Collaboration between parents and children to raise cybersecurity awareness

Farzana Quayyum
farzana.quayyum@ntnu.no
Norwegian University of Science and Technology
Trondheim, Norway

ABSTRACT

In the early years of children's lives, parents and caregivers greatly influence children's device use and access to online activities. Children's learning and online behavior typically start to develop based on their experiences within the family environment. In this paper, we highlight the significant role of parents and the importance of parent–child collaboration in cybersecurity education. We also briefly present our ongoing efforts to improve parent–child collaboration in cybersecurity education through a game-based learning approach. When crafting solutions to increase children's cybersecurity awareness, future researchers and designers should take into account and ensure an active and engaging role for parents that goes beyond merely monitoring and regulating children's online access and activities.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**.

KEYWORDS

Cybersecurity awareness, parent–child collaboration, game-based learning, parents, children

ACM Reference Format:
Farzana Quayyum. 2023. Collaboration between parents and children to raise cybersecurity awareness. In *European Interdisciplinary Cybersecurity Conference (EICC 2023), June 14–15, 2023, Stavanger, Norway*. ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3590777.3590802

1 CYBERSECURITY AWARENESS AND CHILDREN

The importance of developing digital skills among children is recognized by many countries and reflected in school curricula worldwide. Developing digital skills leads children to use the internet, online services like email, and a wide range of online software. They use the internet for education, entertainment, and communication. While online, children encounter a significant number of opportunities and risks. However, they are less likely to understand the overall risks, the ramifications of disclosing their personal information, and the implications of their actions on their own or others' lives [9]. Thus, children need help to use the internet safely and to learn about the possible risks and consequences.

Children's cybersecurity awareness research is currently receiving significant attention from both industry and the scholarly community. Research shows that children are also vulnerable to many risks in the digital world [24, 26]. Privacy violations, password security, stranger dangers, cyberbullying, phishing, targeted marketing, exposure to inappropriate content, identity theft, and financial scams are just some examples of these risks [24]. Researchers have designed and proposed various tools for teaching children about cybersecurity, in addition to investigating the relevant risks for children and how they are affected by those risks [24, 31].

While proposing techniques for raising cybersecurity awareness and developing tools such as games or mobile applications for children, most existing research focuses on children alone (for example, [3, 15, 30]). Especially when designing educational games for children, we often see children as the only user group in the game (for example, [5, 15]). Thus, adults usually do not participate in the game itself in any meaningful way. Very few existing resources (including [2, 18]) actively involve the parents or caregivers in the game or media. Adults are mainly expected to facilitate, control, or monitor children's access and activities [22]. However, because children do not have the same maturity and cognitive ability as adults, it might be difficult for them to learn alone and develop the required abilities to grasp internet safety and threats without sufficient engagement and guidance from adults. In most existing research that proposes or applies a game-based learning strategy, parents are insufficiently involved, despite their significant impact on their children's internet activity and online behavior.

At the same time, it may be difficult for many parents to keep up with the rapid technological progress and maintain the same digital competence and speed as their children [11, 23]. Today's children have been born and raised in a digital environment and are surrounded by any number of advanced technology and devices in practically every aspect of their lives. However, this is not the case for adults born 30 or 40 years ago. As a result, it is essential that parents and children collaborate to help one another with knowledge and skills related to online security.

In our study, we address this need by designing a collaborative cybersecurity awareness game for children and parents. Our study aims to increase children's cybersecurity knowledge and awareness in a playful and engaging manner by using game-based learning and to involve parents in this process to improve familial communication and parental understanding of children's internet use and cybersecurity. Along with increasing children's awareness, encouraging dialogue between parents and children will help parents

EICC 2023, June 14–15, 2023, Stavanger, Norway

ACM ISBN 978-1-4503-9829-9/23/06.
https://doi.org/10.1145/3590777.3590802

to enhance their knowledge about recent technologies and online security topics.

