Empowering Parents to Support Children's Online Security and Privacy: Findings from a Randomized Controlled Trial

Xiaowei Chen*
Department of Behavioral and Cognitive Sciences
University of Luxembourg
Esch-sur-Alzette, Luxembourg

Verena Distler
Department of Computer Science
Aalto University
Espoo, Finland

Chloe Gordon
Institute for Positive Psychology and Education
Australian Catholic University
Melbourne, Australia

Yaxing Yao
Department of Computer Science
Johns Hopkins University
Baltimore, United States

Ziwen Teuber
Department of Behavioral and Cognitive Sciences
University of Luxembourg
Esch-sur-Alzette, Luxembourg

Abstract

In the ubiquitous computing society, parenting "digital natives" presents unprecedented challenges. Parents often rely on online resources to support and guide their children in security and privacy (**S&P**) related topics. However, the abundance of online resources makes it challenging for parents to find high-quality and relevant resources that align with their S&P needs. Further, the longitudinal development of parental competence and coping strategies in S&P topics remains largely unexplored.

We conducted a formative study with 210 U.S. parents of children (M_{age} = 11.73 years, SD = 3.15) to investigate the challenges parents face in educating children about online S&P topics and to inform the design of a remote intervention program (six short videos). In the main study, we evaluated this intervention's efficacy using a 14-week longitudinal randomized controlled trial, which consisted of 201 U.S. parents, with 113 assigned to the control group and 88 to the intervention group.

We found that short videos significantly enhanced parents' security awareness and their conversation strategies. Notably, parents who initially exhibited lower levels of these measurements benefited the most from the intervention. Moreover, short videos were effective in enhancing parents' self-efficacy in protecting their children from online risks. This study provides valuable insights into various challenges parents face and respective coping strategies that could be implemented to address S&P concerns in family settings. The design and evaluation of the intervention program serve as a foundation for future S&P researchers and educational stakeholders.

CCS Concepts

• **Security and privacy → Usability in security and privacy**; • **Applied computing → Education**.

Keywords

Security and privacy risks, Security intervention, Vulnerable groups, Educational short videos, Intervention evaluation, Measurement, Usable security and privacy, Human-centered security

ACM Reference Format:
Xiaowei Chen, Verena Distler, Chloe Gordon, Yaxing Yao, and Ziwen Teuber. 2025. Empowering Parents to Support Children's Online Security and Privacy: Findings from a Randomized Controlled Trial. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3719027.3765214

1 Introduction

Internet usage among children[1] has dramatically increased, with one in three Internet users worldwide being a child, and more than 175,000 children going online for the first time every day [1, 98]. Although the cyber world offers abundant opportunities for learning and creativity, it also presents various security and privacy (S&P) risks for children, such as harvesting of sensitive personal data and exposure to cyberbullying and harmful content [54]. For instance, about 55% of high school students in the United States have experienced online bullying or harassment [71]. Another German survey revealed that malware, account compromises, online shopping fraud, and data abuse are prevalent security threats among teenagers [41]. These S&P incidents can severely disrupt children's academic and socioemotional development and contribute to mental health issues.

We refer to *online security for children* as the practices, tools, and measures implemented to protect children from threats such as unauthorized access, cyberattacks, or other abnormal activities in digital spaces. Relevant topics include safeguarding children's digital devices, accounts, and communications to ensure confidentiality, integrity, and availability [1, 92]. *Online privacy for children* can be

[*] Corresponding Author. Contact: xiaowei.chen@uni.lu

[1] Definition of a child: any individual under the age of 18 [99].

CCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1525-9/2025/10
https://doi.org/10.1145/3719027.3765214

conceptualized as controlling the collection, use, and sharing of children's personal information in digital spaces, focusing on protecting sensitive data (e.g., identity, browsing habits, and communications) from unauthorized access or misuse without consent [58, 91]. Finally, *online safety for children* refers to protecting children from online threats that could harm their physical and mental health [93]. When a child's online security or privacy is compromised, it may lead to safety issues. For example, when smart security cameras installed in children's bedrooms are compromised [93], predators may exploit them to harass children remotely.

For children, including those considered "digital natives" [73], acquiring online S&P skills is a developmental learning process. Teaching these skills requires a shared responsibility between schools and families [4, 56]. Even for young educators, they do not adequately possess S&P knowledge and are not prepared to educate students on these topics [74]. Many educators rely on search engines to find relevant resources, whereas more experienced educators have accumulated trusted resources (e.g., slides, curricula, and videos) or seek recommendations from their colleagues [62]. Teachers might intentionally refrain from teaching certain topics they perceive as sensitive or uncomfortable [62], such as sexting. These points underline the critical role of family members in shaping children's S&P practices [41].

Many parents might themselves have limited S&P literacy, thereby influencing the extent to which they expose children to digital devices and informs their mitigation strategies [56, 93]. Prior studies [6, 32] have examined a number of off-the-shelf tools that enable parents to manage security and privacy in family settings. Parental control apps can enable parents to monitor children's unhealthy behaviors and keep them safe; however, these tools have also been criticized as overly restrictive and, in some cases, an invasion of children's privacy [32]. Further, researchers have indicated that vulnerabilities in parental control tools could be exploited and lead to security issues [6], such as device compromise and account takeover. Parents need to scrutinize the data such apps collect and evaluate the trustworthiness of their makers [7]. Consequently, the development of parents' S&P literacy is essential for the oversight of children's digital devices and management of off-the-shelf tools.

While considerable efforts have been made to address S&P issues in schools [17, 50], **how to support parents in developing awareness and coping strategies to address S&P risks in a family setting remains largely underexplored** [54, 55]—despite the fact that many S&P threats occur with children's digital devices outside of school premises and hours. The present study aimed to fill this research gap with a mixed-methods approach. We conducted a formative study to inform the design of a remote intervention program and a main study to evaluate the efficacy of the intervention. This work makes the following contributions:

- The creation of our intervention program provides a scalable solution that can be widely implemented to support parents in managing children's S&P in a family setting. We provide the interventions as supplemental materials for other researchers to adapt and use.
- The empirical validation of meaningful metrics for evaluating interventions offers a rigorous approach for future S&P studies, enabling reliable and consistent evaluation of similar interventions. We provide these metrics in the appendix for future use.
- The evaluation offers novel empirical insights into the effectiveness of parental support programs and we provide recommendations on how they can be tailored to address real-world concerns.

In the sections that follow, we review existing work on S&P education in family settings, explore these issues from a developmental psychology perspective, and present our research questions and hypotheses.

2 Related Work

2.1 Mitigation Strategies for S&P Risks and Available Educational Resources for Parents

Children encounter various online threats, such as cyberbullying, predators, invasion of privacy, inappropriate content, financial scams, hacking, and viruses [66]. Therefore, it is important for parents to have open communication with children about their online activities [31]. Another approach to mitigating these risks is to use parental monitoring applications to limit screen time, access to certain websites, and downloads. However, prior work found that parents had doubts about the feasibility and functionality of monitoring teenagers [76]. Researchers have suggested that parental monitoring may foster a perceived sense of parental control over children's internet use, which could lead to negative outcomes, such as lowering their guard to potential risks [31]. Researchers suggested that parents should support children in managing S&P issues rather than managing them on behalf of children [51].

Schoolteachers, parents, and governmental bodies are primary stakeholders for children's cyber security education [84]. Children commonly gain cybersecurity knowledge from family, friends, and other trusted individuals [41, 66]. Family conversations about S&P serve as an important mean for shaping children's S&P literacy [4]. Alghythee et al. [4] identified the following five conversation approaches: (a) rule-based, (b) example-based, (c) decision-making process-focused, (d) consequence-based, and (e) contextual conversations. While rule-based conversations were the most commonly reported approach by parents [4], tailoring S&P discussions to specific applications and combining multiple conversational strategies in parent-child interactions may be more effective than relying on a single approach. This requires parents to be knowledgeable about S&P topics and possess effective communication skills [82], which is not always the case. Enhancing parents' technical skills and self-efficacy is essential to overcoming these barriers [54]. Unfortunately, many resources designed to educate S&P topics appear to focus primarily on the school environment/children's needs [54, 106] and are inadequate for use in family settings. One potential solution is the development of literacy programs that specifically support parents in their role as guardians [54], equipping them with communication strategies for S&P conversations. To structure the skills parents needed to oversee digital natives, Romero [82] proposed a Parental Digital Literacy Framework. The framework highlights four sub-sets of skills [82]: (a) basic skills to manage privacy, content and technology, (b) communication skills, (c) creativity, problem-solving, attention and self-regulation skills, and (d) life-long learning.

Interventions aimed at developing parents' S&P literacy are scarce [55]. Prior media literacy interventions, including those targeting parents, have demonstrated effectiveness in enhancing parents' awareness of media influence, critical evaluation of media content, and domain-specific knowledge [47]. Informal sources, including interpersonal stories, news articles, and online content offering security advice [77], play an important role in shaping individuals' security practices. Other approaches to develop parents' S&P literacy include in-person workshops [40], parent-teacher conferences (hosted by school, municipality, or church), peer-to-peer learning, and community-based learning [55]. Additionally, parents can learn about S&P topics through video platforms, online communities, and educational content created by NGOs and governmental bodies [2, 82]. For example, NGOs like Common Sense Media and Family Online Safety Institute (both US-based) deliver curricula and strategies to promote safe and secure digital engagement within families. However, research has identified several unresolved challenges in using these online materials to effectively develop digital literacy, including difficulties in finding the relevant content, insufficient tailoring to varying literacy levels, and inadequate adaptation to the needs of the target audience [5].

2.2 Family Security and Privacy from a Developmental Psychology Perspective

Building on the definition used in parenting research [36], we define *family S&P education* as parental practices aimed at developing children's S&P awareness in online activities and safeguarding them from S&P risks. Decades of parenting research suggest that parents' support for their children's development in specific domains has a positive impact on overall child development [48]. Specifically, in the context of S&P, emerging studies highlight the pivotal role of family education in equipping children with the necessary skills to navigate digital challenges [37, 54, 75]. We focused on parents with children (in Grade 6-9), a group classified as "early adolescence" [64]. This developmental stage marked by significant biological, cognitive, social, and emotional changes that influence parent-child relationships [64]. During this period, children increasingly seek independence and become more involved in activities outside the family, often accompanied by reduced parental supervision. Parents navigate a renegotiation of authority and relationship boundaries with early adolescents, which can lead to conflicts [13] and pose challenges for parents in providing effective support during this critical stage [83]. On one hand, parents must demonstrate perseverance and consistency to achieve their parenting goals despite setbacks and difficulties. On the other hand, they must adapt to their children's evolving needs while maintaining these goals [34].

