Understanding parents' perceptions of children's cybersecurity awareness in Norway

FARZANA QUAYYUM*, JONAS BUEIE, DANIELA S. CRUZES, LETIZIA JACCHERI, and JUAN CARLOS TORRADO VIDAL, Norwegian University of Science and Technology (NTNU), Norway

Children are increasingly using the internet nowadays. While internet use exposes children to various privacy and security risks, few studies examine how parents perceive and address their children's cybersecurity concerns. To address this gap, we have conducted a qualitative study with twenty-five parents living in Norway with children aged between 10 to 15. We have conducted semi-structured interviews with the parents and performed a thematic analysis with the interview data. Results of this paper include a list of cybersecurity awareness needs for children from a parent perspective; a list of learning sources for children; and a list of challenges for parents to ensure cybersecurity at home. Our results are useful for developers and educators to develop solutions for cybersecurity for children. Future research should focus on defining cybersecurity theories and practices that contribute to children's and parents' awareness about risks, needs, and solutions.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**.

Additional Key Words and Phrases: Cybersecurity, Cybersecurity awareness, Children, Parents.

ACM Reference Format:
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. 1, 1 (June 2021), 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Children are becoming more and more global citizens who use the internet daily and spend numerous hours on the internet for education, entertainment, and communication. While online, children meet a significant number of opportunities that unlock the potential of individuals, technology, and collaboration to create a positive societal impact[1]. Children, while online, meet risks as well. Thus, children must learn to use computers and the internet in a safe and secure manner that is both effective and efficient[2]. However, sometimes, children are not aware of the cybersecurity risks they may get exposed to over the internet. International Telecommunication Union (ITU) defines cybersecurity as "... the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets[3]". Cybersecurity awareness is defined "as a methodology to educate internet users to be sensitive to the various cyber threats, and the vulnerability of computers and data to these threats" [Abd Rahim et al. 2015]. Without cybersecurity awareness, children are less likely to understand the risks and the future implications of their actions on their or others' lives [Clemons and Wilson 2015]. Thus, adults, especially parents, have a responsibility to help children to use the internet safely and make them aware of the cybersecurity risks and consequences.

Parents recognize the importance of their role as the mediators of their children's technology use and online security [Moreno et al. 2013]. Parents control the resources available to the children and manage the environment to protect children from any harmful social influences, including potential negative effects of adolescents' internet use [Livingstone and Helsper 2008; Shin and Kang 2016]. Considering the big role parents can play in children's cybersecurity awareness, it is essential to know what parents think about their children's cybersecurity. Researchers have studied different parenting styles, and the role of parents in shaping children's online behavior and safety [Rode 2009; Valcke et al. 2010].

However, little discussion has focused on the parent's perceptions about their children's cybersecurity awareness needs. Managing technology use within the family home is an evolving and dynamic endeavor changing with time, presenting new concerns and challenges for the parents. Moreover, this evolvement can be dynamic around the world when influenced by culture. Demographic changes, culture, socioeconomic status may also impact the socially structured patterns of parenting [Elstad and Stefansen 2014].

In our study, we recognize parents as important stakeholders in raising cybersecurity awareness among children. We have investigated parents' cybersecurity concerns, the awareness needs for children, and the challenges for parents in the context of Norway. We have addressed the following research questions.
RQ1. What are the cybersecurity awareness needs for children?
RQ2. How much the children currently know about cybersecurity and from which sources they learn?
RQ3. What are the challenges to ensure cybersecurity at home?

To answer our research questions, we have conducted semi-structured interviews with parents. We have presented the findings in terms of children's awareness needs, learning sources, and challenges for parents.

*Corresponding author
[1]What is Social Good?. https://www.socialchangecentral.com/what-is-social-good
[2]Informatics and Digital Skills. https://www.informaticsforall.org/informatics-digital-skills/

Authors' address: Farzana Quayyum, farzana.quayyum@ntnu.no; Jonas Bueie, jonasbue@stud.ntnu.no; Daniela S. Cruzes, daniela.s.cruzes@ntnu.no; Letizia Jaccheri, letizia.jaccheri@ntnu.no; Juan Carlos Torrado Vidal, Juancarlos.Torrado@uib.no, Norwegian University of Science and Technology (NTNU), Trondheim, Norway.

