JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGY
https://e-journal.uum.edu.my/index.php/jict

How to cite this article:
Hassan, S., Ahmad, R., Abd-Wahab, A., Mohammed, F. & Purbasari, A. (2025). Parental strategies for mitigating online threats and enhancing children's cybersecurity awareness. *Journal of Information and Communication Technology, 24*(4), 111-134. https://doi.org/10.32890/jict2025.24.4.5

Parental Strategies for Mitigating Online Threats and Enhancing Children's Cybersecurity Awareness

[1]Syahida Hassan, [2]Rahayu Ahmad, [3]Alawiyah Abd Wahab, [4]Fathey Mohammed & [5]Ayi Purbasari
[1,2&3] School of Computing, Universiti Utara Malaysia, Malaysia
[4]Department of Business Analytics, Sunway University, Malaysia
[5]Fakultas Teknik, Universitas Pasundan, Indonesia

[*1]syahida@uum.edu.my
[2]rahayu@uum.edu.my
[3]alawiyah@uum.edu.my
[4]fatheym@sunway.edu.my
[5]pbasari@unpas.ac.id
*Corresponding author

Received: 31/1/2025 Revised: 31/3/2025 Accepted: 31/7/2025 Published: 31/10/2025

ABSTRACT

The widespread adoption of digital technology has also resulted in a concerning trend: the rise in online threats targeted at children. As online threats to children continue to increase, parents need to take proactive steps to protect their children's safety on the Internet. This research explores how parents respond to online threats affecting their children by examining their cyber-parenting approaches and coping strategies through Protection Motivation Theory (PMT). This research involved semi-structured interviews with nine parents whose children had experienced online threats. The study revealed that authoritative parenting, which balances autonomy with guidance, was the most adopted approach by parents. Conversely, parents with a high level of digital literacy tended towards an authoritarian style, characterised by rigorous monitoring of their adolescents' online activities. Following online threat incidents, parents adopted both problem-focused coping and emotion-focused coping. These responses reflected varying degrees of threat appraisal and coping appraisal, consistent with PMT constructs. By identifying prevalent parenting styles and coping strategies, this research contributes to a deeper

understanding of how parental behaviours influence children's online behaviours and resilience to cyber incidents. The study also found that effective parental mediation not only reduces children's exposure to harm but also plays a critical role in fostering their cybersecurity awareness, empowering them to recognise risks, apply protective behaviours, and navigate digital environments with greater confidence. Such insights are critical for designing effective interventions and educational initiatives aimed at fostering safer digital practices among families, particularly in raising children's awareness.

Keywords: Children's cybersecurity awareness, online threats, digital parenting approaches, cybersecurity awareness, information security.

INTRODUCTION

Nowadays, with easy access to the Internet and social media during childhood, children develop a growing dependency on technology (Pazarcikci, 2024) and become habituated to having it as part of their everyday lives. Children typically engage in more risk-prone behaviours than older age groups. This inclination is often influenced by peer pressure, making younger individuals more susceptible to engaging in high-risk activities, including deviant or criminal behaviours (Balogh et al., 2013; Steinberg, 2008). Consequently, this vulnerability can lead young people to commit criminal acts and become targets for online offenders (Aiken et al., 2016; Brewer et al., 2018).

Online threat refers to threats committed online, utilising a computer as either a tool, a targeted individual, or a combination of both (Sabillon et al., 2016). Usually, online threat happens silently without the target realising it. Online threats can occur in various forms, such as phishing, identity theft, viruses and malware, cyberstalking, cyberbullying, online harassment, and hacking. The prevalence of online threats can be denoted by the statistics reported by Bernama (2022), where 13,000 complaints were made in 2019 and increased to over 20,000 cases in 2021. The number of children targeted by online threats increased by nearly 20% between 2015 and 2022 (Federal Bureau of Investigation, 2022). For a child, the online threats may result in social isolation, social withdrawal, mental health issues (such as depression and anxiety), substance abuse, self-harm or suicide, low self-esteem, problem within the family, problems at school, lack of trust, emotional well-being, sense of security, as well as an increased likelihood of exhibiting abusive behaviours themselves in adulthood (UNICEF, n.d.; Chang et al., 2023; Borwell et al., 2025).

Given the evolving nature of online threats and the potential impact on children's well-being, a nuanced exploration of effective parenting strategies in the digital age is crucial. Any parenting approach designed to foster a safe online environment for children is considered a cyber parenting strategy (Shin & Luin, 2022). These strategies involve active engagement with children's digital activities, providing guidance on appropriate online behaviour, and implementing measures to protect them from potential online threats. These practices do more than just regulate access, as they play a significant role in shaping children's digital literacy and cybersecurity awareness. Chen et al. (2024) found that effective parental mediation increases teenagers' privacy risk perception and self-efficacy in managing online threats, which are key cognitive components in developing online threat-conscious behaviour.

Similarly, Sciacca et al. (2022) found that active and restrictive parental mediation are associated with enhanced digital literacy skills and safer online practices among children. Sciaca's findings suggest that cyber parenting is not merely about control but also about equipping children with the awareness and skills necessary to navigate digital environments safely and responsibly. Other research suggests that

higher parental digital literacy is associated with enhanced online safety for children; however, the mechanisms underlying this relationship remain poorly understood (Wisniewski et al., 2017). Despite the growing importance of digital parenting, there remains a lack of research examining how parents with differing levels of digital literacy manage their children's online safety (Tomczyk & Potyrała, 2021). For instance, it is unclear how parents with varying levels of digital literacy interpret online risks, respond to these threats, educate their children about them, and monitor their children's online activities.

While previous studies highlight the impact of various parenting strategies, the results have been inconsistent. For example, an authoritative parenting style is linked to a reduced risk of children being exposed to online threats (Okeke et al., 2024), whereas children raised by permissive or uninvolved parents are more likely to engage in inappropriate online behaviour due to limited guidance and supervision (Elsaesser et al., 2017). However, some research has produced conflicting results. For example, Katz et al. (2019) found that neither general cyber parenting strategies nor cyber-specific mediation styles reliably predicted children's involvement as targets of online threats. In addition, limited studies are focusing on how parents cope after their children have been exposed to online threats (Elsaesser et al., 2017; Tomczyk & Potyrała, 2021; Benatov, 2019).

Addressing these gaps, the present study aims to explore how parents with various levels of digital literacy appraise and respond to online threats affecting their children, and how these appraisals shape their cyber parenting approaches. By documenting both the parenting strategies employed and the coping mechanisms adopted during and after such incidents, this study offers valuable insights into how families navigate children's exposure to online risks. The Protection Motivation Theory (PMT) is used as the guiding framework for this study. This theory is chosen as it explains how individuals assess threats and their capacity to manage them, thereby influencing protective behaviours (Rogers, 1975; Dodge et al., 2023). Applying PMT in the context of cyber parenting helps to clarify the link between parents' perceptions of digital risks and their motivation to act to protect their children. Importantly, these protective actions are not only about risk avoidance but also contribute to children's development of cybersecurity awareness, equipping them with the skills and confidence to navigate digital environments more safely and independently.

LITERATURE REVIEW

Protection Motivation Theory (PMT)

PMT explain individuals' motivation to engage in protective behaviour in response to perceived threats (Rogers, 1975). It is originally grounded in health psychology; however, it has been widely adopted in other research domain, which includes cybersecurity and technology use (Rogers & Prentice-Dunn, 1997; Dodge et al., 2023). PMT describes how individuals evaluate threats and assess their ability to cope with the threats. The evaluation is conducted through two primary cognitive processes, (1) threat appraisal - assessing the perceived severity of a threat and one's vulnerability to it (Rogers, 1983; Conner & Norman, 2015), where the greater the perceived risk and impact, the higher the motivation to adopt protective behaviours (Chenoweth et al., 2009) and (2) coping appraisal - evaluates one's belief in the efficacy of the protective response, self-efficacy, and response costs.