2 WHY DO WE NEED PARENT–CHILD COLLABORATION?

Schools and families play an essential role in helping children learn about online etiquette, cybersecurity, and the risks linked with virtual platforms. Lester et al. [17] demonstrated that involving families in school efforts to prevent and manage bullying behavior can help reduce children's bullying behavior and positively impact parent–child communication about bullying. In the early years of children's lives, they start learning at home with the help of parents or caregivers, long before they go to school. Thus, it is critical that parental guidance and home-based learning about cybersecurity begin as soon as children start using smartphones or tablets for entertainment. More cybersecurity education and digital skill development can be provided in schools once children have a basic understanding of how to use the internet and online services.

Parental privacy concerns and mediation techniques can impact children's internet use and online privacy practices [29]. Research also shows that security risks such as children's privacy violations can be (unwittingly) perpetrated by their parents or relatives [20]. Therefore, parents themselves may not be sufficiently knowledgeable about internet use and cybersecurity issues to provide their children with the necessary guidance [11] and need additional support and resources to keep their children safe online [10].

We believe collaboration between parents and children can make this endeavor more effective and beneficial, as they need the same knowledge and abilities. Engaging parents in learning activities with children (such as reading books and using computers for education) supports the growth of children's cognitive abilities [16]. The success of one participant aids the achievement of other participants in collaborative learning because individuals are accountable for both their own learning and that of their peers [13]. Hence, having acknowledged the benefit and value of parent–child collaboration, researchers have begun looking into ways to improve that collaboration, as in technology use [8] and jointly managing parental control tools [1, 14]. These existing studies have demonstrated the value of involving parents in raising children's awareness and shaping their behavior.

When it comes to children's cybersecurity awareness and the role of parents and caregivers, researchers have largely studied adults' perceptions (for example, [23, 27]) and concerns about children's cybersecurity knowledge and awareness (for example, [4, 19, 21]). Although all these studies on cybersecurity awareness training emphasize parental and caregiver involvement, we have not come across any that use a game-based learning strategy to encourage parent–child collaboration in cybersecurity awareness learning. As primary caregivers, parents are generally expected to play an active role in ensuring their children's internet safety and privacy, particularly for children under 13. Adopting such a mediating position for the parents can be difficult and delicate [23] because building that kind of parent–child relationship requires understanding and communication. However, when holding parents primarily responsible for mediating children's online interactions, we sometimes overlook the importance of providing meaningful opportunities for parents to engage in their children's online interactions when designing digital solutions for children [22, 25].

3 THE PROSPECT OF GAME-BASED LEARNING

According to Zhang-Kennedy and Chiasson [31], digital games are one of the most widely used tools to raise cybersecurity awareness. Using games for educational purposes is now very popular, regardless of target user age. When education becomes fun and attractive, children become more motivated and interested in learning. Several studies on this issue have been carried out and many cybersecurity-based gaming applications developed in the last few years to educate users (for example, [3, 5, 12, 30]). Most of those studies report positive results and impacts on users in employing game-based learning and games as cybersecurity education tools. These applications and games seek to teach users about various cybersecurity issues and risks like privacy, phishing, password hygiene, and malware.

Since game-based learning has been shown to be beneficial for both adults and children, using this method to increase parent–child cooperation and raise cybersecurity awareness has significant potential. As noted above, researchers who have explored ways to increase parent–child collaboration found promising results. Hence, we believe that combining this perspective on collaboration with game-based learning techniques is worth exploring in future research.

4 OUR ONGOING EFFORTS

Recognizing the importance of parent–child collaboration and the value of games as learning tools, we are in the midst of designing and testing a collaborative family game for cybersecurity awareness. Our aim is to help parents and children learn about cybersecurity topics and facilitate dialogue and collaboration between parents and children on these subjects.

4.1 The game

Our proposed game, "CyberFamily," is a two-player maze game that parents and children will play together (Figure 1). Puzzle games like mazes are widely acknowledged for teaching players patience, persistence, critical thinking, and problem-solving techniques. Inspired by existing studies [6, 7, 28] that use maze games for educational purposes, we have used this game genre in our study for cybersecurity awareness and education. We have also included other game components, such as challenges and questions, in our proposed game. The game consists of the following steps.