XXXX-XXXX/2021/6-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

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

The structure of the paper is as follows: Section 2 introduces related studies about cybersecurity awareness for children with a focus on the role of parents. Section 3 explains the research method, data collection, and analysis, as well as the ethical issues. Results are presented in Section 4 organized around the three research questions. Section 5 discusses the finding of this research and Section 6 concludes the paper.

2 BACKGROUND

Awareness of cybersecurity is vital for children to cope with the safe use of the internet and emerging technologies. In recent years, children's cybersecurity has gathered much attention both from academia and from the industry. Researchers have proposed and designed various training programs and games for children that can help them to raise awareness on cybersecurity. For example, [Bioglio et al. 2019] has developed a serious game for primary and secondary school children to enhance user perception and awareness of privacy on social networks. [Prior and Renaud 2020] has developed an ontology of "best practice" password principles for children depending on the age. With this ontology, educators and parents will be able to guide children about the password-related principles, what password principles young children should know, and at what age this information should be imparted. Many other studies have also worked on raising cybersecurity awareness among children, including [Baciu-Ureche et al. 2019; Lastdrager et al. 2017; Zhang-Kennedy et al. 2017].

Many researchers have explored other topics related to cybersecurity for children. For example, [Moreno et al. 2013] has explored the perspectives of different stakeholders about internet safety education for children. Research studies have been carried out exploring the role and involvement of parents in ensuring children's security online [Shin and Kang 2016; Wisniewski et al. 2015, 2017b]. Studies have investigated how families manage and negotiate cybersecurity within the home [Muir and Joinson 2020]; family preferences concerning children's online privacy and data mining [Clemons and Wilson 2015]. Some researchers have also investigated the mediation strategies parents use to mediate their children's online risk exposure [Kumar et al. 2017; Muir and Joinson 2020; Rode 2009]. Overall, it is evident that parents can play a significant role in children's online behavior and awareness. However, most of these prior studies have focused on children and have not discussed or reflected upon parents' views and concerns regarding children's cybersecurity awareness.

Research studies have shown that different parenting styles can influence children's behavior [Clausen 1996; Shin and Kang 2016; Wisniewski et al. 2015]; and the effects of different parenting styles on children have been shown to vary within, and across culture [Bornstein et al. 2011]. In addition, parenting styles and parenting attributes differ from country to country, and studies have shown that Scandinavian parents are usually less authoritative towards their children [Bornstein et al. 2011]. Our study extends related work by understanding parents' perceptions of children's cybersecurity awareness in a Scandinavian country (i.e., Norway). To the best of our knowledge, we have not found any study investigating parents' perspectives about children's cybersecurity in the context of Norway. Therefore, build on this work by exploring children's cybersecurity awareness needs from their parents' perspectives. We also explore how children learn about cybersecurity and if the parents face any challenges in ensuring cybersecurity at home.

3 METHODS

We have conducted semi-structured interviews with twenty-five parents (who have children aged between 10 to 15 years) to examine our research questions. We have used semi-structured interviews so that our interviewees can speak in more detail on the issues we ask and also can introduce issues of their own that they think relevant to our themes. We have performed a thematic analysis of the interview data, following the recommended steps proposed by [Cruzes and Dybå 2011]. We took an integrated approach to the analyzing process. We approached the data with specific questions (the research questions) in mind that we wished to code according to; on the other hand, we also related to the interviewees' concepts. The codes were examined and grouped into broader, predominately descriptive themes (i.e., they described patterns in the data relevant to the research questions). To identify the interview questions, we have used the Goal Question Metric (GQM) approach proposed by [Basili et al. 1994]. Our study's goal was to have a clear understanding of parents' perception of children's cybersecurity. Thus, our interview questions emphasized parents' opinions and concerns about children's cybersecurity, their own experiences at the family, and the underlying processes of ensuring children's cybersecurity, such as understanding the strategies they use at home and related challenges. The interviews were conducted between July to August 2020. All the interviews have been audio-recorded, and the interview subjects were explicitly asked to give consent in advance of the interview. Most of the consents were given in writing, but some consents were given orally as well before starting the interviews.