In cybersecurity contexts, PMT has been employed to understand how individuals make decisions about adopting protective behaviours such as using strong passwords, installing antivirus software, or avoiding suspicious websites (Dodge et al., 2023; Chenoweth et al., 2009), and intention to protect

oneself in e-services (Hassan et al., 2024), avoiding phishing attack (Manoharan et al., 2022), or reducing data breaches (Rubis, 2024). Studies show that users are more likely to take proactive digital safety measures when they perceive online threats as severe and themselves as capable of managing them (Martens et al., 2019).

In cyber parenting research, PMT can explain how parents assess online threats to their children and choose corresponding strategies. However, its application in cyber parenting remains underexplored. While previous literature has emphasised parenting styles, IT or digital literacy, and coping strategies (Elsaesser et al., 2017; Wisniewski et al., 2017), PMT allows the connection between risk perception and how the parents deal with it. By incorporating PMT, researchers can better explain variations in parental monitoring, education, and intervention following online threat incidents involving their children. For example, Hwang et al. (2017) demonstrated that both perceived severity and self-efficacy significantly influence the adoption of active and restrictive parental mediation strategies. Similarly, Teimouri (2015) found that parents with stronger perceptions of online threat severity and higher efficacy are more likely to engage in protective actions that reduce children's exposure to online risks. Notably, these actions not only serve to shield children but also play a formative role in enhancing their cybersecurity awareness, particularly when mediation involves discussion, guidance, and the development of coping skills (Livingstone & Helsper, 2008; Livingston et al., 2015). Thus, PMT not only supports the theoretical framing of parental protection behaviours but also helps clarify how such behaviours shape children's understanding and resilience in the digital environment.

Types of Common Online Threats Targeting Children

One of the most prevalent online threats targeting children is cyberbullying. Numerous studies confirm that online harassment of youth is widespread globally. In the Malaysian context, cyberbullying appears alarmingly common. Prior studies among Malaysian children found prevalence rates as high as 52% (Marret & Choo, 2017; Samsudin et al., 2023). A 2020 global survey ranked Malaysia second in Asia for youth cyberbullying incidence (Razali & Nawang, 2022), indicating that Malaysian children are disproportionately at risk of online harassment by peers. This underscores that cyberbullying is not only a global phenomenon but also a pressing local issue. Many studies demonstrated that females were more likely to be cyberbullied than males (Zhu et al., 2021). Research suggests that parental inconsistency in monitoring children's online activities and parental neglect are linked to the direct or indirect harm of cyberbullying (Hong et al., 2018; Katz et al., 2019).

Another online threat targeted at children is online sexual exploitation, which includes grooming, sextortion, and the spread of child sexual abuse materials. Sextortion, where children are coerced via nude images or videos and then blackmailed for more content or money, has surged in recent years, with a 7,200% increase between 2021 and 2022 (We Protect Global Alliance, 2024). Malaysian children are not immune to these dangers. Malaysian authorities have recently received reports of child grooming groups operating on popular social platforms (Basir, 2024). A UNICEF Malaysia study in 2021 found that about 4% of Malaysian internet users aged 12–17 had encountered threats of online sexual exploitation or abuse, a concerning figure given the under-reporting in this domain (UNICEF, n.d.). These trends illustrate that sexual predators are leveraging technology to reach minors worldwide, necessitating stronger safeguards and awareness to protect children from such threats.

Children are also susceptible to phishing, hacking, and other online threat tactics. Attackers may target minors through deceptive emails, messages, or in-game chats to steal personal information, account credentials, or even money. Young users often have limited ability to recognise scams, making them

easy prey for identity thieves and fraudsters. Data breaches affecting children's personal information further amplify this risk. In recent years, breaches of student databases and learning platforms have exposed millions of children's records (Jang & Ko, 2023). Jang and Ko (2023) argue that children typically have little control over how their data is collected or used and lack the critical judgment to consent to complex terms.

Since the COVID-19 pandemic, society has become increasingly reliant on online meeting tools, transitioning from in-person business meetings, online classes, and social gatherings to virtual platforms. However, the widespread use of these services has also facilitated a new form of attack wherein perpetrators infiltrate and intentionally disrupt virtual meetings, commonly referred to as "Zoom bombing." Zoombombing is usually initiated by a legitimate participant in the meeting call (e.g., a student in an online lecture) who shares the meeting details and invites other community members to participate in a coordinated attack (Ling et al., 2021). Subsequently, the attackers may divulge details such as meeting passwords or personal information about the host. They then infiltrate the online meeting to torment participants, which may include sending hateful messages or displaying offensive or indecent images.

The impacts of online threats on children's mental health and well-being are severe. For example, children often suffer anxiety, depression, low self-esteem, academic problems, and even suicidal ideation (Samsudin et al., 2023). Given their limited cognitive maturity and digital experience, it is the responsibility of adults, particularly parents, to guide and educate them on cybersecurity awareness (Livingstone et al., 2015; Lee & Chae, 2007). This includes helping children recognise, evaluate, and respond appropriately to potential online risks.

Parents' Digital Literacy

Parenting in the digital age often evokes emotions of fear, confusion, and overwhelm. Cyber parenting extends beyond essential supervision to include educating and guiding children in the safe and effective use of technology. Cyber parenting is a continuous effort to recognise that parents must stay up-to-date on technological developments to guide their children effectively (Plowman, 2015). Parents must acquire the knowledge and skills to effectively use computers, smart devices, and the Internet while also understanding the associated risks (Livingstone et al., 2015). Parents should create a safe online environment by choosing devices and content suitable for their children's ages. In addition, implementing control measures such as active supervision and content filtering is needed. These responsibilities define the role of digital parents in ensuring their children's online safety and healthy media consumption habits (Mallik & Radwan, 2020).

The literature on parental digital literacy suggests that digitally literate parents are better equipped to navigate complex parental control settings, enabling them to install effective filters and monitoring tools that create a more secure online environment (Wisniewski et al., 2017). Children of parents with high digital literacy generally demonstrate stronger ethical awareness in digital interactions (Guo et al., 2024), mainly because their parents understand critical topics such as digital footprints and data privacy. This awareness helps these children to act more cautiously and responsibly online, while effective filters and monitoring tools further reduce their exposure to online risks (Barnes & Potter, 2020).

Some parents may rely on providing children with the latest gadgets to keep them occupied and avoid interruptions to their work (Brauchli et al., 2024; Chong et al., 2023), regardless of their digital literacy level. Consequently, both parents and children become absorbed in their respective devices, which can

lead to a lack of supervision and, in some cases, children misusing the Internet (Hidayat & Listiawati, 2018). Lou et al. (2010) found that parents with limited digital literacy often impose stricter controls on their children's online interactions. Meanwhile, digitally literate parents tend to place more trust in their children's online behaviour and provide less guidance, potentially due to their reliance on technical safeguards such as firewalls and security software. However, Yaman et al. (2021) challenge these findings, suggesting that digitally literate parents are not necessarily more trusting of their children's online activities. Instead, Yaman et al. (2021) emphasise that digital literacy tends to improve over time with experience.

Past studies have revealed that parents consistently express a need for information and guidance when online threats occur, emphasising the necessity of informed parental involvement (Tomczyk & Potyrała, 2021). As technology advances, the need for parents to adapt and enhance their skills becomes increasingly essential, as parents' knowledge can significantly influence children's digital competencies (Ayyash et al., 2024). Therefore, parents must continuously update their knowledge to guide their children effectively. However, studies indicate parents often have low knowledge or digital literacy, particularly in online interactions (Waldman-Levi et al., 2013; Mascheroni et al., 2018). This competence gap, where children surpass their parents in using digital technology, intensifies feelings of inadequacy within families. The gap in knowledge or literacy often causes parents to struggle to find information and intervene effectively. Ongoing research is needed to better understand the relationship between parents' knowledge of digital literacy and cyber parenting approaches.