Previous quantitative studies have attempted to investigate how parenting behaviors impact their children through the lens of the four classical parenting styles: authoritative, authoritarian, neglecting, and permissive [9, 60]. These styles are defined by the combination of two key parenting dimensions: responsiveness (warmth) and demandingness (behavioral control). Authoritative parenting is characterized by high responsiveness and high demandingness, while permissive is characterized by high responsiveness and low demandingness. Since the 2000s, researchers [35] have acknowledged the critical role of autonomy—the sense of psychological liberty and the perception of self-directed choice, reflecting an individual's ability to act upon their own values and internal will [23]. Parental monitoring as a form of behavioral control may not be appropriate to guide early adolescents who seek for independence and autonomy; thus, parents should adapt their digital parenting strategies and styles according to their children's developmental stages.

The dynamic management of boundaries between teenage technology users, the outside world, and their parents has long been a complex issue. In the human-centered security and privacy community, researchers have investigated children's privacy and security, investigating topics such as connected toys [63], password behaviors [97], misinformation [88], reactions to phishing [53]. Cranor et al. [22] investigated parents' and teenagers' views of privacy in semi-structured interviews, comparing their differing views on boundaries. The authors found that parents struggled to conceptualize their teenagers' privacy boundaries, for instance, the extent to which text messages and apps were considered private by their kids. Children considered their phones more private than computers. Thus, intervention programs that target parenting strategies in the domain of online S&P in children need to respect their privacy. This aligns with research highlighting the importance of parents having conversations about decision-making thought processes with their children [4]. Parental approaches that balance guidance with autonomy—such as providing rationales rather than enforcing strict rules—help children develop critical thinking and skills in managing online risks.

In summary, it is important for parents to be aware of the various risks their children are exposed to when in their online endeavors. An effective intervention program to support parenting should align with their children's developmental stages. Such a program should not only provide parents with actionable toolkits but also remind parents to respect early adolescents' privacy and support them in developing their S&P competence.

3 Research Objectives

The overarching goal of our study was to develop a first version of a S&P intervention aimed at parents and to evaluate its efficacy. In the long run, we hope that this effort supports the research community and practitioners in working towards an evidence-based S&P intervention program for the family environment. To achieve this, we conducted a formative study and a main study. Through the formative study and post-intervention questionnaire, we sought to address the first research question (open and descriptive):

RQ1: What considerations should be taken into account when designing intervention programs to support parents in educating their children about online security and privacy?

The main study aimed to evaluate the effectiveness of the intervention program using a randomized controlled trial. According to the Protection Motivation Theory [57, 80], two key cognitive processes contribute to individuals' behavior change: (a) threat appraisal, which involves parents' awareness of the severity of online risks and children's vulnerability to such risks, and (b) coping appraisal, which refers to parents' belief in the efficacy of protective actions and their ability to perform them. Specifically, within the human-centered security community, Sasse et al. [85] emphasized the indispensable role of self-efficacy in individuals' adoption of new security behaviors. If parents have higher self-efficacy in guiding and protecting their children on S&P topics, they are more likely to implement related S&P practices. Thus, to empower parents in supporting their children's S&P, it is essential to enhance both parental awareness and parenting self-efficacy. This led to the second research question:

RQ2: How does a remote intervention influence parents' awareness, self-efficacy, and coping practices (e.g., parental mediation strategies and conversation approaches) in educating their children about security and privacy?

To test the intervention's effectiveness, we hypothesized the following:

H1: Parents in the intervention group will demonstrate a greater awareness of their children's online risks than those in the control group.

H2: Parents in the intervention group will report higher self-efficacy in supporting their children with online challenges than those in the control group.

H3: Parents in the intervention group will employ a broader range of mediation strategies and conversation approaches (or use them more frequently) compared to those in the control group.

H4 (exploratory): Levels of parental concerns about their children's online S&P may not differ between groups, as parents in the intervention group, while becoming more aware of potential risks, may also develop self-efficacy in managing them.

4 Methods

4.1 Formative Study

The formative study utilized a **questionnaire** comprising both open-ended questions and scale items, and it served two key purposes. First, it aimed to identify parents' difficulties and needs in supporting their children's online S&P. This was achieved through qualitative thematic analysis, with the findings directly informing the design of the intervention program to ensure its relevance and practicality. Second, the formative study assessed the measurements intended for use in the main study to evaluate the program's effectiveness. This step was critical, as some of these measurements had not undergone rigorous psychometric validation in prior research (e.g., [24]). Consequently, items on some scales were adapted or removed based on their theoretical alignment and psychometric properties, assessed through internal consistency estimates (Cronbach's alpha and McDonald's omega) and confirmatory factor analysis (**CFA**).

4.1.1 Participants. Parents residing in the United States with at least one child in Grades 6-9 were eligible to participate in this study. In September 2024, a total of 210 U.S. parents (53.33% mothers, n = 112) participated in the formative study via the online platform *Prolific*, with a mean age of 42.46 years (SD = 8.65). Approximately 62% held at least a bachelor's degree, and 80% reported being in a committed relationship. When answering questions about their children, parents were instructed to refer to their youngest child in grades 6 to 9. Among the referred children, 103 (49%) were girls and 107 (51%) were boys, with a mean age of 11.73 years (SD = 3.15). The socioeconomic status, assessed using the highest parental socioeconomic index (HISEI, [69]), was notably higher than the U.S. average (M = 65.32 vs. 55.7; [79]).

4.1.2 Challenges Parents Face. To address RQ1, we asked study participants, *Could you please elaborate on the difficulties you encountered when teaching your child about online security and privacy topics (e.g., online risks and privacy settings of apps)*? After removing ten empty answers, we recorded 200 valid answers. Three authors each familiarized themselves with 50 unique answers and then jointly created a first bottom-up categorization of meaningful codes [14]. Following this, the first author created an integrated coding scheme and coded all answers with MAXQDA [100], no new codes generated in this process. 65% of the answers were double-coded by another two authors; inter-rater reliability was analyzed using Cohen's κ, demonstrating substantial agreement (κ = 0.79). We include the coding scheme in **Appendix A**. 38 parents (19%) reported they had not encountered any challenges. In the following paragraphs, we present the four main categories of challenges that we identified:

Parental concerns about online risks (n = 67): Parents expressed concerns associated with their children's online activities. Many children were perceived to be overly trusting and did not always heed warnings (P2, P56), believing that strangers they meet online are who they claim to be and will be kind to them (P27, P32, P37). This over-trust might lead to dangerous situations, as children may share personal information or engage with strangers (P9, P21, P32). Additionally, parents worried that children often did not understand the potential dangers of the internet, feeling invincible due to a lack of negative experiences (P8, P68, P151). Parents also struggled with their children's overconfidence and resistance to their advice and stated that children believed they were more tech-savvy than their parents (P35, P96, P162).

Complexity of S&P topics from parents' perspective (n = 49): Many parents did not consider themselves knowledgeable in S&P topics (P64, P79, P200) or lacked confidence in explaining these topics (P13, P112, P135). Some indicated that they were not tech-savvy enough to teach their children, while others found it hard to keep up with new applications their children use and different privacy settings (P35, P85). Many parents also felt overwhelmed by the constantly evolving digital landscape, making it challenging to stay up-to-date on emerging threats (P1, P15, P75, P186). P163 expressed the need for "a reputable resource that stayed on top of things and offer digestible information."

Parenting challenges (n = 62): Many parents struggled to attract their children's attention and interest when having S&P conversations with them (P12, P54, P97). While parents acknowledged the need for parental monitoring, they expressed technical constraints, ethical concerns, and reluctance from their children (P22, P28, P109). Lastly, a few parents found S&P conversations awkward (P114), or they did not feel close enough to their child to discuss such topics (P146); as P44 described "(My child) doesn't want to talk to me about stuff like this. If I push it, she gets irritated and leaves the room."

Parents' critical reflections (n = 11): A few parents found it challenging to balance trusting and monitoring (P76), "teaching

Table 1: Summary of topics parents wanted to learn about.

Categories	Occurrence	Exemplary Topics
Online privacy-related topics	95	Privacy protection, privacy settings, keep personal information safe, sharing personal content/info/nudes online, digital footprints, keeping accounts private, and secure personal data
Online security-related topics	90	General security concerns, and specific threats (including hacking, phishing, scams, email/website account security, false identities, police involvement, passwords, virus, and ransomware)
Parental monitoring and parenting strategies	84	Setting parental controls, track kid's online behavior, location tracking, technology to protect children, websites that kids can access, good online habits, mental mindset, general tips; and how to teach children recognizing/avoiding online threats, securing their accounts, resources for teens to communicate with other youth, online safety for teenagers
Online protective actions	78	Websites should avoid, examples of dealing with specific websites; mental health and peer relationship issues, including smartphone addiction, cyberbullying; and safe social media usage, grooming, catfishing, and identity thief
Online harmful content	63	Pornography, racism, fake news, internet danger, drugs, bots on social media, hoax news, harmful websites, and misinformation
Current trends and emerging risks	12	AI-generated content, deepfake, sexting, latest applications and technologies

them and them tuning you out" (P77), and "fostering independence while ensuring security" (P153). Furthermore, in some cases, the social environment seemed to cause parents difficulties in pursuing S&P in the family; for example, P206 was frustrated by the insecure password policy suggested by their child's school, and the parents of their child's friends were extremely permissive when it came to digital devices, causing serious strain and power struggles between P130 and their child. Lastly, a couple of parents reflected on the challenges posed by tech companies and the lack of proper legislation (e.g., luring the attention of children, P36; lack of privacy protection for teenagers in the US, P29).

4.1.3 Intervention Design. Research indicates that short videos can be an effective training approach to engage trainees with S&P topics [10, 62]. Short videos can deliver a lot of content in a short time, catch viewers' attention, and have both short- and long-term training effects [10]. Short videos are an effective format for explaining complex S&P concepts [49, 90]. Furthermore, short videos are more cost-effective for large-scale deployment than in-person training or games [90, 106], which require more resources and logistics. Lastly, short videos can be accessed via different digital devices and have the potential to seamlessly integrate into parents' daily media consumption. Given these advantages, we selected educational short videos as the intervention approach in this study.