To find the interview subjects, we adapted the self-selection and snowball strategy. We contacted a list of people our research team members knew, with children in the correct age group. We advertised about our research to them and asked if they want to participate in our interviews. To include a more versatile sample, we did not consider any specific gender, profession, or educational backgrounds of the parents. We interviewed the individuals who agreed to participate in the research. Some of the interview subjects also provided contact details of other people they knew who might be interested in taking part in this study. We contacted the potential interview subjects by e-mail or SMS and invited them for the interviews. Finally, we interviewed 25 parents. Three interviews were conducted face-to-face, and the rest of the interviews were conducted either online (using Microsoft Teams, Zoom, or FaceTime) or over mobile phones. The duration of each of the interviews varied from 10 minutes to 34 minutes. The participants included eight fathers and 17 mothers, and the age range varied from 38 to 56 years old. The parents who participated in the interviews have 26 children (in our target age group), age ranging from 10 to 15 years (6 girls and 20 boys).

Before starting the data collection process, this study applied for approval from the Norwegian center for research data (NSD)[4].

[4]https://www.nsd.no/en/about-nsd-norwegian-centre-for-research-data/

Moreover, during the interviews, the interviewer reminded the participants to avoid mentioning any personal information about any third person (names or identity).

4 RESULTS

This section presents the results of this study, organized around the research questions.

4.1 RQ1. What are the cybersecurity awareness needs for children?

In the interviews, we asked parents about the security concerns they have for their children when they are online. We also asked them about their opinions on what kind of awareness children need to stay safe online. Thus, based on the parents' opinions, we have identified some needs that parents believe children should have to stay safe online and presented in Figure 1.

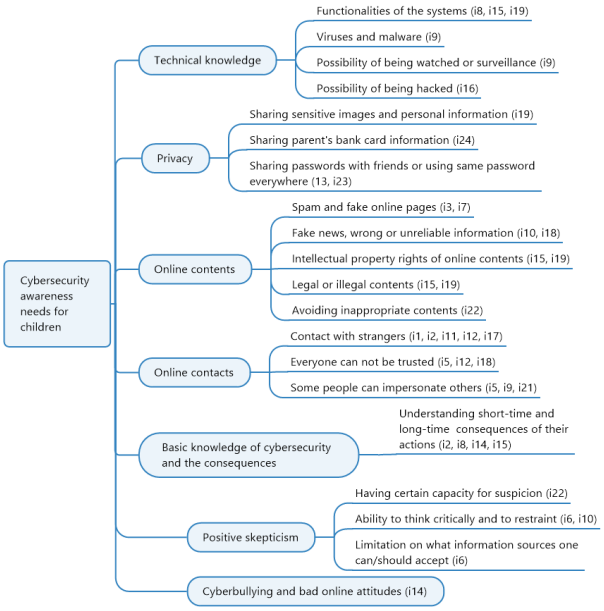

Fig. 1. Cybersecurity awareness needs for children (from parent's perspectives)

The parents expressed that children need both awareness and some behavioral attributes to stay safe online. They believe children should know and understand the technology they use, for example - how the system works, how the information is flowing in the system and what information is being stored, etc. Children also need to know about viruses and malware; the quality, reliability, and the legal aspects of the contents they see on the internet and use; what contact they have online; and a good understanding of their privacy. When we asked the parents about what kind of awareness they think children need when they use the internet, one parent stated that,

"It's both fundamental to understand how things are stored and how systems work, and of course both storage and sharing. It also concerns laws and regulations, i.e. what is actually legal and illegal. (i15)

Along with awareness, parents believe children should also have some behavioral attributes, for example, having some skepticism before they accept and believe any information from the internet, ability to think critically and restrain from acting if something does not feel right. Children also need to be aware of their attitudes when they post or comment on anything online; they should be aware of avoiding behaviors that can result in bullying someone, and children also need to think about the consequences of their actions before they act. One parent stated about the needs as below.
"Critical sense of what is there, and that you should not press 'yes' and 'ok' on everything." (i10)

4.2 RQ2. How much the children currently know about cybersecurity, and from which sources they learn?

Parents of younger children reported that their children have some basic awareness about cybersecurity. However, the adolescents' parents reported that their children know quite a bit about cybersecurity and the risks. Children are learning about cybersecurity both from home and school. Children get training on security topics such as sharing personal information with others, good password practices, how to handle bullying problems, sexual abuse, use of social media, etc., from schools.

4.2.1 Discussing cybersecurity at home. The majority of the parents (15/25) have explicitly mentioned that they talk about online security issues with their children at home. They discuss it from their experiences or when any cybersecurity case appears in the media; they try to make the children understand what has happened to others and what could happen to them, and what they can do if something happens. Thus, parents try to teach and increase their children's awareness about the risks and the consequences through conversations. Some parents have mentioned that they also show interest and engage in their kids' online activities; this way, they can both monitor what the children are doing online and also get the opportunity to discuss the security issues.