Cyber Parenting Approaches

Parental supervision in preventing cyberbullying is associated with factors such as digital parenting awareness, active mediation, content-specific restrictive interventions, and overall supervision (Durak et al., 2024). Parents are aware of the potential threats associated with the Internet, but their awareness level remains moderate, which may not fully protect children from online threats (Ahmad et al., 2019). It is crucial to recognise that children's Internet usage can potentially lead to Online threats, and the parenting style practised by parents significantly influences this outcome (Kanan et al., 2018).

There are four main categories of parenting styles, which are: (1) authoritative, (2) authoritarian, (3) permissive/indulgent, and (4) neglectful parenting styles (Baumrind, 1991; Kuppens & Ceulemans, 2019). Authoritative parenting style is characterised by raising children on a reasonable basis. The parents are warm, treat their children with care, and are very supportive of their children. They also offered their children opportunities to do or act autonomously (Moreno-Luiz et al., 2019; Yusuf et al., 2020). In contrast, authoritarian parenting is characterised by high demands and low responsiveness (Hoskins, 2014). Parents believe their children must follow their rules and obey their decisions without question. Next is the permissive parenting style. It is characterised by high responsiveness but low demand (Baumrind, 1991). Based on previous studies, parents who apply a permissive parenting style do not or occasionally discipline their children and allow them to settle on significant choices without help from anyone else, with practically no rules or limiting standards (Benedetto & Ingrassia, 2021; Kanan et al., 2018). Meanwhile, neglectful parenting style is marked by low responsiveness and low demands, the least involved parenting style (Kanan et al., 2018). The parents gave their children freedom without educating them about the essential things they must follow.

The complexity of cyber parenting styles and their impact on children's Internet usage has become a focus of contemporary research. Parenting approaches play a pivotal role in determining how protected or vulnerable children are in cyberspace. A growing body of research shows that authoritative parenting

tends to be a protective factor for children's online safety (Gómez-Ortiz et al., 2018). In contrast, Gómez-Ortiz et al. (2018) also found that authoritarian or neglectful parenting styles can increase a child's vulnerability to online threats. Past studies indicate that an authoritative approach to cyber parenting tends to result in safer and more responsible Internet use among children (Yusuf et al., 2020). Similarly, an earlier study by Valcke et al. (2010) found that children of authoritarian and authoritative parents are less likely to experience cyberthreats. In contrast, children raised by permissive or neglectful parents are more susceptible to such activities as too much screen time and potential exposure to online risks (Lo et al., 2020).

Other research shows that boys and girls have different risks of facing online threats. Specifically, boys raised with lenient parenting are less likely to get involved in online threats. However, girls raised with strict parenting have a higher risk of engaging in online threats (Moreno-Ruiz et al., 2019). While these studies primarily examine parenting styles, their implications extend directly to children's cybersecurity awareness. Parenting that combines warmth with guidance tends to promote open communication, digital literacy, and responsible online habits in children, which may lead the children to develop critical thinking about online risks, understand privacy concerns, and engage in protective behaviours. Conversely, permissive or neglectful parenting often leaves children without sufficient support or oversight, which may limit their awareness of digital threats and reduce their preparedness to respond to them. Therefore, cyber parenting styles do not merely influence exposure to online risks but also shape the development of children's cybersecurity awareness and their capacity to navigate the digital world safely and responsibly.

Coping Strategies

Coping theory suggests two main categories: problem-focused and emotion-focused (Baker & Berenbaum, 2007; Folkman & Lazarus, 1988; Wechsler, 1995; Lai et al., 2012; Lazarus, 1993). Problem-focused coping addresses the root cause of the problem through actions aimed at rectifying the strained relationship between the individual and their surroundings (Folkman & Lazarus, 1988; Wechsler, 1995). This approach emphasises acting against problems for desirable outcomes (Green et al., 2010; Lazarus, 1993). In contrast, emotion-focused coping concentrates on managing emotions or stress without directly tackling the underlying problem. These strategies vary widely and may include venting emotions or seeking social support (Green et al., 2010), making them more challenging to define than problem-focused coping.

METHODOLOGY

This study employed qualitative research methods to gain a deeper understanding of the underlying issues related to cyber parenting in the context of children's exposure to online threats. This approach provided a rich and flexible framework to capture a range of insights into parents' experiences with online threats and their strategies for managing these challenges.

Data Collection

The initial phase of this study involved recruiting participants, specifically parents with experience handling online threats, through a Google Form distributed in collaboration with the Ministry of Higher Education. The Google Form includes a brief overview of the study's objectives, expectations, and eligibility requirements. A snowball sampling technique was used to broaden recruitment reach. Parents who are interested in participating were asked to provide their contact details for follow-up.

In total, 15 parents expressed interest in participating. However, five later withdrew, leaving 10 parents available for interview. The participants were assigned reference numbers P1, P2, and so on until P10. Interview sessions were scheduled via Webex, and participants received digital calendar invitations confirming their session times. Each interview lasted approximately 30 minutes to one hour, following a semi-structured format that allowed for flexibility in exploring emerging themes. The data were collected over 6 months, from April 2022 to October 2022.

Each session began with an introduction from the interviewer, followed by a brief overview of the study's purpose. The participants were informed of the interview ground rules and asked for consent to record the conversation to ensure ethical consideration for this study. They were assured that they could skip any questions they felt uncomfortable answering and that recordings would be deleted once the data was fully extracted and analysed. Once the participant agrees to the terms and conditions, the interview session starts. The interviewers then proceed with a series of pre-determined, open-ended questions. A preliminary set of questions was prepared, allowing flexibility to incorporate additional relevant questions during the interviews as needed. At the end of each interview, participants were thanked for their time and encouraged to reach out with any further questions or comments for the research team.

Data Analysis

Following the completion of the interview sessions, the next phase of the research involved transcription and coding of the data. The responses from nine of the 10 parents were analysed, as one interview was excluded due to incomplete data. Transcriptions were meticulously prepared to ensure an accurate representation of the interview content. Atlas.Ti was utilised for coding purposes. Two cycles of thematic coding were conducted to ensure the reliability of the analysis. In the first cycle, three coders developed an initial thematic framework using primarily deductive coding. In the second cycle, two independent coders engaged in discussions to refine and agree on suitable codes, combining both inductive and deductive approaches. Inductive coding involved identifying patterns and themes emerging directly from the data, while deductive coding applied predefined categories based on the existing literature and the research objectives.

Through iterative discussions, a comprehensive coding framework was developed to facilitate systematic qualitative data analysis. By adhering to these methodological procedures, the research aimed to ensure rigour, transparency, and reliability in the data collection and analysis processes, thereby enhancing the validity and trustworthiness of the study findings. Finally, the relationship based on the emerging theme is analysed and presented to answer the research questions. Table 1 includes the emerging themes from the analysis, guided by PMT. Upon the development of the coding framework and identification of key themes, the final stage of the analysis involved mapping the emergent categories onto the constructs of PMT. PMT was used to interpret the behavioural patterns of parents in responding to online threats experienced by their children.

The themes related to 'digital literacy' align with the 'Self-Efficacy' construct within PMT's Coping Strategies framework. This is because past research found that parents with high digital literacy skills feel more aware and capable of guiding their children's online activities (Fidan & Olur, 2023; Kalkim et al., 2024). Meanwhile, the 'Cyber Parenting Strategies' were aligned with the other PMT's Coping Strategy constructs, which encompass response efficacy and perceived response cost when dealing with children's online threats. Similarly, the themes under 'Threat Appraisal', including perceived severity and perceived vulnerability, were derived directly from parents' subjective evaluations of the risks

associated with their children's online behaviours and the consequences of online threats. By systematically linking these themes to PMT constructs, the study was able to explain how variations in parents' digital confidence, awareness of online threats, and parenting styles influenced their protective behaviours and coping mechanisms.