In the formative study, we surveyed the parents: *We're developing a program to help parents protect their children's online security and privacy. If you were to join this program, which three topics would you most like to learn about?* We received valid answers from 208 participants. After removing the irrelevant answers and merging similar topics, we summarize topics that parents want to learn in Table 1. Informed by the topics and challenges reported by parents, we developed six themes to address in our video series. It was not feasible to address every topic indicated by parents; therefore, we focused on categories-level and highlighted relevant S&P risks alongside respective coping strategies. Notably, our study participants often mixed online safety with security, prompting us to include certain online safety topics—such as avoiding online predators and harmful content—in our video episodes. Besides parents' expectations, we carefully estimated the potential impact that our intervention might have on their children (primarily "early adolescents"). We verified all the examples prior to including them in the videos with reputable media outlets. When we provided suggestions in the videos, they were based on peer-reviewed publications or relevant institutions (e.g., the Family Online Safety Institute). Considering early adolescence is a stage of seeking increasing levels of autonomy [83], we emphasize open communication in the family environment and parents' role in supporting children to develop their ability to manage their digital devices and accounts. We avoided emphasizing restrictive or authoritarian parenting styles and intentionally presented early adolescents' perspectives (e.g., using sarcasm, criticism, and yelling in serious conversations reduces effective communication [12]).

The production of each episode followed a structured process: defining the goal of each episode (see **Appendix B**), gathering relevant scientific papers and news stories, outlining the structure, drafting the script, recording audios, and completing visual editing. We used stock image/video/audio from Envato and Pexels, with Final Cut Pro as our editing tool. Two researchers with a background in educational psychology and media production and one media producer collaboratively created the following six short videos (in total 29 minutes):

Episode 1: Protecting kids' online security and privacy (3:51). In the introduction episode, we provide easy-to-understand definitions for online security [1] and online privacy [58] and examples relevant to children's online activities, including social media profile settings, meeting new friends online, online password protection, and downloading free games from unknown websites.

Episode 2: Seven steps to good digital parenting (5:00). We use educational videos created by Family Online Safety Institute (FOSI) as learning material in this episode[2]. The video emphasizes the following key steps to good digital parenting: a) talk with your child about what they are doing online, b) educate yourself to stay updated with technology, c) use parental controls to manage your child's online experience, d) set ground rules and enforce them, e) friend and follow, but don't stalk them, f) explore, share, and celebrate with your child, and g) be a good digital role model.

Episode 3: Dos and don'ts of parental monitoring (4:51). The episode starts with an overview of different ways of monitoring children's online activities, i.e., parental control applications (benefits and risks of using such apps [3]), setting rules and boundaries, and having weekly conversations with their child on their online activities. We introduce the key features of default parental control apps on iOS, Android, macOS, and Windows systems. The video ends with a call for direct communication within the family to support children in navigating the digital world safely.

Episode 4: Popular applications and associated risks (5:23). The episode first lists the 11 most popular apps among American teenagers, as reported by the Pew Research Center [8]. Then, we describe some potential risks associated with using these applications, such as account security threats, cyberbullying, online privacy issues, harmful content, online safety, and digital well-being, referring to various news articles.

Episode 5: Communication strategies on privacy and security (4:55). This episode highlights three strategies that parents can use to talk to their teenagers about online privacy and security (presented in [4]): sharing your own experiences to teach your child about the decision-making thought process, discussing the consequences of online actions, and tailoring advice to what your child actually uses (contextual conversations).

Episode 6: Emerging risks and parental support (5:12). We introduce emerging risks associated with children's usage of generative AI (identified by Yu et al. [105]), the improper use of deepfake technology, and sextortion targeting teenagers. We suggest parents have open and non-judgmental conversations, develop digital literacy alongside their child, and provide reassurance and support to mitigate emerging risks. The video ends with a recap of the key topics we introduced in the past five episodes.

4.1.4 Measurement Validation. Table 2 gives an overview of the measurements evaluated in the formative study, including a brief description of each construct, the number of facets and items, and goodness-of-fit. These measurements were informed by prior empirical studies [2, 4, 33] and grounded in established theoretical frameworks [57, 80]. All adapted measurements are included in **Appendix D**.

Parental security awareness (parental awareness). Parental cybersecurity situational awareness was assessed using a scale developed by Ahmad et al. [2], comprising six items (e.g., "I am aware of what my child is accessing"). Participants responded on a five-point Likert scale ranging from 1 (*strongly disagree*) to 5 (*strongly agree*). During analysis, the fourth item ("I realize how difficult it is to control my child's internet usage") displayed negative correlations with all other items and a negative factor loading in the CFA. After removing this item, the scale demonstrated a one-factor structure.

Parental concerns about security and privacy of their children (parental concerns). Parental concerns about children's online security and privacy were assessed using a 13-item scale informed by findings from the Australian Government's eSafety program [24]. The items addressed a range of potential online risks for children, such as "being called insulting names." Responses were recorded on a five-point Likert scale (1 = not at all, 5 = very much). A confirmatory factor analysis indicated an acceptable fit for a one-factor model.

Internet-specific parenting self-efficacy (parenting self-efficacy). We measured parents' confidence in managing their children's exposure to online risks with a scale developed by Glatz et al. [33]. Participants rated their confidence on eight five-point Likert items (e.g., "How confident are you in your ability to prevent your child from coming into contact with dangerous individuals?", 1 = *extremely unconfident* to 5 = *extremely confident*). The results of a CFA indicated a good fit for a one-factor model.

Internet-specific parental mediation (parental mediation). The items were adapted from the parental internet-specific mediation scale [33] to measure the frequency with which parents employ different mediation strategies to manage their children's online activities. The scale encompassed four dimensions. The first dimension, restrictive mediation, referred to parental rules about online activities and the use of monitoring software programs, including items such as, "How often do you use filtering software installed on your child's devices?" The second dimension, demands child disclosure, assessed how often parents require their children to provide information about their online activities, with items like, "How often do you demand to know which websites your child has visited?" The third dimension, active mediation, measured the frequency of discussions with the child about internet use, as captured by items such as, "How often do you talk to your child about what they are doing on the internet?" Finally, proximity refers to being physically present while the child uses the internet without actively interfering, with items such as, "How often do you sit with your child while they are online?" Answers were rated on a five-point Likert scale (1 = *never*, 5 = *always*). We performed a four-factor CFA model, which showed close fit.

Parental conversation approaches on security and privacy (conversation approaches). To evaluate the various approaches parents use when discussing S&P topics with their children, we developed a scale comprising five dimensions, based on a qualitative study [4]. The first dimension, rule-based conversations, involved parents discussing rules for digital privacy and security with their child (e.g., "I regularly discuss online safety rules with my child"). The second dimension, example-based conversations, focused on using illustrative examples to explain privacy and security concepts (e.g., "I show my child phishing emails I receive to help them recognize online scams"). The third dimension, decision-making thought processes, measured how parents guided their child in making rational decisions about digital privacy (e.g., "I explain to my child how I make choices about keeping our online information safe").

[2] We received authorization from FOSI to use their videos for research purpose. Link to the video series: https://www.fosi.org/how-to-be-good-digital-parent

Table 2: Overview of the measurements evaluated in the formative study.

Construct	Description	Factors (Items)	Response	α/ω	CFA Goodness-of-fit
Parental awareness [2]	It evaluates the level of a parent's awareness to protect their children from online risks.	1 (5)	1-5	.82/.83	$\chi^2(4)$ = 8.96, p = .06; CFI = .99; RMSEA = .08, 90% CI [.00, .15]; SRMR = .03
Parental concerns [24]	It measures parent's concerns about negative online experiences that might happen to their child online.	1 (13)	1-5	.82/.83.	$\chi^2(4)$ = 8.96, p = .06, CFI = .99, RMSEA = .08, 90% CI for RMSEA [.00, .15], SRMR = .03
Parenting self-efficacy [33]	It measures the extent to which a parent believes they can influence children's online behaviors and prevent them from online risks.	1 (8)	1-5	.93/.93	$\chi^2(19)$ = 48.04, p < .001; CFI = .95; RMSEA = .09, 90% CI [.06, .11]; SRMR = .04
Parental mediation [33]	It measures the frequency with which a parent uses different mediation strategies to manage their children's online activities.	4 (8)	1-5	.95/.95	$\chi^2(19)$ = 48.04, $\chi^2(48)$ = 97.177, p < .001; CFI = .97; RMSEA = .07, 90% CI [.05, .09]; SRMR = .04
Conversation approaches [4]	It assesses the extent to which a parent applies five conversation approaches when discussing S&P topics with their children.	5 (20)	1-5	.96/.96	$\chi^2(160)$ = 384.38, p < .001; CFI = .90; RMSEA = .08, 90% CI [.07, .09]; SRMR = .07

The fourth dimension, consequence-based conversations, emphasized highlighting the outcomes of privacy-related actions to raise the child's awareness (e.g., "I actively discuss with my child the potential risks and consequences of their online actions"). Lastly, contextual conversations involved discussing privacy and security issues specific to particular apps or platforms used by the child (e.g., "I discuss privacy issues with specific apps and platforms my child uses"). Items were evaluated on a five-point Likert (1 = *strongly disagree*, 5 = *strongly agree*). The five-factor CFA model demonstrated an acceptable fit.

Covariates: security attitudes and online privacy concerns Participants' general security attitudes were assessed using a scale developed by Faklaris et al. [27], consisting of six items. An example item is "I seek out opportunities to learn about security measures that are relevant to me." A unidimensional CFA model fit the data well. For online privacy attitudes, we adapted a scale validated by Buchanan et al. [15]. We selected six items related to online activities from the original scale (e.g., "Are you concerned about online organizations not being who they claim they are?"). The fifth item was removed as suggested by both scale analysis and CFA. Thus, the scale showed a one-factor structure with excellent goodness-of-fit.

4.2 Main Study

The main study was a randomized controlled trial (**RCT**) with a 2 (Treatment Condition: Intervention or Control) × 2 (Time: pre and post) design conducted over a 14-week period. Thus, it consisted of three phases: a pre-questionnaire, a 12-week remote intervention, a post-questionnaire. During the 12-week interval, participants in the intervention group received a short video and a feedback questionnaire every two weeks via *Prolific.* The intervention was evaluated both during the program (via a short questionnaire after each episode) and afterward (through pre- and post-intervention test comparisons). Refer to Figure 1 for an illustration of our experiment design.