4.2.2 Cybersecurity awareness from schools. It is evident that the schools in Norway are playing an important role in creating cybersecurity awareness among the children. Cybersecurity is not formally included in the school curriculum as a subject, but the schools arrange awareness programs on different security topics. To prepare and conduct these programs, the schools coordinate with other organizations that work to raise cybersecurity awareness among children. From the interviews, we have known about three such organizations that the schools are working with to arrange training programs on cybersecurity and online etiquette; the organizations are Barnevakten[5], Bruk Hue[6], and Medietilsynet[7]. These organizations help the schools by providing training and lectures (both for students and teachers), preparing content for training, and organizing parents' meetings to discuss cybersecurity topics

[5]https://www.barnevakten.no/
[6]https://brukhue.no/
[7]https://medietilsynet.no/

with the parents and raise parental awareness. All the parents in our study have provided positive feedback for these training programs and appreciated the schools' initiatives in raising children's cybersecurity awareness.

4.3 RQ3. What are the challenges for parents to ensure cybersecurity at home?

Throughout the interviews, all the parents spontaneously discussed their feelings about the challenges in ensuring security for their children's online activities. We have grouped and categorized all the challenges based on their focus: keeping control, limitation of knowledge, understanding the risks, limitation of parental control tools, and balancing between trust and control (see Fig. 2).

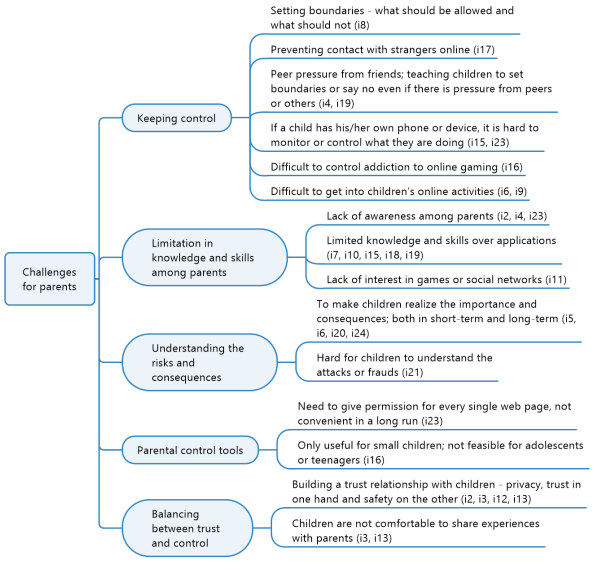

Fig. 2. Challenges mentioned by the parents in ensuring cybersecurity at home

Overall, all the parents in our study have mentioned facing challenges in ensuring their children's security online. Nine out of twenty-five parents have commented that they find it difficult to control their kids' online activities (for example, contacting a stranger). Parents have mentioned some reasons that make controlling children difficult for them. These reasons include personal devices of the children, peer pressure from classmates or friends (of children), the easy and open nature of some software (for example, online games) that allow users to contact others without restriction. The second most common challenge is the lack of knowledge and skills among the parents. Nine out of twenty-five parents have mentioned that they lack the necessary knowledge and skills themselves to protect their children from online risks.

The majority of the parents (18/25 parents) in our study have mentioned using parental control, mostly the default parental control features provided by the devices. However, two of the parents have expressed having challenges related to the parental control systems. These challenges are related to the system's feasibility for older children (the teenagers) and their functionality. The parents are using parental control mostly to limit the screen time, limit access to different websites, and limit download opportunities.

5 DISCUSSION

In this section, we discuss the main findings from our research in relation to the research questions of this study.

5.1 Cybersecurity awareness needs for children

As gatekeepers of children's use of technology and the internet, all the parents we interviewed have concerns for their children's safety online. Parents are aware that children can still be at risk without proper awareness despite such strategies. Parents discussed their concerns about cybersecurity risks like privacy, cyberbullying, stranger danger (like impersonation and grooming), online content, technical threats (like hacking, malware, and viruses).

However, here it is interesting to see that some parents have expressed some awareness needs for the children, which we have not seen being mentioned or studied much in the literature. For example, three parents have said that children should understand the systems when they use them. Children should understand how the system works, the systems' functionalities, how the information flows in the system, which information the system collects from the users, how the data is stored, etc. Parents believe that understanding or knowing the system will help the children to use the systems in a more secure and mature way. We suggest children's software and interaction designers consider this thought when designing products or services for children. Providing the privacy policy in a child-friendly way, simplified user guidelines, and instruction notes either inside the system or as a separate user manual can help the children to have a more clear understanding of the system.