Table 1

Themes Emerged in the Analysis

Themes	Sub-themes	Descriptions
Parents' Digital Literacy	High	Digitally skilled and confident parents who can monitor, guide, and support their children online
	Moderate	Parents who have some digital literacy skills but are still learning. They often learn together with their children.
	Low	Parents who have limited digital knowledge and skills. Their children are usually more tech-savvy than they are.
Cyber Parenting Strategies	Authoritarian	Strict control over children's online activities, with little flexibility.
	Authoritative	Sets clear online rules while encouraging open communication and shared decision-making.
	Permissive	Gives children a lot of freedom online with little guidance.
Parents' coping strategies	Problem-focused coping	Parents actively solve online safety issues by taking clear actions to protect their children.
	Emotion-focused coping	Parents focus on managing their own emotions, often by seeking support or reducing stress.
Threat Appraisal	Perceived Severity	How seriously do parents think online threats are for their child.
	Perceived Vulnerability	How likely do parents think their child could become a target of online threats.
Coping Appraisal	Self-Efficacy	Parents' confidence in their ability to keep their children safe online.
	Response Efficacy	How effective parents believe their actions will be in reducing online risks.
	Response Cost	The effort or stress parents feel when trying to take protective actions.

The classification of parents' statements into 'Low', 'Moderate', or 'High' levels for each PMT construct was developed using a combined deductive–inductive approach. This process was guided by core PMT literature (Rogers, 1983; Maddux & Rogers, 1983) and following previous PMT studies in online safety contexts (e.g., Woon et al., 2005). For example, statements minimising potential consequences (e.g., describing online threats to their children as 'not a big deal') were coded as 'Low Perceived Severity', whereas statements acknowledging serious or lasting harm were coded as 'High'. The classification framework was refined iteratively by comparing theory-driven indicators with emergent themes from the actual interview data. This allowed the coding to remain theoretically anchored while responsive to parents' lived experiences (Terry et al., 2017; Braun & Clarke, 2006). To enhance consistency, all coded segments were cross-checked against the indicator table, and coding disagreements were discussed until consensus was reached. Representative quotes were selected to demonstrate how each level was operationalised, strengthening transparency and trustworthiness.

FINDINGS AND DISCUSSIONS

This section will present the findings of this study. The discussion of the findings and how they relate or contrast with similar existing research will also be presented to reveal the meaning of the findings.

Participants's Profile

The parents selected as respondents for this study were those whose children had been exposed to online threats. The affected children were predominantly from secondary schools, with two cases involving primary school pupils and another two cases involving college or university students. The online threats experienced ranged from account hacking and Zoom raids to incidents of cyberbullying. Notably, most of the children affected were male. Among the participating parents, three demonstrated high levels of digital literacy, while four were classified as having high cybersecurity awareness. Two parents with high digital literacy adopted an authoritarian parenting approach, imposing strict controls and restrictions on their children's online activities. In contrast, six parents employed an authoritative approach, which emphasised greater autonomy for their children while maintaining casual monitoring of their online behaviour. One parent reported using an authoritative approach with younger children, combined with a more permissive approach for older children.

Parents' Digital Literacy

Parents have various digital literacy levels, ranging from low to highly literate. In general, we found that the effect of parents' digital literacy on their children's tech-savviness reflects the methods parents use to understand, navigate, and interact with technology, particularly concerning Internet and computer use. The findings in Table 2 revealed diverse views among parents about their level of digital literacy. While some parents felt less digitally capable, others believed they were on par with or even more tech-savvy than their children.

Table 2

Evidence of Parents' Level of Digital Literacy

Level	Descriptions	Verbatims
High-Level	Enabled them to take a more proactive and informed approach to guiding their children's online activities	*"Regarding what's up to date, usually, it's my husband. Because it's his field, you know, he's a software engineer, so he's the one who knows the latest." (P7).*
Moderate Level	Parents who have embarked on a continuous learning journey, actively seeking advice from friends or older children	*"Usually, I will ask my older children because they are even more advanced. So, they are the ones who will monitor the younger siblings." (P4).*
Low-Level	Admit that their children's greater proficiency with digital platforms	*"They are indeed more proficient in matters related to smartphones, internet, and games." (P3).*

These findings reinforce the need for continuous, active parental involvement that goes beyond technical competence, ensuring children are supported in recognising and responding to online threats in real time. Parents need to consistently support the development of their children's digital literacy and cybersecurity awareness, equipping them to navigate online threats more effectively.

Parents' Digital Literacy as the Indicator for Self-Efficacy

In PMT, self-efficacy refers to a parent's confidence and beliefs in their ability to protect their children online (Rogers, 1975; Hwang et al., 2017). Research shows that digital literacy is a key factor that shapes this belief, whereby the parents who are more skilled with digital tools feel more competent to monitor, guide, and mediate their children's online activities (Fidan & Olur, 2023). Therefore, we argue that parents' digital literacy is an indicator of self-efficacy. For example, high-level digital literacy parents demonstrated high self-efficacy. Meanwhile, moderate-level digital literacy showed moderate self-efficacy. They weren't highly confident initially, but they built their skills by learning alongside their children, boosting their self-efficacy over time. Lastly, parents with low digital literacy skills felt less confident. Their children often surpassed them in tech knowledge, leading to uncertainty in taking protective actions. This is indicative of low self-efficacy.

Cyber Parenting Approaches

Following the interview analysis, three themes (as shown in Table 3) of parenting emerged: (1) trust but keeping an eye on things (Authoritative), (2) monitoring every step of the way (Authoritarian), and (3) freedom first, no worries here (Permissive). None of the parents adopts neglecting parenting.

Table 3

Cyber Parenting Approaches

Approaches	Descriptions	Verbatims
Authoritarian	Parents who enforce rules.	*"Before this, I installed a tracker in my kids' phones and monitor what they are watching and streaming" (P2).*
Authoritative	These parents give their children some freedom in managing their online activities.	*"I don't usually ask for passwords, but I will sometimes ask them to let me view their social media account" (P3).*
Permissive	Parents in this category face challenges in controlling their children's activities online, partly due to addiction.	*"For my two smaller kids, I really cannot control their online gaming activities. They just don't listen"(P6).*

Parental Coping Strategies in Response to Children's Online Threats

This study analysed the coping strategies of parents after online threat incidents by their kids. Parents employ several coping strategies, including seeking help, taking proactive action, and offering advice to their children. These coping strategies were then mapped with the three types proposed by Lazarus (1993). While parents demonstrated both problem-focused and emotion-focused coping strategies (as shown in Table 4) in response to online threats, there was no indication of appraisal-focused coping in the data.

Table 4

Coping Strategies

Strategy	Descriptions	Verbatims
Problem-focused coping	Reporting to the authority, engaged in collective discussion, implementing technical measures, and offering advice to the children.	*"After this incident, we parents from the same class spent 2-3 days discussing this matter." (P5)*
Emotion-focused coping	Retaliate against the cyberbullying.	*"I also replied to his comments before I closed the comments, you know... I said, 'My son is only 9 years old, why would he say something like this, right?" (P9)*

Interpreting Parenting Styles through the Lens of PMT

This section presents the interpretation of cyber parenting styles through the framework of PMT. Analysis of the interview data revealed distinct patterns in how parents assess and respond to online risks experienced by their children. These patterns correspond closely with the core constructs of PMT, illustrating how variations in parenting styles and digital literacy shape parental protective behaviour.

As outlined in the previous section, digital literacy is reflected in the 'Self-Efficacy' component of PMT, indicating parents' confidence in using digital tools to safeguard their children. Meanwhile, parenting styles and their related behaviours, such as the use of rules, discussions, and emotional reactions, are captured through the constructs of 'Threat Appraisal' and 'Coping Appraisal', which encompass perceived severity, vulnerability, response efficacy, and response cost. In addition, the parental coping strategies identified in the previous section can be situated within the PMT framework by aligning them with the coping appraisal process. In this context, parents' engagement in problem-focused and emotion-focused coping reflects their appraisal mechanisms for coping. Table 5 summarises key insights and evidence from the data, categorised according to each core PMT component. Each level (low/moderate/high) provides illustrative examples of parents' perceptions, behaviours, and confidence in managing digital threats, supported by direct quotes from participants.