4.2.1 Data Collection and Participants. Before data collection, we estimated the optimal sample size using a prior power analysis with the program *G*power* [28]. With the expectation of a medium effect size of η^2 = .06 as a more conservative estimate, a total sample size of 128 (i.e., 64 in each group; using the F-test) should be sufficient to detect main and interaction effects (1-β = 80). Taking possible attrition into account ([25] shows an attrition rate up to 30% in an in-person intervention program) and recognizing that online interventions assume even higher attrition rates (e.g., due to reduced personal engagement or technical barriers), an oversampling of N = 320 was reasonable.

In September 2024, 320 U.S. parents with at least one child in Grades 6-9 were invited to participate in the study via the online platform *Prolific.* Of these, 135 parents were randomly assigned to the control group, and 185 to the intervention group. All participants completed a pre-questionnaire upon enrollment. Subsequently, parents in the intervention group received a *Qualtrics* survey every two weeks via their Prolific accounts. Each contact point included informed consent, one video episode, a multiple-choice question to review the key points of the episode, feedback questions, and a playlist link to all previous videos. We did not provide specific instructions to parents after videos, as family contexts varied (e.g., device use and family rules). The videos were hosted on YouTube for its wide accessibility and lack of account restrictions for viewing. In comparison with the alternative approach of asking parents to subscribe to a channel on their preferred video platforms, this controlled setting enabled us to isolate, to a certain extent, contextual variability across platforms, which facilitated evaluations that were less confounded by differences in media platforms.

In Episode 1 of the intervention, 160 out of 185 parents participated; however, the responses of eight parents were excluded due to a completion duration shorter than the length of the video (n = 152). In Episode 2, seven parents dropped out, and the responses of eleven parents were removed for short durations (n = 134). In Episode 3, 16 more participants dropped out, and 17 participants' responses were excluded due to rapid completion times (n = 114). Episode 4 saw

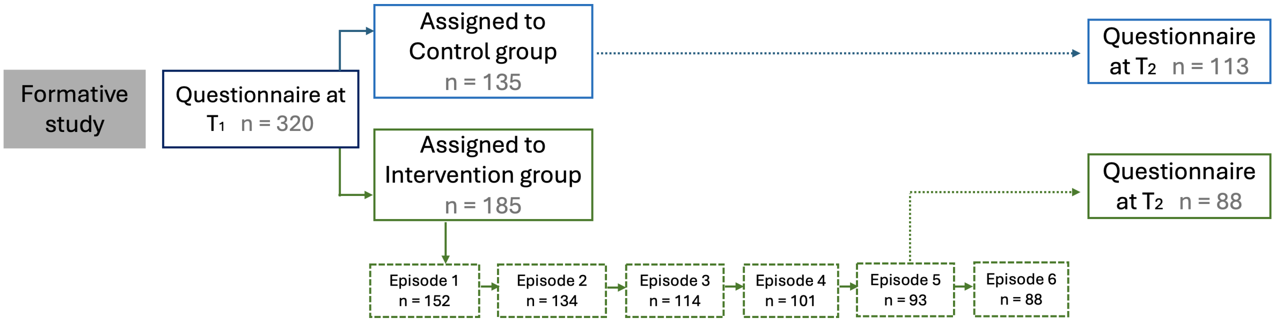
Formative study
Questionnaire at T₁ n = 320
Assigned to Control group n = 135
Assigned to Intervention group n = 185
Questionnaire at T₂ n = 113
Questionnaire at T₂ n = 88
Episode 1 n = 152
Episode 2 n = 134
Episode 3 n = 114
Episode 4 n = 101
Episode 5 n = 93
Episode 6 n = 88

Figure 1: Flowchart of our experiment design: 14-week interval between timepoint 1 (T_1) and timepoint 2 (T_2).

eight additional dropouts, along with five responses removed for short completion durations (n = 101). Finally, in Episode 5, five parents dropped out, and the responses of three parents were excluded for the same reason (n = 93). We invited participants who watched all of the first five episodes and all participants assigned to the control group to complete the post-questionnaire. This time, five participants from the intervention group and 21 from the control group dropped out. Refer to **Appendix E** to see the dropout rate table.

Thus, the sample for the quantitative evaluation of the intervention's efficacy consisted of a total of 201 parents (111 mothers), with 88 in the intervention group and 113 in the control group. On average, participants were 44.89 years old (SD = 8.71) and had 2.19 children (SD = 0.96) in their household. The average HISEI score was 64.95 (SD = 17.53), which exceeded the U.S. average level. No statistically significant differences were found between the intervention group and control group in terms of sociodemographics, including age, gender distribution, number of children, and socioeconomic status. For the qualitative feedback analysis, we included participants who took part in each episode. Although some of them dropped out in later episodes, their suggestions remained constructive for improving our intervention.

4.2.2 Measurements. To evaluate the efficacy of the intervention, we assessed the following measurements in both pre- and post-questionnaires with *Likert scales*:

- Parental security awareness
- Parental concerns about S&P of their children
- Internet-specific parenting self-efficacy
- Internet-specific parental mediation
- Parental conversation approaches on S&P
- *Covariates*: general security attitude and privacy concerns

Single question feedback: Participants' subjective evaluation of each episode was assessed using the following indicators: (1) the perceived usefulness and clarity of the video (e.g., "Please rate the usefulness/clarity of the video"), rated on a five-point Likert scale ranging from 1 (*Poor*) to 5 (*Excellent*); and (2) the likelihood of recommending the video to others (e.g., "How likely are you to recommend this video to another parent?"), rated on a five-point Likert scale ranging from 1 (*Very unlikely*) to 5 (*Very likely*).

Open-ended questions: Participants were invited to provide suggestions for improving each episode by responding to an open-ended question: "Do you have any suggestions for improving the video?" Additionally, we asked participants after Episode 6, "Are there any other topics you would like us to include in future Parenting Digital Natives series?" Lastly, in the post-questionnaire, we asked the participants, "Have you tried any of the recommended strategies? If so, could you briefly share your experience with us?"

4.3 Ethics Considerations

The research project received approval from the Ethics Review Panel of [anonymized for review] prior to implementation. Participation was entirely voluntary, and informed consent was obtained from each participant. Detailed information about the study's purpose was provided to participants, and they were reminded of their right to withdraw at any time without needing to give an explanation. For the main study, on average, participants spent 10.88 minutes in the questionnaire at pre-questionnaire; for the questionnaire at post-questionnaire, participants spent 9.40 minutes. We provided $10 to each participant who completed the pre- and post-questionnaires. The intervention group participants further received $2 for attending each session (5-6 min per session). Additionally, a bonus of $5 was awarded to those who attended all of the first five sessions. Participants could also request their data be withdrawn at any stage without facing any negative consequences. All data sets were identifiable only through a pseudo-anonymous identifier, accessible exclusively by *Prolific*. This identifier was deleted after data matching.

4.4 Data Analysis

In the preregistration, we initially planned to use analysis of variance (ANOVA) with repeated measures. Instead, we decided to use generalized linear regressions to investigate the effect of the intervention. This method is flexible in handling missing values and random effects, accommodates unbalanced groups, and enables the inclusion of covariates and additional predictors. Compared to ANOVA (including non-parametric forms of ANOVA, like ART-ANOVA), it provides richer insights into the effect size of predictors [95]. We used MAXQDA to analyze qualitative data [100]. We followed an inductive thematic analysis approach [14] to familiarize ourselves with the data, generate meaningful codes, categorize coded segments, and summarize descriptively the key findings. The coding and theme development were driven by the data content, which ensured that the participants' voices remained central in the data analysis.

Table 3: Mean (*SD*) of measurements and t-tests of between-group difference. Note: CG for control group; IG for intervention group. * *p* < .05; ** *p* < .01; *** *p* < .001.

Variable	Pre-questionnaire			Post-questionnaire		
	CG	IG	*t*	CG	IG	*t*
Parental awareness	4.16 (0.61)	4.31 (0.5)	-1.86	4.14 (0.54)	4.3 (0.42)	-2.35*
Parental concerns	3.12 (1.04)	3.01 (1.12)	0.73	3.3 (1)	3.13 (1.13)	1.09
Parenting self-efficacy	3.31 (0.81)	3.5 (0.72)	-1.82	3.27 (0.85)	3.59 (0.73)	-2.83**
Parental mediation	3.13 (0.8)	3.16 (0.91)	-0.21	3.14 (0.81)	3.25 (0.78)	-0.98
Conversation approaches	3.82 (0.74)	3.87 (0.7)	-0.52	3.85 (0.71)	3.97 (0.61)	-1.27
Consequence-based conversations	4.03 (0.86)	4.13 (0.74)	-0.92	4.06 (0.76)	4.21 (0.58)	-1.57
Decision-making thought process	3.82 (0.87)	3.9 (0.86)	-0.63	3.83 (0.81)	4.06 (0.66)	-2.16*
Security attitude	3.8 (0.68)	3.88 (0.78)	-0.81	3.81 (0.69)	3.98 (0.69)	-1.74
Privacy concerns	3.52 (0.96)	3.43 (1.02)	0.64	3.65 (0.96)	3.58 (1.01)	0.55

5 Results

5.1 Intervention Efficacy

In both pre- and post-questionnaires, we examined parental awareness, parental concerns, parenting self-efficacy in preventing children from online risks, parental mediation, and parental conversation approaches. Furthermore, we measured two covariates: general security attitude and privacy concerns. Table 3 presents the descriptive statistics for all measurements. The Shapiro-Wilk tests revealed that, except for parental mediation, all other measurements were not normally distributed. For between-group comparisons, we used t-tests. Notably, the measurements at pre-questionnaire showed no statistically significant differences between the control group and the intervention group. At post-questionnaire, the intervention group demonstrated significantly higher levels of parental awareness, parenting self-efficacy, and decision-making thought processes (a key dimension of parental S&P conversation approaches) compared to the control group. For within-group comparisons, we conducted Wilcoxon signed-rank tests. Among our target outcomes, while the increase of parental awareness, parental concerns, and parenting self-efficacy in the intervention group did not reach statistical significance, decision-making thought processes demonstrated significance (V = 637.5, p = .03). In terms of covariates, we observed a significant increase in privacy concerns from pre-questionnaire to post-questionnaire for both the control group (V = 1671.5, p = .02) and the intervention group (V = 798, p < .05).