(1) The players take turns playing.
(2) Player 1 (either parent or child) enters the maze from one point and advances first.
(3) When Player 1 reaches a challenge, he or she picks up a challenge card and answers the questions on that card.
(4) After Player 1 responds to the first challenge, Player 2 begins the game from a different entry point.
(5) When one player engages in play, the other player will pause and watch until that player has responded to a challenge.
(6) Player 1 will continue moving through the maze once Player 2 has responded to one challenge.

(7) The game continues until both players arrive at the endpoint of the maze.
(8) At any point during the game, the players can interact and help each other answer the challenges.

The players will encounter challenges in the form of questions as they advance through the maze. To design these challenges, we combined a quiz-style design with storytelling. Each challenge will present a cybersecurity-related scenario and ask the player to answer questions related to that scenario. In order to keep moving, players need to answer these questions. Before arriving at the destination, each player must complete five challenges by answering the questions correctly. The children's challenges focus on how much they understand the risks presented in the scenarios and how they would act in a similar situation. Meanwhile, the parent-specific challenges are more concerned with parents' perspectives and how they would respond in similar circumstances involving their children.

4.2 Initial findings

We have already conducted a pilot study with four pairs of parents and children to test the feasibility of the game using a low-fidelity paper prototype. Children aged 9 to 12 and their parents are the game's intended demographic. In the pilot study, the parent–child pairs played the game and participated in focus group discussions. It is important to note that, during the pilot study with this initial version of the game prototype, we aimed to promote discussion and dialogues among the parents and children; thus, we did not introduce a rule for the game on whether the payers need to answer the questions correctly or not. We allowed the parents and children to discuss the questions and help each other with the correct answer. In the focus groups, we asked the parents and children about their experiences of the game and their opinions about it. Our preliminary findings suggest promising outcomes. The game's concept was well received by both parents and children, who offered helpful feedback. In this study, we mainly tested the feasibility of the game idea to see how the participants reacted to the idea of a collaborative game for parents and children. However, we did not perform a thorough evaluation of the game and its learning impact at this stage.

4.3 Future works

We are now working on further developing the game. The user interface of the game will be improved in the next stage to make it more appealing to children. We are also aiming to improve the game's challenges and introduce new ones. Furthermore, as noted above, the primary goal of our pilot research was to assess the overall feasibility of the game. We intend to carry out additional user trials with a larger group of participants to evaluate the game's learning impact and viability. The next stage will be an experiment to test the following hypotheses:

H1. A collaborative family game can facilitate collaborative learning between parents and children.

H2. The collaborative aspect of a game can create an environment for dialogue between parents and children.

H3. A collaborative family game on cybersecurity can be engaging for both parents and children.

Our next experiment will test these hypotheses by determining whether the game can in fact teach parents and children about cybersecurity. It is reasonable to assume that parents are more knowledgeable about and aware of the risks involved with online activity, but it will be both intriguing and important to observe whether the game and the attendant interaction with children can teach parents anything new. We also want to assess whether and how the game encourages conversations between children and their parents, in addition to assessing the learning impact. Finally, we want to see if the proposed collaborative family game can be entertaining and engaging for both parents and children.

The target audience of this study will be the same as our pilot study; that is, children aged 9 to 12 and their parents. The participants will be recruited through a local technology club for children. Children participate in various activities at this club, including robotics competitions and Lego leagues at the national and international levels. This club is a voluntary organization run primarily by parents of the participating children; it currently has 11 children who regularly take part in its activities, while some other children participate occasionally.

5 CONCLUSION

In this paper, we seek to emphasize the value of parent–child collaboration in educating both parents and children about cybersecurity. We argue that while developing cybersecurity education tools and solutions for children, future researchers need to think more about the role of parents and the importance of their involvement. Our efforts to ensure that children are safe online will be more successful if we give parents a chance to get involved and give them a proactive role in interacting.

However, it is also worth noting that children need to develop independence, the ability to think critically, and the capacity for autonomous decision-making. Parental involvement in the educational process must be carefully balanced and must not impair children's cognitive growth. We argue that parents should start educating children about internet safety and use at home as soon as children are exposed to devices and the internet so that, as they grow up and start using devices and online services on their own, young people will be able to recognize security concerns and take appropriate action. In addition, the collaboration between parents and children should give children the self-assurance to share both positive and negative internet experiences with their parents and ask for assistance, if necessary.