Table 5

Key Insights from the Data According to the Core Components of PMT

PMT Constructs	Level	Key Insights from Findings	Verbatim Quotes
Threat Appraisal: Perceived Severity	Low	Minimal concern; belief that children are resilient or unlikely to be harmed.	No evidence of Low Perceived Severity
	Moderate	Some awareness of risk, but see occasional exposure as manageable.	*"Sometimes I do worry, but I feel it's okay because my child knows what to do." (P7)*
	High	Strong concerns about exposure to inappropriate content and online harassment; threats are seen as emotionally and psychologically damaging; regret for delayed action.	*"I get really scared. Especially when they're at the stage of growing up, it scares me. I'm really scared" (P6)*

(continued)

PMT Constructs	Level	Key Insights from Findings	Verbatim Quotes
Threat Appraisal: Perceived Vulnerability	Low	Believe children are tech-savvy and unlikely to be deceived.	*"My child knows more about IT than I do. I trust that they can take care of themselves." (P1)*
	Moderate	Concern about peer influence and social media exposure. But it is recognised as an inevitable part of growing up in the digital age.	*"What I'm worried about is the girl..the one who's in Year Five now.. It's because her TikTok account has 13,000 followers. But… so far, even though there are thousands of followers, from what I see, they're mostly school kids. Kids around her age. So it's okay, I guess" (P4)*
	High	Children with unsupervised or frequent online access are seen as highly vulnerable; girls are perceived to face greater risks; behavioural and emotional changes reinforce the perception.	*"I saw how my son changed emotionally after he was body-shamed." (P9)*
Coping Appraisal: Response Efficacy	Low	Doubtful about the effectiveness of their actions.	*"Even if we set rules, kids nowadays can bypass them. It's hard to control."(P6)*
	Moderate	Believe that a mix of rules and communication can work.	*"If you talk to them nicely, they'll usually listen." (P4)*
	High	Strong belief that monitoring and restrictions are effective; favour combining technical controls with open communication.	*"Monitoring, tracking apps, sharing passwords of their social media accounts, these methods work for us." (P2)*
Coping Appraisal: Response Cost	Low	Few barriers; rules are accepted by children.	*"My kids understand why they have to put away their phones by 10 pm, so it's not a problem." (P7)*
	Moderate	Some resistance from children, but it is manageable.	*"If he plays too long, I just hide the phone. He won't get it for weeks. He'll throw a tantrum for about 5 to 10 minutes, I just endure it while he screams and cries. After that, he stops crying" (P9)*
	High	High emotional toll, conflict, stress, and struggle with enforcement.	*"When I install the app, they'll argue, 'how am I supposed to access it if the teacher gives homework', and so on….. It's tiring" (P6)*

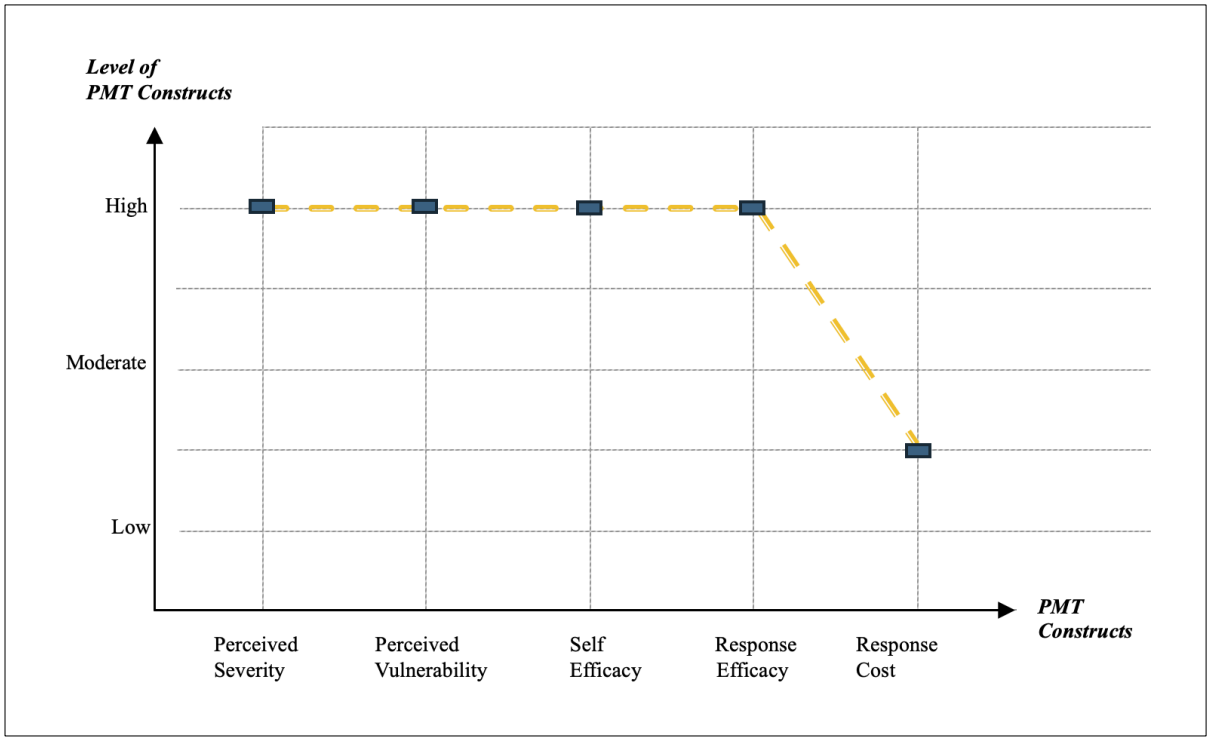
The next sub-sections will explain the relationship between parenting style and PMT components based on the findings that have been discussed in this section. These findings not only demonstrate the diversity of parental experiences and strategies but also offer a nuanced understanding of how digital literacy, or in PMT's context, self-efficacy, influences parental strategies for mitigating online threats and enhancing children's cybersecurity awareness and digital literacy.

Authoritarian Parenting: High Threat and Strong Coping Appraisal

Authoritarian parents reflected high threat appraisal, perceiving online risks as both severe and their children as highly vulnerable, especially in cases involving scams, data breaches, or stranger contact. These parents typically had high digital literacy, giving them strong self-efficacy, and they strongly believed in the effectiveness of strict interventions, which denotes high response efficacy. Their coping strategies included using surveillance tools, enforcing curfews, and monitoring device activity. Some parents took the initiative to attend parenting seminars to prepare their children to face online threats. They also made efforts to explain the dangers of these threats to their children regularly. These actions were taken with low to moderate concern for response cost, where parents were willing to endure emotional tension or conflict if it meant protecting their children. From the PMT lens, authoritarian parenting styles reflect a high threat–high coping profile, which PMT predicts will produce strong protective behaviours, not only to the parents but also their children. These parents engaged in strict problem-focused coping, acting decisively and proactively to reduce perceived risks, indirectly increasing the children's digital literacy in facing online threats. Figure 1 illustrates the pattern observed in authoritarian parents in this study.

Figure 1

Trends in Authoritarian Parenting Styles Based on PMT Components



Our findings are supported by Hwang et al. (2017), who confirm that authoritarian parenting is associated with high perceived severity, high self-efficacy, and strong belief in the effectiveness of mediation strategies (high response efficacy). In their study, authoritarian parents tend to adopt restrictive and active mediation strategies when they believe their children are vulnerable to online threats and that their interventions can mitigate these threats.