We used generalized linear regressions to investigate the effect of the intervention. In all regressions, each target outcome at the post-questionnaire was predicted by its (a) respective value at pre-questionnaire, (b) general privacy concerns at pre-questionnaire, (c) security attitude at pre-questionnaire, (d) condition/group assignment (i.e., 0 = *CG*, 1 = *IG*), (e) the interaction a*d, and (f) whether any strategies learned in the intervention were applied (1 = *applied*, 0 = not *applied*; 63 indicated applied). Furthermore, we controlled for sex and age.

The results showed that the main effect of condition was not significant for parental concerns, overall parental mediation, or general conversation approaches, indicating that being in the intervention group did not influence these factors. However, significant main effects of the intervention were observed for parental awareness, parenting self-efficacy, and consequence-based conversations and decision-making thought processes—two specific aspects of conversation approaches. Regarding the main effects, the intervention increased parental awareness (B = 1.38, SE = 0.42, t = 3.26, p < .01), parenting self-efficacy (B = 1.18, SE = 0.46, t = 2.53, p < .05), consequence-based conversations (B = 0.82, SE = 0.37, t = 2.22, p < .05) and decision-making thought processes (B = 0.87, SE = 0.35, t = 2.53, p < .05). In terms of time × condition interaction effects, a significant negative effect was found between pre-questionnaire parental awareness and intervention (B = -0.31, SE = 0.10, t = -3.11, p < .01); also between pre-questionnaire consequence-based conversations and intervention (B = -0.20, SE = 0.09, t = -2.22, p < .05). Additionally, a significant negative interaction was identified between pre-questionnaire decision-making thought processes and the intervention (B = -0.20, SE = 0.08, t = -2.41, p < .05). See **Appendix F** for regression tables. These findings indicate that the intervention had a diminishing effect on gains in awareness, consequence-based conversations, and decision-making thought processes as baseline levels increased, suggesting a stronger impact on parents with lower initial scores and a leveling effect at higher initial scores.

Key results. The video series effectively increased parental awareness and parenting self-efficacy. While it did not significantly impact overall parental mediation or conversation approaches, a closer examination of specific facets revealed that the intervention increased the frequency of consequence-based conversations and sharing decision-making thought processes.

5.2 Intervention Feedback

The mean value of clarity/usefulness for all episodes reached a score above 4, indicating "very good" in delivering the planned topics of the episode. With a mean of 4.46, participants of Episode 5 generally found the video to be between "Very good" and "Excellent" in terms of clarity in explaining the different communication strategies for privacy and security. Regarding the likelihood to recommend, except for Episode 2, all other episodes achieved a score of 4 or above, indicating they would "likely" recommend the respective

Table 4: Mean (SD) of feedback questions of each episode. Note: "-" indicates the metric was not measured for the episode.

	Episode 1	Episode 2	Episode 3	Episode 4	Episode 5	Episode 6
Clarity	-	4.39 (0.72)	-	4.38 (0.68)	4.46 (0.65)	4.39 (0.70)
Usefulness	4.01 (0.84)	-	4.12 (0.78)	-	-	-
Likelihood to recommend	4.05 (0.98)	3.95 (1.10)	4.00 (1.04)	4.17 (0.93)	4.17 (0.97)	4.25 (0.93)

episode to other parents. We include the mean (SD) of feedback questions of each episode in Table 4.

The high scores in clarity, usefulness, and likelihood to recommend align with the predominantly positive feedback we received in response to the open-ended question, "Do you have any suggestions for improving the video?" Of the 544 responses, 352 (65%) indicated that they had no suggestions for improvement. The most frequently mentioned keywords in the positive responses were: "great" (45 times), "informative" (29 times), "high quality" (27 times), "excellent" (17 times), "useful/helpful" (16 times), "concise/clear/straightforward" (14 times), and "easy to understand" (14 times). Additionally, in 76 instances, participants provided suggestions for improving the video series, focusing on the following aspects:

More engaging narrative: Most participants praised the audio for being clear and understandable. In all episodes, we had a native American male from [anonymized for review] as the narrator. However, some participants suggested that the pacing could be faster (E4P16, E4P85, E5P92[3]). A few participants criticized the monotone narrative style as lacking engagement (E1P63, E2P9). E4P64 specifically recommended a female voice to better engage the audience. Surprisingly, E1P93 misperceived the narrator as an AI voice, noting that "the pronunciation came off weird quite a few times, as well as the inflection." These suggestions highlight the important role of the narrator in engaging the audience.

Better visual presentation: Several participants suggested improving the visual presentation with animations (E1P110) or high-quality images (E1P144). We used stock videos/photos from Envato and Pexels for the visual elements, but some scene compositions were less polished than others in the video (E4P77). E1P111 suggested using a more casual and personable presentation manner to make the video more relatable and engaging. Further, regarding content accessibility and retention, E3P72 recommended providing a text summary of key points at the end of the video for easier reference. E2P84 suggested adding descriptive words during the narrative to emphasize key points could guide viewers' attention to important aspects of the video.

Further in-depth content: Several participants recommended creating videos with more actionable advice, particularly in areas like addressing children's antagonistic or hostile attitude when establishing rules on internet use (E2P81), as well as easier-to-follow tutorials (e.g., "digital parenting for dummies", E4P91). Participants also preferred videos that address specific concerns, such as the dangers of online predators (E2P69), how to respond when "seeing something bad" (E2P99), and children's interaction with specific apps (E1P91), in dedicated videos. Overall, they called for videos that not only offer general advice but also provide in-depth, actionable, and application-specific guidance.

Broader target audience: The intervention program aimed to support parents in having security and privacy conversations within a family setting. Many participants perceived the program as successful, with E2P103 noting that "it did a great job of showing it can be easy and fun to get involved with my kids and what they are doing online." Some participants reported that they were already applying what they had learned from the videos and sharing these educative materials (E5P68). However, some parents suggested the creation of videos specifically designed for children (E1P100), as well as videos that parents and children could watch together. Such resources could help bridge the knowledge gap between parents and children (E5P83).

When it comes to **topics for future episodes**, most participants considered the six episodes covered well the topics that they were interested in (E6P26, E6P46, E6P61). Meanwhile, participants expressed that the videos should be an evolving program, as "online landscape is always changing" (E6P36) and "threats keep emerging time to time" (E6P48). Participants, especially, expected more GAI-related content (E6P66, E6P30) and videos about the consequences of neglecting security and privacy (E6P67). Further, participants wanted to receive suggestions on where to find relevant resources (E6P65). Lastly, participants called for tutorial videos, showing them the parental controls available on a phone (E6P29), how to adjust settings on various digital devices (E6P68), and how to break screen time habits for both parents and children (E6P17).

> *Key results.* Parents found the short videos"great," "informative," and of "high quality," and expressed their high likelihood of recommending the video series to other parents. Meanwhile, they suggested a more engaging narrative, better visual presentation, further in-depth content, and a broader target audience for future series. The video intervention should be an evolving program tailored to parents' specific needs.

6 Discussion

6.1 Anticipating User Needs to Inform Intervention Design

The formative inquiry laid a solid foundation for designing our intervention. A key challenge in designing the intervention was to ensure the content remained relevant to target users. Informed by User Experience (**UX**) scholars [52, 101], we used open-ended questions to collect parents' needs (difficulties in teaching S&P topics) and their anticipation of the intervention program (topics that they want to learn). This step informed the thematic topics that guided our intervention goals for each episode. Although most of these topics have already been highlighted as important in recent

[3] E5P92: Participant 92 of Episode 5

S&P literature [4, 41, 105], without empirical inquiry, we cannot match them to our target parents (of children in Grades 6–9). It is important to note that one limitation of this formative inquiry is that parents could not anticipate the S&P risks they were unaware of or not engaging with (e.g., in the Character.ai case [72], parents could not predict the harm of conversational agents they were not familiar with). In addition to the qualitative survey, other methods (e.g., in-depth interviews [44] and focus groups [19]) can also serve as formative inquiry methods.

Although the video series received positive feedback from parents, practitioners can apply various strategies to further engage the audience. We primarily used the following strategies to create our videos: translating scientific knowledge into relatable language, explaining S&P topics with news stories, matching image cues with narratives, and presenting key points in a structured way (similar to academic presentations). The video series was produced with a singular narrative, aligning speech with online stock visuals. Additional visual design and communication techniques could be adopted in future video interventions to enhance audience engagement (see section 5.2). Additionally, when combined with storytelling techniques [46, 104], short videos can serve as an effective format for teaching S&P topics.

6.2 Short Video as a Scalable and Flexible Intervention Approach

Short videos can serve as an effective intervention approach for addressing S&P topics within the family environment. Both quantitative and qualitative data from the current study supported the effectiveness of the video format, with participants rating all intervention videos as "very good" in terms of clarity and usefulness. Further, the videos increased parental awareness, parenting self-efficacy and two of the targeted conversation approaches in relation to security and privacy issues. There are several reasons why short videos may work as an effective intervention for parents. People learn best when complementary information is presented simultaneously to both the auditory and visual systems [59, 81]. Another key advantage of videos is their asynchronous nature, which provides greater control over their learning process [68]. Parents can pause videos to take notes, skip less relevant sections, or revisit information as needed. These features may be particularly beneficial for parents with limited time, as they help reduce cognitive load and facilitate information retention. Additionally, short videos are a relatively low-cost intervention, as they can be easily and widely distributed once produced, and recent work [42] suggest to explore it as an innovative format to educate the public of emerging scams.

Some of our targeted outcomes did not achieve statistical significance through the intervention program, including parental mediation strategies (the frequency with which parents employ specific mediation strategies to manage their children's online activities) and contextualizing S&P conversations. The following three factors might cause this. First, our intervention might not have delivered the various mediation strategies as effectively as it did for other planned topics (see section 4.1.3). As suggested by participants, in-depth or step-by-step videos on specific mediation strategies might address this flaw. Second, we postulate a group difference between measurements. Significant results related to attitudes and beliefs (parental awareness/self-efficacy), while non-significant measurements captured the frequency of mediation. Third, although 63 participants reported applying strategies, the extent varied, and the behavioral impact might take an extended time to reach statistical significance. This highlights the value of longitudinal designs and triangulating scale measurements with other data sources.