REFERENCES

[1] Mamtaj Akter, Amy J Godfrey, Jess Kropczynski, Heather R Lipford, and Pamela J Wisniewski. 2022. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (2022), 1–28.
[2] Johann Allers, Günther R Drevin, Dirk P Snyman, Hennie A Kruger, and Lynette Drevin. 2021. Children's awareness of digital wellness: a serious games approach. In *Information Security Education for Cyber Resilience: 14th IFIP WG 11.8 World Conference, WISE 2021, Virtual Event, June 22–24, 2021, Proceedings 14*. Springer, 95–110.
[3] Faisal Alotaibi, Steven Furnell, Ingo Stengel, and Maria Papadaki. 2016. A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res.(IJISR)* 6, 2 (2016), 660–666.
[4] Fernanda Maria Pinheiro Amâncio, Ana Paula Souza, Marcelo Fantinato, Sarajane Marques Peres, Patrick CK Hung, Luis Gustavo Coutinho do Rêgo, and Jorge Roa. 2023. Parental perception of children's privacy in smart toys in countries of different economic levels. *Technology in Society* 72 (2023), 102180.

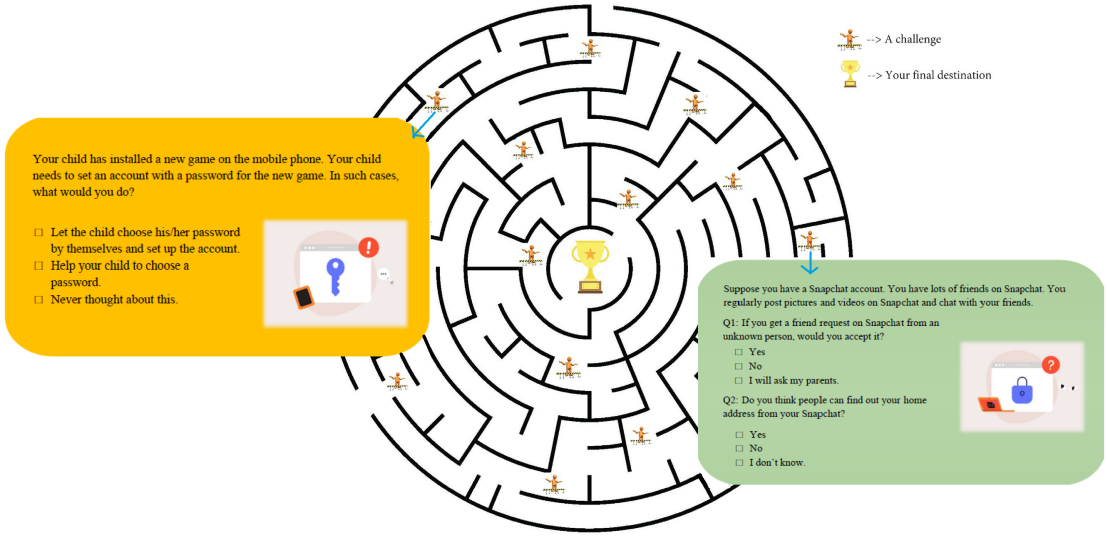

Figure 1: The maze game and examples of the challenges (Yellow cards for parents and green cards for children)

[5] Ovidiu-Gabriel Baciu-Ureche, Carlie Sleeman, William C Moody, and Suzanne J Matthews. 2019. 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*. 118–123.

[6] Boyan Bontchev, Albena Antonova, Valentina Terzieva, and Yavor Dankov. 2021. "Let Us Save Venice"—An Educational Online Maze Game for Climate Resilience. *Sustainability* 14, 1 (2021), 7.

[7] Boyan Bontchev and Radina Panayotova. 2017. Generation of Educational 3D Maze Games for Carpet Handicraft in Bulgaria. *Digital Presentation and Preservation of Cultural and Scientific Heritage* 7 (2017), 41–52.