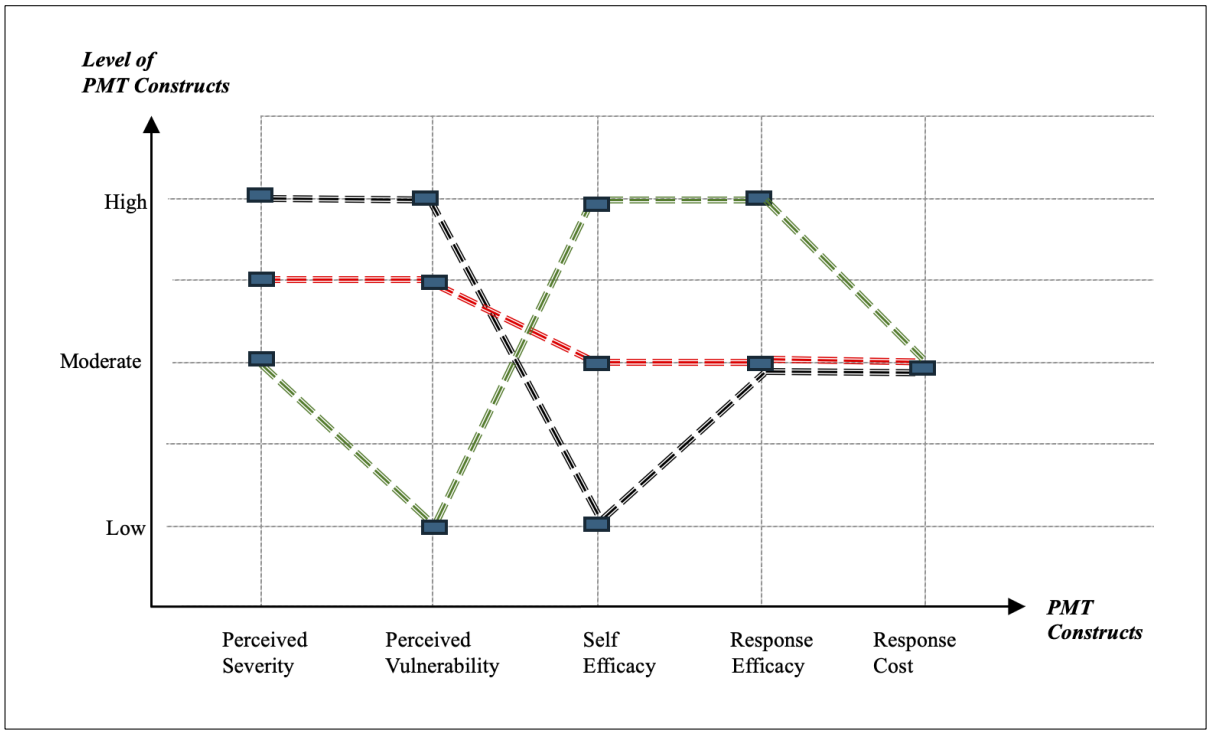
The findings are also consistent with Sciacca et al. (2022), who found that parental concerns about online risks and digital literacy skills drove restrictive mediation. Sciacca et al. argue that the authoritarian parents who are digitally literate are usually more proactive and confident in using strict strategies like monitoring and restrictions. However, Sciacca's findings also suggest that overly restrictive mediation without clearly explaining it to the children is likely to reduce children's digital literacy and resilience. This contrasts slightly with the assumption that all authoritarian strategies work well for children. Nonetheless, in our study, we found that the children were generally receptive to parental monitoring or restrictions, as the authoritarian parents balanced their strict monitoring by explaining their reasons and educating the children about the risks of digital spaces. This approach not only encouraged safer online behaviour but also fostered mutual understanding.

Authoritative Parenting: Balanced Threat and Coping Appraisal

Parents with an authoritative parenting style trust their judgment while maintaining awareness. This study found that while these parents demonstrated characteristics of authoritative parenting, their digital literacy skills (Self-Efficacy) varied significantly (as shown in Figure 2), which influenced how they assessed online threats and their coping responses, as conceptualised in PMT.

Figure 2

Trends in Authoritative Parenting Styles at Varying Levels of Self-Efficacy within the PMT



Legends:

Authoritative Parents with High Level Self-Efficacy (Digital Literacy)

Authoritative Parents with Medium Level Self-Efficacy (Digital Literacy)

Authoritative Parents with Low Level Self-Efficacy (Digital Literacy)

Parents with high self-efficacy, typically those with advanced IT skills, tended to perceive online threats as moderately severe but believed their children had low vulnerability. These parents exhibited high response efficacy and viewed the cost of protective actions as moderate, indicating confidence in their ability to manage risks effectively without being overly alarmed. In contrast, parents with moderate self-efficacy showed greater concern, appraising both threat severity and vulnerability as moderate to high, yet maintained a reasonable belief in the effectiveness of their coping strategies, with response costs still perceived as manageable.

Meanwhile, parents with low self-efficacy, often those with limited digital skills, perceived online threats as highly severe and their children as highly vulnerable. Although they believed that certain protective responses could be effective, their confidence in implementing these strategies was only moderate, and they perceived similar moderate levels of effort or cost required. These patterns suggest that digital literacy plays a critical role in shaping not only parents' digital competence but also their cognitive and emotional responses to their children's online safety. Some of the authoritative parents showed moderate self-efficacy, either due to their existing digital literacy skills or through co-learning with their children. They also have a moderate to high threat appraisal. This study is in line with Hwang et al. (2017), who found that authoritative parents normally had higher perceived severity and high self-efficacy.

The response efficacy demonstrated by authoritative parents in this study was found to be moderate to high. These parents believed that strategies such as guidance, trust-building, and occasional monitoring could help mitigate online risks. However, they did not consistently express full confidence that such measures would be entirely effective in preventing online threats. This contrasts with the findings of Hwang et al. (2017), who reported that authoritative parenting was positively associated with high response efficacy. Parents in their study appeared more assured that their protective and intervention efforts would successfully protect their children in the digital environment.

Additionally, we found that response costs (e.g., emotional strain, time investment, or effort required to implement protective measures) appeared to be moderate or manageable for authoritative parents, regardless of their self-efficacy level. This may explain their continued use of balanced strategies. This finding supports the study by Sciacca et al. (2022), which claims that authoritative parents often employ a combination of active and restrictive mediation. This reinforces the view that these parents are actively involved in discussing the digital risks with their children while maintaining a flexible and supportive approach.

Permissive Parenting: High Threat, Low Coping Appraisal

Interestingly, despite their low digital literacy, permissive parents showed high perceived severity and vulnerability, especially when their children were exposed to inappropriate content or excessive gaming. This shows that the parents are aware of the risk that comes when letting their kids use the Internet without supervision. However, unlike authoritarian parents, they exhibited low self-efficacy, often feeling incapable of using or managing digital tools effectively.

Parents with permissive styles also showed low response efficacy. They often doubt whether their actions in setting limits will be effective. Additionally, they experienced high response costs, such as emotional exhaustion, guilt over restricting other children's access, or fear of child resistance. These barriers hindered consistent protective action. As a result, their coping strategies were frequently emotion-focused or avoidant, including relying on external sources to solve the problem, such as teachers or peers (Chen et al., 2023).

From the PMT perspective, permissive parenting thus aligns with a high-threat–low-coping profile, which tends to result in weaker protective behaviours, which could impact the children's awareness of online threats. These findings align with prior studies indicating that permissive parenting is negatively associated with effective digital mediation and positively associated with children's online vulnerabilities (Hwang et al., 2017; Teimouri, 2015). Figure 3 shows the trends in permissive parenting styles.