Another interesting finding is some specific concerns about online content. While in the literature we have seen researchers mostly focusing on issues like pornography [Ahmad et al. 2019; Maoneke et al. 2018; Wisniewski et al. 2017b], age-inappropriate contents [Kritzinger 2015; Muir and Joinson 2020; Zhao et al. 2019], and spam [Giannakas et al. 2016; Martin et al. 2018], here some parents (7/25 parents) mentioned that children also need awareness about reliability and credibility of online contents; fake or real, intellectual property rights, what is legal and what is illegal with the online contents. Some parents have expressed their concerns about how online contents can affect children with a bad and negative influence.

Additionally, some parents (3/25 parents) have also pointed out the need for positive skepticism in children. It is about the awareness that children need a certain capacity for suspicion if something unusual happens online. Having this skepticism capacity can also help them think critically and restrain before pressing "OK or YES" on everything when needed. With positive skepticism, they can also limit the information sources they accept online. However, positive skepticism is not something that we can teach children directly in schools or in institutions. Rather, we as parents or adults can help them to understand what positive skepticism is and why it is a key part of critical thinking. It is also important that we help the children understand and differentiate between positive and negative

skepticism. Discussing critical thinking and positive skepticism with the children can be a good strategy here, just like discussing the cybersecurity risks and concepts.

5.2 Children's knowledge of cybersecurity and their sources of learning

Aligned with the literature [Bioglio et al. 2019; Muir and Joinson 2020; Shin and Kang 2016], in our study, we have seen both parents and teachers are playing an essential role in creating cybersecurity awareness among children in Norway. Most parents believe that their children (who are around ten years old or above) have some awareness of cybersecurity. This belief can be supported by finding from other studies as well [Kumar et al. 2017, 2018; Zhao et al. 2019]. At the same time, parents also mentioned that there is a difference between knowing it and using it or understanding it. Moreover, there is probably a lot they do not know as well. Thus, they still need more training and awareness on this topic. At home, parents try to increase children's awareness mainly by discussing the relevant security topics with them. Parents often use the cybersecurity-related cases that come from the media as examples for the discussions.

Here, it is worth discussing the initiatives from the schools. From the conversation with parents, it is evident that the schools in Norway have taken good initiatives on cybersecurity awareness for children. The schools are collaborating with organizations that have expertise in the area and trying to increase cybersecurity awareness not only among children but also among teachers and parents. Parents have mentioned multiple cybersecurity topics that their children have learned from the schools, including password practices, privacy, information sharing, contacting strangers, sexual abuse, social media, and cyberbullying. The schools are arranging meetings and seminars for parents also focused on cybersecurity, where all the parents can learn about it and share their experiences with each other. We believe such initiatives from the schools can be even more effective and extensive if collaborated with the government regulatory bodies and other stakeholders (such as the industry). These initiatives from Norwegian schools can be a good example for other countries also to develop frameworks and initiatives to raise cybersecurity awareness among children.

5.3 Challenges for parents

It is evident from previous research studies that parents can play an essential role in shaping children's online behavior and making them aware of cybersecurity [Livingstone and Helsper 2008; Shin and Kang 2016; Wisniewski et al. 2015]. Thus, it is necessary that the parents also get enough training and awareness on the topic, enabling them to help their children. If the parents get relevant training and knowledge, they will better understand the risks and consequences; and will be able to help their children more effectively and with confidence. Researchers and other stakeholders (such as the industry) can help parents with necessary training and guidelines on what to do as parents or what not to do or how to address the challenges, etc. Though Norwegian parents (like parents in other Scandinavian countries) are less authoritative and prefer modern child-rearing attitudes as shown in [Bornstein et al. 2011], still they face challenges to balance between trust and control when it comes to keeping control of their children's online activities. Regarding the challenges of keeping control, building trust-based relationships with children, balancing between trust and control, social and behavioral scientists can play a significant role here by exploring the parent-child relationship when negotiating cybersecurity within family homes.