6.3 Adding a Control Group and Evaluating Over Time Makes a Difference

Even without intervention, the control group showed a statistically significant increase in general privacy concerns from pre- to post-questionnaires. This unexpected finding has several important implications. First, the act of responding to items related to privacy concerns may have prompted parents to reflect on their attitudes and behaviors and heightened their awareness of privacy-related issues. This phenomenon, known as the mere measurement effect [65], suggests that simply engaging with privacy topics can influence cognitive processes and inspire self-reflection. Second, the rise in privacy concerns suggests that these concerns may evolve with time, for instance, influenced by exposure to news reports on the topic or experiences in the personal environment of the participant. Without a control group, it may be difficult to discern whether observed changes result from the intervention itself or other external factors, such as natural development, stimuli from external events, or participant expectations. By isolating the treatment effect, the control group provides a clearer, more reliable measure of the intervention's true impact [89]. Together, these implications highlight the critical importance of including a control group to differentiate the effects of the intervention from potential influences of self-reflection triggered by measurement and the passage of time.

Lessons learned from a 14-week experiment: *dropout rate, application*, and *those who stayed*. Evaluating S&P interventions presents significant challenges for the research and practitioner community [43]. Lack of longitudinal and in-the-field evaluations limits the ecological validity and generalizability of findings [18, 20]. Further, the design and implementation of longitudinal experiments necessitate careful consideration during interpretation [16]. 16% of the participants from the control group dropped out over the period of 14 weeks, and 5-15% of the participants from the intervention group dropped out at each contact point (excluding the ones declined our study invitation). Future researchers may consider our dropout rate as a point of reference when designing longitudinal experiments. Further, the longitudinal design allows parents to digest and apply what we delivered in the video series, as evidenced by 63 of them indicating they had applied the learned strategies in the post-questionnaire. Additionally, we postulate that the contact points can serve as biweekly reminders of learning, similar to "triggers" in Fogg's behavior change model [29], which prompted them to pay more attention to S&P topics in their daily life. It is noteworthy that, although our intervention received relatively high ratings in the feedback questions (Table 4), the rising positive ratings between Episodes 2 and 6 require scrutiny, considering that parents who did not like our interventions might have dropped out.

6.4 Collaborative Approaches to Developing S&P Literacy in Families

Mitigating online S&P risks in families requires a collaborative approach involving both parents and their children. Our study not only validates the importance of this collaborative approach [3, 70] but also contributes insights into how we can form this collaborative approach in practice. Research on mitigating S&P risks in smart homes [93] emphasizes that transparency between parents and children can facilitate knowledge sharing and open communication, thus supporting joint learning and shared oversight. When parents adopt a more open yet constructive attitude toward their children's online behaviors, they can foster a positive emotional climate at home and have a positive impact on their children's digital habits and decision-making. Further, Alghythee et al. [4] suggested designing privacy literacy interfaces that support the interaction between parents and children in the learning process. This aligns with the suggestion from our study participants to create video series suitable for parents and children to learn together, creating occasions that they can exchange on various S&P topics.

In our study, some parents described tension with their children when addressing S&P topics and found it difficult to initiate conversations. Indeed, a study investigating the experiences of "security adepts" (referring to adults) [30] found that challenges included a lack of interest, a feeling of judging others' behaviors, and fear of being perceived as paranoid. The authors recommended the use of conversation starters (e.g., media coverage, action days, movies; see also [78]) to break the ice. When parents frequently use rule-based conversations, they may encounter resistance from their children [4]. However, diversifying S&P conversation approaches requires parents to update their digital literacy, actively collect materials, and learn about the applications their children are using. 81% of parents in the formative study expressed varying degrees of difficulty in addressing S&P topics. As most security interventions predominantly focus on student demographics [94], parents would appreciate more structured intervention programs to support the development of their S&P literacy. Our intervention program only dived into three conversation strategies and provided overviews for S&P concepts, and good digital parenting. Many other topics that parents wanted to learn (see Table 1) can be included to develop future intervention programs to empower parents.

6.5 Creating Hassle-free Interventions for Families

Addressing the security and privacy challenges faced by the general public requires an interdisciplinary approach. Whenever a new technology is deployed in society, malicious players find ways to exploit these technologies and put people's security and privacy at risk [39]. As technologies have assimilated into families, organizations, and government bodies, S&P literacy has become necessary for the general public. We combined expertise in digital literacy, security and privacy intervention design, and developmental psychology to address this challenge. So far, cybersecurity is still an emerging theme for the media literacy community [26]. This work can draw the attention of the media literacy community to integrate family S&P topics into their research scope. Furthermore, the developmental needs of children require further consideration in prioritizing safety and privacy by design from technology makers [38]. For instance, platforms should take more responsibility for protecting children from harmful content and online predators (see Table 1), reducing the burdens parents experience in their everyday lives. Lastly, the development of S&P literacy among the public, in tandem with technological deployment, is imperative for mitigating various risks posed by adversarial players. How to design relevant and hassle-free interventions for everyday technology users remains an important area for further exploration. Our positive feedback highlights that interventions which adopt formats already embedded in individuals' daily lives, are tailored to relevant topics, and impose minimal costs on target users are likely to be accepted by them.

When an intervention is embedded into the existing workflows and routines of target users, it creates less friction. In contrast, some intervention formats, e.g., in-person workshops [20] or online courses [106], require dedicated time slots, pulling users away from their daily routines. A widely adopted, though controversial, example of workplace embedded training is the simulated phishing campaign. However, such an approach is not easily transferable to non-work environments. Moreover, researchers have criticized it for being less effective than assumed [45] and for inducing negative emotions in recipients [19, 87]. In light of this, low cost refers not only to individual time investment but also to emotional costs [103]. Furthermore, individuals present varying levels of security and privacy literacy; when an intervention does not align with users' skill levels, they may perceive it as having low task value and disengage from it [21]. Another promising direction to make interventions more relevant is to personalize them based on users' differing levels of proficiency [86]. In addition to tailored short videos, researchers can further explore how to utilize existing household devices to create low-effort and emotionally positive interventions [102]. Opportunities such as "learning interfaces" [4, 67] may also act as stimuli to raise S&P awareness in families.

6.6 Limitations and Future Directions

The present study has some limitations. First, while it is one of few longitudinal study designs in human-centered security, our dependent variables were measured at two points of time, two weeks before and after the intervention. This does not allow us to investigate the sustainability of the intervention, which could be addressed in future research, for example, by incorporating follow-up assessments after five months [11]. Second, our collected data relied on self-reports, which could be triangulated with teenager self-reported data, or even observational insights in the future. Conversely, we were interested in parents' concerns, beliefs, and attitudes, which are intrapsychic constructs and can be ideally measured through self-reports [61]. We did not investigate teenagers' views in the present study due to the limitation of data collection through a crowdsourcing platform. While parents might feel more aware and self-efficacious after the intervention, we did not investigate how these changes were perceived by their children. Third, the sample in the main study consisted of parents of schoolchildren in grades 6-9 and had a higher socio-economic status compared to the U.S. average, limiting the generalizability of the results to the broader population of U.S. parents or parents from other regions[42].

Furthermore, we did not include a knowledge quiz or attempt to assess parents' new knowledge. Future work might set more specific learning objectives and assess whether these were reached. Parents in the intervention group may have developed increased curiosity about S&P topics and sought additional resources. Future studies might include it as a possible confounding variable, as some observed outcomes may be attributable to participants' independent learning rather than the intervention content alone.

Last but not least, although the video format offers several advantages for parenting interventions, a potential limitation is its reliance on internet availability and a certain level of digital competency. Short videos have become a popular medium consumed by the general public, offering opportunities to deploy educational content across different platforms. By aligning with individuals' existing media consumption habits, short videos can reduce cognitive barriers to engagement and potentially foster S&P awareness in a more contextually relevant and accessible manner. However, parents with lower digital skills may be less likely to access or engage with video interventions, even though they may have a greater need for such resources due to a wider gap between their own and their child's digital competencies. Future research could explore which parent groups may be underserved by video interventions and investigate alternative formats (e.g., community-based learning [55]) to ensure these groups are also supported effectively.

7 Conclusion

In this study, we aimed to bridge the gap between research and practice by developing an evidence-based intervention program to support parenting in the context of protecting children from online S&P risks. Through a 14-week randomized controlled trial, the evaluation revealed that short videos can be an effective approach to enhance parental awareness, develop parenting self-efficacy, and diversify conversation approaches.

The feedback from our intervention points to promising directions for future research in the family environment to protect children from security and privacy risks. Some key implications include: (a) anticipating target users' needs to inform intervention design, and suggesting various strategies researchers can apply to further engage the audience with short video format interventions; (b) short videos can be a scalable and flexible intervention approach in families, and future in-depth or tutorial videos on specific topics can further support parents; (c) it is important to include a control group to differentiate the effects of the intervention from potential influences of self-reflection and the passage of time, and to interpret longitudinal results with scrutiny; and (d) short videos can be a suitable medium for learning and exchange on S&P topics between parents and children; practitioners and researchers could explore topics not covered in our study in future intervention programs to support parents. As an additional resource associated with this paper, we provide the video series and the validated measurement scales for future research and application.

Data Availability Statement

The preregistration [96], Appendixes, intervention program, anonymized datasets generated in the main study, and R scripts used for analysis are included in the OSF repository: osf.io/x3ust.

Acknowledgments

Author 1 gratefully acknowledges the financial support of the Institute for Advanced Studies (IAS) at the University of Luxembourg through a 'Young Academics' grant awarded in 2021. The study was supported by the User Lab of the University of Luxembourg. We thank Christine Schiltz (Cognitive Science and Assessment Institute) and Sascha Helsper (MEDIACentre) for their support in producing the video series. We thank Family Online Safety Institute for allowing us to include *Seven steps to good digital parenting* in our video series. We also thank Marek for his contribution to video design and voiceovers.

References

[1] Wasyihun Sema Admass, Yirga Yayeh Munaye, and Abebe Abeshu Diro. 2024. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications* 2 (2024), 100031.

[2] Nazilah Ahmad, Umi Asma'Mokhtar, Wan Fariza Paizi Fauzi, Zulaiha Ali Othman, Yusri Hakim Yeop, and Siti Norul Huda Sheikh Abdullah. 2018. Cyber security situational awareness among parents. In *2018 cyber resilience conference (crc)*. IEEE, 1–3.

[3] 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.