Figure 3

Trends in Permissive Parenting Styles Based on PMT Components

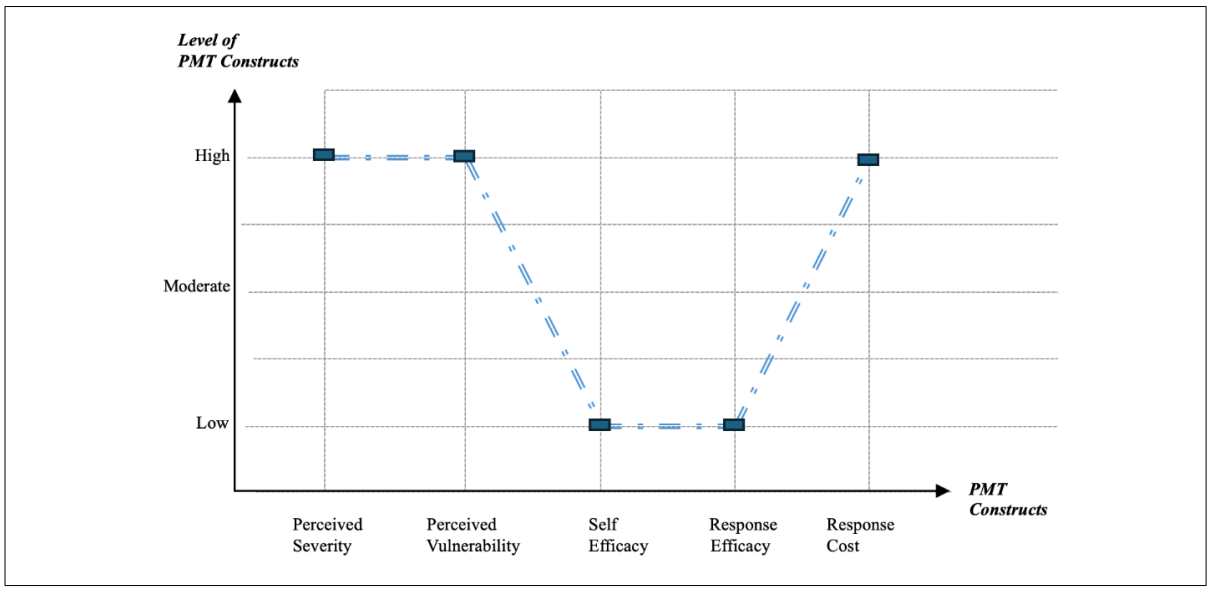


Figure 4

How PMT Components Relate to Parental Digital Literacy and Coping Strategies

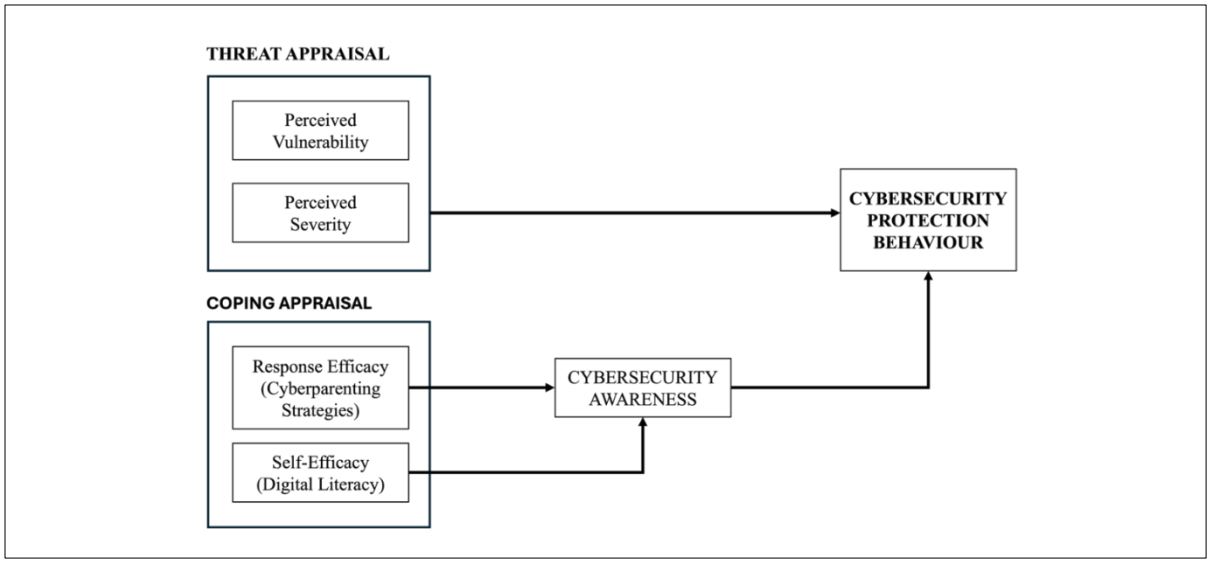


Figure 4 shows how PMT components (threat appraisal and coping appraisal) relate to parental digital literacy (self-efficacy) and coping strategies. It highlights critical gaps where targeted support, such as

digital literacy training or structured parenting guidance, could empower less responsive parents to become more effective digital guardians and consequently help to boost the children's cybersecurity awareness.

Overall, the study reveals that parental responses to online threats are shaped by both awareness and confidence in managing risk. When threat appraisal and coping appraisal are both high, parents are more likely to implement problem-focused coping strategies. However, when self-efficacy is low and response costs are high, parents may fall back on emotion-focused coping or adopt more lenient parenting approaches, which do not effectively help children build digital literacy and cybersecurity awareness. These findings support the work of Zhang et al. (2022), who emphasised the critical role of digital self-efficacy and parenting style in promoting cyber safety behaviours. Beyond immediate protection, these parental strategies play a formative role in cultivating children's cybersecurity awareness and skills.

Parents with high digital literacy skills and structured mediation approaches are more likely to engage in open discussions about online risks, demonstrate safe online behaviours, and involve children in reflective decision-making processes. As shown by Teimouri et al. (2015), such engagement enhances children's risk perceptions and self-efficacy, equipping them to apply security practices independently and responsibly. Moreover, consistent modelling of proactive behaviours or coping strategies, such as reporting incidents, managing privacy settings, or evaluating digital content, may translate into tacit learning experiences for children, which build their confidence and autonomy in digital environments. Ultimately, cyber parenting is not merely a protective shield; it functions as an informal but powerful educational process through which children acquire essential digital competencies and internalise cyber-safe norms.

CONCLUSION

The findings of this study reflect that parents' digital literacy and parenting styles significantly shape how they perceive and respond to cyberthreats involving their children. Using PMT as the theoretical guide, we identified distinct differences in threat and coping appraisals across authoritarian, authoritative, and permissive parenting styles. Authoritarian parents displayed strong self-efficacy and employed strict, problem-focused strategies. This is due to their high level of digital literacy. Meanwhile, authoritative parents balanced digital autonomy with some level of freedom, using flexible and collaborative approaches. In contrast, the permissive parents showed lower self-efficacy and relied more on emotional or avoidant coping due to uncertainty and perceived response costs, although they managed to evaluate the threats.

PMT explains parental decision-making and the importance of interventions that enhance self-efficacy in protecting their children. Theoretically, this study contributes by extending PMT in the cyber parenting domain. It reveals that even parents with low digital literacy and self-efficacy are aware of the risks associated with online engagement. Furthermore, parents' varying levels of digital literacy influence how they manage to mitigate online threats targeting their children. This study also refines the application of PMT by showing the interplay between perceived severity, vulnerability, self-efficacy, and response efficacy in real-life parenting practices.

From a practical perspective, the study provides important insights for educators, policymakers, and organisations working to support parents in providing safe online environments to their children. The findings suggest that interventions should focus not only on building parents' digital literacy but also

on boosting their confidence in handling cyber incidents. Programs that promote digital co-learning between parents and children, provide accessible tools for monitoring and guidance, and address the emotional strain of digital parenting may be especially effective in helping families manage online threats. Parents' digital literacy and parenting approaches not only shape the precautions families take online but also profoundly influence how children learn about and internalise cyber-safe behaviour. In particular, parents who themselves possess strong ICT skills can model and teach safe practices (for example, demonstrating how to verify information or configure privacy settings), so that children acquire these competencies indirectly.