For the last few years, using parental control is becoming more and more popular among parents. Nowadays, most devices have some form of parental controls built into their systems by default, allowing parents to restrict or control the usage and access. [Wisniewski et al. 2017a] conducted a feature analysis of 75 Android mobile apps designed to promote adolescent online safety. In their study, the researchers found that parental control apps strongly favored features that promote parental control through monitoring and restricting teens' online behaviors; rather than teen self-regulation or more communicative and collaborative practices between parents and teens. We can connect this finding from Wisniewski et al. [Wisniewski et al. 2017a] with the challenges mentioned by the parents from our study regarding the feasibility and functionality of parental control apps. Theoretically, parental control apps can be useful for children until 18 years of age. In practice, however, it is difficult for parents to control or restrict children's online usage once they become adolescents or teenagers. To solve the challenges reported by the parents, we suggest involving both parents and children in the design process before developing such parental control systems. Involving teenagers and adolescents in the design process along with parents can help designers understand the perspectives of both user groups; it will reflect the expectations of both parents and children. Involving parents and children will also increase the collaboration and communication among them, resulting in better understanding and more effective use of parental control.

5.4 Limitation and future work

This study's sample primarily includes highly educated parents. Though we did not have any criteria or requirement about the parents' educational qualification, after the interviews, it appeared that all the parents in our interviews were highly educated. This self-selection bias that accompanies interview-based research may have influenced the results of this study. Highly educated parents may be more interested and concerned about cybersecurity than less-educated parents. Future research can study perceptions of parents who have more diverse educational backgrounds and compare if there is any significant difference from the results of this study.

As our future work, we aim to develop a framework for parents to equip them with the necessary cybersecurity knowledge and skills so that they can raise cybersecurity awareness in their children. Findings from this current study will help us design and develop the framework to incorporate the parents' views and needs.

6 CONCLUSION

In this paper, we presented the results of a qualitative study to understand the perceptions of parents on cybersecurity and cybersecurity awareness needs for children. Parents in our study believe that children need knowledge and understanding about the technologies they use, privacy issues, online content, online contacts, and also

the long-term and short-term consequences of the actions. Children also need some behavioral attributes, like positive skepticism and good netiquette, to stay safe online. We recommend that future researchers take parent's opinions and concerns into consideration before developing tools and products for raising cybersecurity awareness among children.

We have found that children in Norway have some level of knowledge and awareness on cybersecurity depending on their age, and they get this knowledge and awareness from their families and from schools. Parents discuss cybersecurity topics at home frequently or occasionally, whereas the schools arrange training programs at schools in cooperation with other organizations. We also explored the challenges for parents in ensuring security for children online. Despite using different strategies, parents face various challenges in protecting their children from cybersecurity risks. We recommend that parents also need awareness, training, and guidelines on cybersecurity issues. Parents may benefit from such training and guidance on how to help children develop good privacy and security practices. This can better prepare the children to manage their cybersecurity and privacy when they start using the internet and internet-connected devices.

ACKNOWLEDGMENTS

We thank all the parents who participated in the interviews and made our research possible.

REFERENCES

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

Nazilah Ahmad, Ahmad Arifin, Umi Asma Mokhtar, Zaihosnita Hood, Sabrina Tiun, and Dian Indrayani Jambari. 2019. Parental Awareness on Cyber Threats Using Social Media. *Jurnal Komunikasi: Malaysian Journal of Communication* 35, 2 (2019), 485–498. https://doi.org/10.17576/JKMJC-2019-3502-29

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 (SIGITE '19)*. 118–123. https://doi.org/10.1145/3349266.3351399

Victor R. Basili, Gianluigi Caldiera, and H. Dieter Rombach. 1994. THE GOAL QUESTION METRIC APPROACH. *Encyclopedia of Software Engineering* (1994).

L. Bioglio, S. Capecchi, F. Peiretti, D. Sayed, A. Torasso, and R. G. Pensa. 2019. A Social Network Simulation Game to Raise Awareness of Privacy Among School Children. *IEEE Transactions on Learning Technologies* 12, 4 (2019), 456–469. https://doi.org/10.1109/TLT.2018.2881193

Marc H. Bornstein, Diane L. Putnick, and Jennifer E. Lansford. 2011. Parenting Attributions and Attitudes in Cross-Cultural Perspective. *Parenting* 11, 2-3 (2011), 214–237. https://doi.org/10.1080/15295192.2011.585568

Sten-Erik Clausen. 1996. Parenting styles and adolescent drug use behaviours. *Childhood* 3, 3 (1996), 403–414.