[8] Pin-Chieh Chen, Min-Wei Hung, Hsueh-Sung Lu, Chien Wen Yuan, Nanyi Bi, Wan-Chen Lee, Ming-Chyi Huang, and Chuang-Wen You. 2022. 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*. 1–15.

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

[10] Lenka Dedkova, David Smahel, and Mike Just. 2022. Digital security in families: The sources of information relate to the active mediation of internet safety and parental internet skills. *Behaviour & Information Technology* 41, 5 (2022), 1052–1064.

[11] Khairi Ghet Elghadafi Elgharnah and Fezile Ozdamli. 2020. Determining Parents' Level of Awareness about Safe Internet Use. *World Journal on Educational Technology: Current Issues* 12, 4 (2020), 290–300.

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

[13] Anuradha Gokhale. 1995. Collaborative learning enhances critical thinking. *Journal of Technology education* 7, 1 (1995).

[14] Yasmeen Hashish, Andrea Bunt, and James E Young. 2014. 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*. 1797–1806.

[15] Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. 2017. How effective is anti-phishing training for children. In *Symposium on Usable Privacy and Security (SOUPS)*. 229–239.

[16] Alexis R Lauricella, Rachel Barr, and Sandra L Calvert. 2014. Parent–child interactions during traditional and computer storybook reading for children's comprehension: Implications for electronic storybook design. *International Journal of Child-Computer Interaction* 2, 1 (2014), 17–25.

[17] Leanne Lester, Natasha Pearce, Stacey Waters, Amy Barnes, Shelley Beatty, and Donna Cross. 2017. Family involvement in a whole-school bullying intervention: Mothers' and fathers' communication and influence with children. *Journal of Child and Family Studies* 26 (2017), 2716–2727.

[18] Sana Maqsood and Sonia Chiasson. 2021. Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. *ACM Transactions on Privacy and Security (TOPS)* 24, 4 (2021), 1–37.

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

[20] Tehila Minkus, Kelvin Liu, and Keith W Ross. 2015. Children seen but not heard: When parents compromise children's online privacy. In *Proceedings of the 24th international conference on World Wide Web*. 776–786.

[21] Kate Muir and Adam Joinson. 2020. An exploratory study into the negotiation of cyber-security within the family home. *Frontiers in psychology* 11 (2020), 424.

[22] Marije Nouwen and Bieke Zaman. 2018. Redefining the role of parents in young children's online interactions. A value-sensitive design case study. *International Journal of Child-Computer Interaction* 18 (2018), 22–26.

[23] Farzana Quayyum, Jonas Bueie, Daniela S Cruzes, Letizia Jaccheri, and Juan Carlos Torrado Vidal. 2021. Understanding parents' perceptions of children's cybersecurity awareness in Norway. In *Proceedings of the Conference on Information Technology for Social Good*. 236–241.

[24] Farzana Quayyum, Daniela S Cruzes, and Letizia Jaccheri. 2021. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction* 30 (2021), 100343.

[25] Nur W Rahayu and Sri Haningsih. 2021. Digital parenting competence of mother as informal educator is not inline with internet access. *International Journal of Child-Computer Interaction* 29 (2021), 100291.

[26] Valdemar Švábenskỳ, Jan Vykopal, and Pavel Čeleda. 2020. 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*. 2–8.

[27] Faiza Tazi, Sunny Shrestha, Dan Norton, Kathryn Walsh, and Sanchari Das. 2021. 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*. 1–5.

[28] Valentina Terzieva, Boyan Bontchev, Yavor Dankov, and Elena Paunova-Hubenova. 2022. How to Tailor Educational Maze Games: The Student's Preferences. *Sustainability* 14, 11 (2022), 6794.

[29] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. " Preventative" vs." Reactive" How Parental Mediation Influences Teens' Social Media Privacy Behaviors. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. 302–316.

[30] Leah Zhang-Kennedy, Khadija Baig, and Sonia Chiasson. 2017. Engaging children about online privacy through storytelling in an interactive comic. *Electronic Visualisation and the Arts (EVA 2017)* (2017), 1–11.

[31] Leah Zhang-Kennedy and Sonia Chiasson. 2021. A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)* 54, 1 (2021), 1–39.