mokhtar, W.F.P. Fauzi, Z.A. Othman, Y.H. Yeop, S.N.H.S. Abdullah, Cyber security situational awareness among parents, in: 2018 Cyber Resilience Conference, Crc, IEEE, 2018, pp. 1–3.
[65] J. Robertson, C. Howells, Computer game design: Opportunities for successful learning, Comput. Educ. 50 (2) (2008) 559–578.
[66] G. Sim, B. Cassidy, J.C. Read, Understanding the fidelity effect when evaluating games with children, in: Proceedings of the 12th International Conference on Interaction Design and Children, 2013, pp. 193–200.