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. https://doi.org/10.1080/07421222.2015.1063277

Daniela. S. Cruzes and Tore Dybå. 2011. Recommended Steps for Thematic Synthesis in Software Engineering. In *2011 International Symposium on Empirical Software Engineering and Measurement*. 275–284.

Jon Ivar Elstad and Kari Stefansen. 2014. Social variations in perceived parenting styles among Norwegian adolescents. *Child indicators research* 7, 3 (2014), 649–670.

Filippos Giannakas, Georgios Kambourakis, Andreas Papasalouros, and Stefanos Gritzalis. 2016. Security Education and Awareness for K-6 Going Mobile. *International Journal of Interactive Mobile Technologies (iJIM)* 10, 2 (2016), 41–48.

E. Kritzinger. 2015. Enhancing cyber safety awareness among school children in South Africa through gaming. In *2015 Science and Information Conference (SAI)*. 1243–1248. https://doi.org/10.1109/SAI.2015.7237303

Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. No Telling Passcodes Out Because They're Private: Understanding Children's Mental Models of Privacy and Security Online. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 64 (Dec. 2017), 21 pages. https://doi.org/10.1145/3134699

Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. 2018. Co-Designing Online Privacy-Related Games and Stories with Children. In *Proceedings of the 17th ACM Conference on Interaction Design and Children* (Trondheim, Norway) *(IDC '18)*. 67–79. https://doi.org/10.1145/3202185.3202735

Elmer Lastdrager, Ines Carvajal Gallardo, Pieter Hartel, and Marianne Junger. 2017. How Effective is Anti-Phishing Training for Children?. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 229–239.

Sonia Livingstone and Ellen J. Helsper. 2008. Parental Mediation of Children's Internet Use. *Journal of Broadcasting & Electronic Media* 52, 4 (2008), 581–599. https://doi.org/10.1080/08838150802437396 arXiv:https://doi.org/10.1080/08838150802437396

Pardon Blessings Maoneke, Fungai Bhunu Shava, Attlee Munyaradzi Gamundani, Mercy Bere-Chitauro, and Isaac Nhamu. 2018. ICTs Use and Cyberspace Risks Faced by Adolescents in Namibia. In *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities* (Windhoek, Namibia) *(AfriCHI '18)*. Article 11, 9 pages. https://doi.org/10.1145/3283458.3283483

Florence Martin, Chuang Wang, Teresa Petty, Weichao Wang, and Patti Wilkins. 2018. Middle School Students' Social Media Use. *Journal of Educational Technology Society* 21, 1 (2018), 213–224. http://www.jstor.org/stable/26273881

M.A. Moreno, K.G. Egan, and K Bare. 2013. Internet safety education for youth: stakeholder perspectives. *BMC Public Health* 13, 543 (2013). https://doi.org/10.1186/1471-2458-13-543

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. https://doi.org/10.3389/fpsyg.2020.00424

Suzanne Prior and Karen Renaud. 2020. Age-appropriate password "best practice" ontologies for early educators and parents. *International Journal of Child-Computer Interaction* 23-24 (2020), 100169. https://doi.org/10.1016/j.ijcci.2020.100169

Jennifer A. Rode. 2009. Digital Parenting: Designing Children's Safety. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology* (Cambridge, United Kingdom) *(BCS-HCI '09)*. BCS Learning Development Ltd., Swindon, GBR, 244–251.

Wonsun Shin and Hyunjin Kang. 2016. Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. *Computers in Human Behavior* 54 (2016), 114 – 123. https://doi.org/10.1016/j.chb.2015.07.062

M. Valcke, S. Bonte, B. De Wever, and I. Rots. 2010. Internet parenting styles and the impact on Internet use of primary school children. *Computers Education* 55, 2 (2010), 454–464. https://doi.org/10.1016/j.compedu.2010.02.009

Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017a. Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety?. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17)*. 51–69. https://doi.org/10.1145/2998181.2998352

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* (Vancouver, BC, Canada) *(CSCW '15)*. 302–316. https://doi.org/10.1145/2675133.2675293

Pamela Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017b. Parents Just Don't Understand: Why Teens Don't Talk to Parents about Their Online Risk Experiences. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17)*. 523–540. https://doi.org/10.1145/2998181.2998236

Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. 2017. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction* 13 (2017), 10 – 18. https://doi.org/10.1016/j.ijcci.2017.05.001

Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. '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 (CHI '19)*. 1–13. https://doi.org/10.1145/3290605.3300336