[4] Kenan Kamel A Alghythee, Adel Hrncic, Karthik Singh, Sumanth Kunisetty, Yaxing Yao, and Nikita Soni. 2024. Towards Understanding Family Privacy and Security Literacy Conversations at Home: Design Implications for Privacy Literacy Interfaces. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–12.

[5] Badr A Alharbi, Usama M Ibrahem, Mahmoud A Moussa, Mona A Alrashidy, and Sameh F Saleh. 2023. Parents' digital skills and their development in the context of the Corona pandemic. *Humanities and Social Sciences Communications* 10, 1 (2023), 1–10.

[6] Suzan Ali, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef. 2020. Betrayed by the guardian: Security and privacy risks of parental control solutions. In *Proceedings of the 36th annual computer security applications conference*. 69–83.

[7] Khalid Alkhattabi, Ahmed Alshehri, and Chuan Yue. 2020. Security and privacy analysis of android family locator apps. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*. 47–58.

[8] Monica Anderson, Michelle Faverio, and Jeffrey Gottfried. 2023. Teens, Social Media and Technology 2023. https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/. Accessed: 10-27-2024.

[9] Diana Baumrind. 1991. The influence of parenting style on adolescent competence and substance use. *The journal of early adolescence* 11, 1 (1991), 56–95.

[10] Benjamin M. Berens, Mattia Mossano, and Melanie Volkamer. 2024. Taking 5 minutes protects you for 5 months: Evaluating an anti-phishing awareness video. *Comput. Secur.* 137, C (4 2024), 19 pages. doi:10.1016/j.cose.2023.103620

[11] Benjamin M Berens, Mattia Mossano, and Melanie Volkamer. 2024. Taking 5 minutes protects you for 5 months: Evaluating an anti-phishing awareness video. *Computers & Security* 137 (2024), 103620.

[12] Better Health Channel. n.d.. Teenagers and communication. https://www.betterhealth.vic.gov.au/health/healthyliving/teenagers-and-communication. Accessed: 2025-01-17.

[13] Susan Branje. 2018. Development of parent–adolescent relationships: Conflict interactions as a mechanism of change. *Child development perspectives* 12, 3 (2018), 171–176.

[14] Virginia Braun and Victoria Clarke. 2021. Thematic analysis: a practical guide to understanding and doing. 1. *Thousand Oaks* (2021).

[15] Tom Buchanan, Carina Paine, Adam N Joinson, and Ulf-Dietrich Reips. 2007. Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American society for information science and technology* 58, 2 (2007), 157–165.

[16] Edward Joseph Caruana, Marius Roman, Jules Hernández-Sánchez, and Piergiorgio Solli. 2015. Longitudinal studies. *Journal of thoracic disease* 7, 11 (2015), E537.

[17] Jake Chanenson, Brandon Sloane, Navaneeth Rajan, Amy Morril, Jason Chee, Danny Yuxing Huang, and Marshini Chetty. 2023. Uncovering Privacy and Security Challenges In K-12 Schools. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, Article 592, 28 pages. doi:10.1145/3544548.3580777

[18] Sunil Chaudhary, Vasileios Gkioulos, and Sokratis Katsikas. 2022. Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal*

of Cybersecurity 8, 1 (2022), tyac006.

[19] Xiaowei Chen, Sophie Doublet, Anastasia Sergeeva, Gabriele Lenzini, Vincent Koenig, and Verena Distler. 2024. What Motivates and Discourages Employees in Phishing Interventions: An Exploration of Expectancy-Value Theory. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 487–506.

[20] Xiaowei Chen, Margault Sacré, Gabriele Lenzini, Samuel Greiff, Verena Distler, and Anastasia Sergeeva. 2024. The Effects of Group Discussion and Role-playing Training on Self-efficacy, Support-seeking, and Reporting Phishing Emails: Evidence from a Mixed-design Experiment. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, Article 829, 21 pages. doi:10.1145/3613904.3641943

[21] Xiaowei Chen, Lorin Schöni, Verena Distler, and Verena Zimmermann. 2025. Beyond Deterrence: A Systematic Review of the Role of Autonomous Motivation in Organizational Security Behavior Studies. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '25)*. Association for Computing Machinery, Article 919, 28 pages. doi:10.1145/3706598.3713122

[22] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy In a Technology-Filled World. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 19–35.

[23] Edward L Deci and Richard M Ryan. 2000. The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological inquiry* 11, 4 (2000), 227–268.

[24] eSafetyresearch. 2019. Parenting in the digital age. https://www.esafety.gov.au/research/parenting-digital-age. Accessed: 12-02-2024.

[25] Heike Eschenbeck, Laya Lehner, Hanna Hofmann, Stephanie Bauer, Katja Becker, Silke Diestelkamp, Michael Kaess, Markus Moessner, Christine Rummel-Kluge, Hans-Joachim Salize, et al. 2019. School-based mental health promotion in children and adolescents with StresSOS using online or face-to-face interventions: study protocol for a randomized controlled trial within the ProHEAD Consortium. *Trials* 20 (2019), 1–12.

[26] Francisco Javier Rocha Estrada, Carlos Enrique George-Reyes, and Leonardo David Glasserman-Morales. 2022. Security as an emerging dimension of Digital Literacy for education: a systematic literature review. *Journal of E-Learning and Knowledge Society* 18, 2 (2022), 22–33.

[27] Cori Faklaris, Laura A Dabbish, and Jason I Hong. 2019. A self-report measure of end-user security attitudes (SA-6). In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*. 61–77.

[28] Franz Faul, Edgar Erdfelder, Albert-Georg Lang, and Axel Buchner. 2007. G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior research methods* 39, 2 (2007), 175–191.

[29] Brian J Fogg. 2009. A behavior model for persuasive design. In *Proceedings of the 4th international Conference on Persuasive Technology*. 1–7.

[30] Nina Gerber and Karola Marky. 2022. The Nerd Factor: The Potential of S&P Adepts to Serve as a Social Resource in the User's Quest for More Secure and Privacy-Preserving Behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 57–76.

[31] Michaela Geržičáková, Lenka Dedkova, and Vojtěch Mỳlek. 2023. What do parents know about children's risky online experiences? The role of parental mediation strategies. *Computers in Human Behavior* 141 (2023), 107626.

[32] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J LaViola Jr, and Pamela J Wisniewski. 2018. Safety vs. surveillance: what children have to say about mobile apps for parental control. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–14.

[33] Terese Glatz, Elizabeth Crowe, and Christy M Buchanan. 2018. Internet-specific parental self-efficacy: Developmental differences and links to Internet-specific mediation. *Computers in human behavior* 84 (2018), 8–17.

[34] Christa L Green, Joan MT Walker, Kathleen V Hoover-Dempsey, and Howard M Sandler. 2007. Parents' motivations for involvement in children's education: An empirical test of a theoretical model of parental involvement. *Journal of educational psychology* 99, 3 (2007), 532.

[35] Shayl F Griffith and Wendy S Grolnick. 2014. Parenting in Caribbean families: A look at parental control, structure, and autonomy support. *Journal of Black Psychology* 40, 2 (2014), 166–190.

[36] Wendy S Grolnick. 2016. Parental involvement and children's academic motivation and achievement. In *Building autonomous learners: Perspectives from research and practice using self-determination theory*. Springer, 169–183.

[37] Moritz Gruber, Christian Höfig, Maximilian Golla, Tobias Urban, and Matteo Große-Kampmann. 2022. "We may share the number of diaper changes": A Privacy and Security Analysis of Mobile Child Care Applications. *Proceedings on Privacy Enhancing Technologies* (2022).

[38] Andrew Hale, Barry Kirwan, and Urban Kjellén. 2007. Safe by design: where are we now? *Safety science* 45, 1-2 (2007), 305–327.

[39] Joseph M Hatfield. 2018. Social engineering in cybersecurity: The evolution of a concept. *Computers & Security* 73 (2018), 102–113.

[40] Cristyne Hébert, Kurt Thumlert, and Jennifer Jenson. 2022. # Digital parents: Intergenerational learning through a digital literacy workshop. *Journal of Research on Technology in Education* 54, 1 (2022), 34–91.

[41] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M Angela Sasse. 2024. Digital Security—A Question of Perspective A Large-Scale Telephone Survey with Four At-Risk User Groups. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 697–716.

[42] Franziska Herbert, Collins W Munyendo, Jonas Hielscher, Steffen Becker, and Yixin Zou. 2025. Digital Security Perceptions and Practices Around the World: A WEIRD versus Non-WEIRD Comparison. In *USENIX Security*. USENIX.

[43] Jonas Hielscher, Markus Schöps, Jens Opdenbusch, Felix Reichmann, Marco Gutfleisch, Karola Marky, and Simon Parkin. 2024. Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors' Promises. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*. 2666–2680.

[44] Myat Pan Hmone, Michael J Dibley, Mu Li, and Ashraful Alam. 2016. A formative study to inform mHealth based randomized controlled trial intervention to promote exclusive breastfeeding practices in Myanmar: incorporating qualitative study findings. *BMC Medical Informatics and Decision Making* 16 (2016), 1–10.

[45] Grant Ho, Ariana Mirian, Elisa Luo, Khang Tong, Euyhyun Lee, Lin Liu, Christopher A Longhurst, Christian Dameff, Stefan Savage, and Geoffrey M Voelker. 2025. Understanding the efficacy of phishing training in practice. In *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE, 37–54.

[46] David Michael Hull, Sebastian Walter Schuetz, and Paul Benjamin Lowry. 2023. Tell me a story: The effects that narratives exert on meaningful-engagement outcomes in antiphishing training. *Computers & Security* 129 (2023), 103252.

[47] Se-Hoon Jeong, Hyunyi Cho, and Yoori Hwang. 2012. Media literacy interventions: A meta-analytic review. *Journal of communication* 62, 3 (2012), 454–472.

[48] William H Jeynes. 2024. A Meta-Analysis: The Association Between Relational Parental Involvement and Student and Parent Outcome Variables. *Education and Urban Society* 56, 5 (2024), 564–600.

[49] Smirity Kaushik, Yaxing Yao, Pierre Dewitte, and Yang Wang. 2021. "How I Know For Sure": People's Perspectives on Solely Automated Decision-Making (SADM). In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 159–180.

[50] Priya C. Kumar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2019. Privacy and Security Considerations For Digital Technology Use in Elementary Schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, 1–13. doi:10.1145/3290605.3300537

[51] Priya C Kumar, Fiona O'Connell, Lucy Li, Virginia L Byrne, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2023. Understanding Research Related to Designing for Children's Privacy and Security: A Document Analysis. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference*. 335–354.

[52] Carine Lallemand and Guillaume Gronier. 2015. *Méthodes de design UX: 30 méthodes fondamentales pour concevoir et évaluer les systèmes interactifs*. Editions Eyrolles.

[53] Elmer Lastdrager, Inés 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, 229–239.

[54] Ann-Kristin Lieberknecht. 2024. Exploring Determinants of Parental Engagement in Online Privacy Protection: A Qualitative Approach. In *Proceedings of the 2024 European Symposium on Usable Security*. 94–111.

[55] Ann-Kristin Lieberknecht and Aline Melanie Ochs. 2024. Safeguarding Children's Digital Privacy: Exploring Design Requirements for Effective Literacy Training for Parents. In *IFIP World Conference on Information Security Education*. Springer, 111–126.

[56] Lanjing Liu, Lan Gao, Nikita Soni, and Yaxing Yao. 2024. Exploring Design Opportunities for Family-Based Privacy Education in Informal Learning Spaces. *Proceedings on Privacy Enhancing Technologies* (2024).

[57] James E Maddux and Ronald W Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology* 19, 5 (1983), 469–479.

[58] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*. 83–95.

[59] Richard E Mayer. 2008. Applying the science of learning: evidence-based principles for the design of multimedia instruction. *American psychologist* 63, 8 (2008), 760.

[60] EE McCoby. 1983. Socialization in the context of the family: Parent-child interaction. *Handbook of child psychology* 4 (1983), 1–101.

[61] Jennifer Dodorico McDonald. 2008. Measuring personality constructs: The advantages and disadvantages of self-reports, informant reports and behavioural

assessments. *Enquire* 1, 1 (2008), 1–19.

[62] Joy McLeod, Leah Zhang-Kennedy, and Elizabeth Stobert. 2024. Comparing teacher and creator perspectives on the design of cybersecurity and privacy educational resources. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 587–603.

[63] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 5197–5207. doi:10.1145/3025453.3025735

[64] Laurie L Meschke, Christina Renee Peter, and Suzanne Bartholomae. 2012. Developmentally appropriate practice to promote healthy adolescent development: Integrating research and practice. In *Child & Youth Care Forum*, Vol. 41. Springer, 89–108.

[65] Vicki G Morwitz, Eric Johnson, and David Schmittlein. 1993. Does measuring intent change behavior? *Journal of consumer research* 20, 1 (1993), 46–61.

[66] 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.

[67] Doruntina Murtezaj, Viktorija Paneva, Verena Distler, and Florian Alt. 2024. Public Security User Interfaces: Supporting Spontaneous Engagement with IT Security. In *Proceedings of the New Security Paradigms Workshop*. 56–70.

[68] Michael Noetel, Shantell Griffith, Oscar Delaney, Taren Sanders, Philip Parker, Borja del Pozo Cruz, and Chris Lonsdale. 2021. Video improves learning in higher education: A systematic review. *Review of educational research* 91, 2 (2021), 204–236.

[69] OECD. 2023. PISA 2022 Results (Volume II): Learning During–and From–Disruption. https://doi.org/10.1787/a97db61c-en.

[70] Jinkyung Katie Park, Mamtaj Akter, Pamela Wisniewski, and Karla Badillo-Urquiola. 2024. It's Still Complicated: From Privacy-Invasive Parental Control to Teen-Centric Solutions for Digital Resilience. *IEEE Security & Privacy* (2024).

[71] J. W. Patchin and S. Hinduja. 2024. 2023 Cyberbullying Data. Cyberbullying Research Center. https://cyberbullying.org/2023-cyberbullying-data. Accessed: 10-23-2024.

[72] Kate Payne. 2025. In lawsuit over teen's death, judge rejects arguments that AI chatbots have free speech rights. https://apnews.com/article/ai-lawsuit-suicide-artificial-intelligence-free-speech-ccc77a5ff5a84bda753d2b044c83d4b6. Accessed: 2025-07-12.

[73] Marc Prensky. 2001. Digital natives, digital immigrants part 2: Do they really think differently? *On the horizon* 9, 6 (2001), 1–6.

[74] Portia Pusey and William A Sadera. 2011. Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education* 28, 2 (2011), 82–85.

[75] Farzana Quayyum. 2023. Collaboration between parents and children to raise cybersecurity awareness. In *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference*. 149–152.

[76] 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.

[77] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (2015), 121–144.

[78] Maike M. Raphael, Aikaterini Kanta, Rico Seebonn, Markus Dürmuth, and Camille Cobb. 2024. Batman Hacked My Password: A Subtitle-Based Analysis of Password Depiction in Movies. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Philadelphia, PA, 199–218.

[79] Kristina Reiss, Mirjam Weis, Eckhard Klieme, and Olaf Köller. 2019. *PISA 2018: Grundbildung im internationalen Vergleich.* Waxmann Verlag.

[80] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91, 1 (1975), 93–114.

[81] Vivien E Rolfe and Douglas Gray. 2011. Are multimedia resources effective in life science education? A meta-analysis. *Bioscience education* 18, 1 (2011), 1–14.

[82] Margarida Romero. 2014. Digital literacy for parents of the 21st century children. *Elearning Papers* 38 (2014), 32–40.

[83] Richard M Ryan, Edward L Deci, Wendy S Grolnick, and Jennifer G La Guardia. 2015. The significance of autonomy and autonomy support in psychological development and psychopathology. *Developmental psychopathology: Volume one: Theory and method* (2015), 795–849.

[84] Rahime Belen Sağlam, Vincent Miller, and Virginia NL Franqueira. 2023. A systematic literature review on cyber security education for children. *IEEE Transactions on Education* 66, 3 (2023), 274–286.

[85] M Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2022. Rebooting it security awareness–how organisations can encourage and sustain secure behaviours. In *European Symposium on Research in Computer Security*. Springer, 248–265.

[86] Lorin Schöni, Neele Roch, Hannah Sievers, Martin Strohmeier, Peter Mayer, and Verena Zimmermann. 2025. It's a Match - Enhancing the Fit between Users and Phishing Training through Personalisation. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, Article 592, 25 pages. doi:10.1145/3706598.3713845

[87] Markus Schöps, Marco Gutfleisch, Eric Wolter, and M Angela Sasse. 2024. Simulated Stress: A Case Study of the Effects of a Simulated Phishing Campaign on Employees' Perception, Stress and Self-Efficacy. In *33rd USENIX Security Symposium (USENIX Security 24)*. 4589–4606.

[88] Filipo Sharevski and Jennifer Vander Loop. 2023. Children, Parents, and Misinformation on Social Media. http://arxiv.org/abs/2312.09359 arXiv:2312.09359 [cs].

[89] Bonnie Sibbald and Martin Roland. 1998. Understanding controlled trials. Why are randomised controlled trials important? *BMJ: British Medical Journal* 316, 7126 (1998), 201.

[90] Garrett Smith, Sarah Carson, Rhea G Vengurlekar, Stephanie Morales, Yun-Chieh Tsai, Rachel George, Josh Bedwell, Trevor Jones, Mainack Mondal, Brian Smith, et al. 2024. "I Know I'm Being Observed:" Video Interventions to Educate Users about Targeted Advertising on Facebook. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–27.

[91] Daniel J Solove. 2005. A taxonomy of privacy. *University of Pennsylvania Law Review* 154 (2005), 477.

[92] William Stallings and Lawrie Brown. 2015. *Computer security: principles and practice.* Pearson.

[93] Kaiwen Sun, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. 2021. Child safety in the smart home: parents' perceptions, needs, and mitigation strategies. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–41.

[94] Valdemar Švábenský, 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.

[95] Barbara G Tabachnick, Linda S Fidell, and Jodie B Ullman. 2013. *Using multivariate statistics.* Vol. 6. Pearson Boston, MA.

[96] Ziwen Teuber and Xiaowei Chen. 2025. Parenting Digital Natives: A Randomized Controlled Trial on Security and Privacy Education in Families. https://doi.org/10.17605/OSF.IO/ZQY7B. OSF Preregistration.

[97] Mary Theofanos, Yee-Yin Choong, and Olivia Murphy. 2021. 'Passwords Keep Me Safe' – Understanding What Children Think about Passwords. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 19–35.

[98] UNICEF. 2018. More than 175,000 children go online for the first time every day, tapping into great opportunities. https://www.unicef.org/eca/press-releases. Accessed: 12-01-2024.

[99] UNICEF. 2023. Convention on the Rights of the Child - Children's Version. https://www.unicef.org/child-rights-convention/convention-text-childrens-version. Accessed: 12-01-2024.

[100] VERBIsoftware. 2024. MAXQDA. https://www.maxqda.com/.

[101] Arnold POS Vermeeren, Effie Lai-Chong Law, Virpi Roto, Marianna Obrist, Jettie Hoonhout, and Kaisa Väänänen-Vainio-Mattila. 2010. User experience evaluation methods: current state and development needs. In *Proceedings of the 6th Nordic conference on human-computer interaction: Extending boundaries*. 521–530.

[102] Alexandra von Preuschen, Carolin Benda, Monika Christine Schuhmacher, and Verena Zimmermann. 2025. Fear, Fun or None: A Qualitative Quest Towards Unlocking Cybersecurity Attitudes. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 1091, 24 pages. doi:10.1145/3706598.3713538

[103] Alexandra Von Preuschen, Monika C Schuhmacher, and Verena Zimmermann. 2024. Beyond fear and frustration-towards a holistic understanding of emotions in cybersecurity. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. 623–642.

[104] Rick Wash and Molly M. Cooper. 2018. Who Provides Phishing Training? Facts, Stories, and People Like Me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–12. doi:10.1145/3173574.3174066

[105] Yaman Yu, Tanusree Sharma, Melinda Hu, Justin Wang, and Yang Wang. 2024. Exploring Parent-Child Perceptions on Safety in Generative AI: Concerns, Mitigation Strategies, and Design Implications. In *Proceedings of 2025 IEEE Symposium on Security and Privacy (SP)* (San Francisco, US, May 12, 2025).

[106] Leah Zhang-Kennedy and Sonia Chiasson. 2021. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Comput. Surv.* 54, 1, Article 12 (Jan. 2021), 39 pages. doi:10.1145/3427920