In future, there is a need to proceed with research that analyses how digital parenting behaviours evolve and how they influence children's online safety, risk-taking, and resilience. It is also important to examine how cultural, gender and socioeconomic factors affect digital self-efficacy and parenting styles. More participants from diverse educational backgrounds and household types should be included to yield more conclusive findings. It is hoped this research area will be an ongoing effort as online threats targeting children continue to evolve. In future, there is a need to proceed with research that analyses how digital parenting behaviours evolve and how they influence children's online safety, risk-taking, and resilience. It is also important to examine how cultural, gender, and socioeconomic factors affect digital self-efficacy and parenting styles, as these can significantly shape how families respond to online threats.

More participants from diverse educational backgrounds and various types of households should be included to enable more conclusive and generalisable findings. It is hoped this research area will be an ongoing effort, especially as online threats targeting children continue to evolve in complexity and frequency. Therefore, parental efforts in securing the online environment for future generations are essential, not only to reduce exposure to risks but also to enhance children's cybersecurity awareness. By fostering early understanding of online threats and promoting protective behaviours, parents can help build a generation of young users who are more informed, resilient, and capable of navigating digital spaces responsibly.

ACKNOWLEDGMENTS

This research was funded by a matching grant from Universiti Utara Malaysia (UUM) and Universitas Pasundan (UNPAS), Indonesia (Kod S/O: 21559).

REFERENCES

Ahmad, N., Arifin, A., Mokhtar, U. A., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental awareness of cyber threats using social media. *Malaysian Journal of Communication, 35*(2), 485–498. https://doi.org/10.17576/jkmjc-2019-3502-29

Aiken, M., Davidson, J., & Amann, P. (2016). *Youth pathways into online threats*. Paladin Capital Group.

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2024). Cybersecurity education and awareness among parents and teachers: A survey of Bahrain. *IEEE Access, 12*, 86596–86617. https://doi.org/10.1109/access.2024.3416045

Baker, J. P., & Berenbaum, H. (2007). Emotional approach and problem-focused coping: A comparison of potentially adaptive strategies. *Cognition and Emotion, 21*(1), 95–118. https://doi.org/10.1080/02699930600562276

Balogh, K. N., Mayes, L. C., & Potenza, M. N. (2013). Risk-taking and decision-making in youth: Relationships to addiction vulnerability. *Journal of Behavioural Addictions, 2*(1), 1–9. https://doi.org/10.1556/jba.2.2013.1.1

Barnes, R., & Potter, A. (2020). Sharenting and parents' digital literacy: An agenda for future research. *Communication Research and Practice, 7*(1), 1-15. https://doi.org/10.1080/22041451.2020.1847819

Basir, E. K. (2024). Addressing social media challenges for children. *Bernama*. https://www.bernama.com/en/bfokus/news.php?current&id=2358825#:~:text=On%20Oct%2026%2C%20Communications%20Minister,groups%20on%20social%20media%20platforms

Baumrind, D. (1991). The influence of parenting style on adolescent competence and substance use. *The Journal of Early Adolescence, 11*(1), 56–95. https://doi.org/10.1177/0272431691111004

Benatov, J. (2019). Parents' feelings, coping strategies, and sense of parental self-efficacy when dealing with children's victimisation experiences. *Frontiers in Psychiatry, 10*, 700. https://doi.org/10.3389/fpsyt.2019.00700

Benedetto, L., & Ingrassia, M. (2021). Digital parenting: Raising and protecting children in media. In *Parenting: Studies by an ecocultural and transactional perspective* (p. 127). https://doi.org/10.5772/intechopen.92579

Bernama. (2022). Almost RM600 million was lost to online threats in 2022. *Bernama*. https://www.bernama.com/en/general/news.php?id=2156221

Borwell, J., Jansen, J., & Stol, W. (2025). The psychological impact of online threat victimisation: The importance of personal and circumstantial factors. *European Journal of Criminology*, 14773708241312506. https://doi.org/10.1177/14773708241312506

Brauchli, V., Sticca, F., Edelsbrunner, P., von Wyl, A., & Lannen, P. (2024). Are screen media the new pacifiers? The role of parenting stress and parental attitudes for children's screen time in early childhood. *Computers in Human Behaviour, 152*, 108057. https://doi.org/10.1016/j.chb.2023.108057

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Brewer, R., Cale, J., Goldsmith, A., & Holt, T. (2018). Young people, the Internet, and emerging pathways into criminality: A study of Australian adolescents. *International Journal of Cyber Criminology, 12*(1), 115–132. https://doi.org/10.5281/zenodo.1467853

Chang, V., Golightly, L., Xu, Q. A., Boonmee, T., & Liu, B. S. (2023). Cybersecurity for children: An investigation into the application of social media. *Enterprise Information Systems, 17*(11). https://doi.org/10.1080/17517575.2023.2188122

Chen, H., Chen, Y., & Chen, J. (2024). Protecting teenagers' gaming privacy: The roles of parental mediation, platform protection, and risky encounters. *Behaviour & Information Technology, 43*(14), 3578-3591. https://doi.org/10.1080/0144929X.2023.2285941

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). *Application of protection motivation theory to the adoption of protective technologies.* In 2009 42nd Hawaii International Conference on System Sciences (pp. 1–10). IEEE. https://doi.org/10.1109/hicss.2009.74

Chong, S. C., Teo, W. Z., & Shorey, S. (2023). Exploring the perception of parents on children's screentime: A systematic review and meta-synthesis of qualitative studies. *Pediatric Research, 94*(3), 915–925. https://doi.org/10.1038/s41390-023-02555-9

Clarke, V., & Braun, V. (2014). Thematic analysis. *In Encyclopedia of Critical Psychology* (pp. 1947-1952). Springer. http://dx.doi.org/10.1080/17439760.2016.1262613

Conner, M., & Norman, P. (2015). *Predicting and changing health behaviour*. McGraw-Hill Education. http://ci.nii.ac.jp/ncid/BB04317870

Dodge, C. E., Fisk, N., Burruss, G. W., Moule Jr., R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy, 22*(4), 849–868. https://doi.org/10.1111/1745-9133.12641

Durak, A., Durak, H. Y., Saritepeci, M., & Dilmaç, B. (2024). Examining the factors affecting parental supervision in cyberbullying prevention: Demographics, parental mediation, and digital parenting awareness. *Families in Society, 106*(1), 176–194. https://doi.org/10.1177/10443894231225793

Elsaesser, C., Russell, B., Ohannessian, C. M., & Patton, D. (2017). Parenting in a digital age: A review of parents' role in preventing adolescent cyberbullying. *Aggression and Violent Behaviour, 35*, 62–72. https://doi.org/10.1016/j.avb.2017.06.004

Federal Bureau of Investigation. (2024, January 16). *Sextortion: A growing threat targeting minors*. FBI Miami Field Office. https://www.fbi.gov/contact-us/field-offices/miami/news/sextortion-a-growing-threat-targeting-minors

Fidan, N. K., & Olur, B. (2023). Examining the relationship between parents' digital parenting self-efficacy and digital parenting attitudes. *Education and Information Technologies*, *28*(11), 15189-15204. https://doi.org/10.1007/s10639-023-11841-2

Folkman, S., & Lazarus, R. S. (1988). Coping as a mediator of emotion. *Journal of Personality and Social Psychology, 54*(3), 466–475. https://doi.org/10.1037/0022-3514.54.3.466

Gómez-Ortiz, O., Romera, E. M., Ortega-Ruiz, R., & Del Rey, R. (2018). Parenting practices as risk or preventive factors for adolescent involvement in cyberbullying: Contribution of children and parent gender. *International Journal of Environmental Research and Public Health, 15*(12), 2664. https://doi.org/10.3390/ijerph15122664

Green, D. L., Choi, J. J., & Kane, M. N. (2010). Coping strategies for victims of crime: Effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping. *Journal of Human Behaviour in the Social Environment, 20*(6), 732–743. https://doi.org/10.1080/10911351003749128

Guo, S., Xu, J., Wang, M., Akezhuoli, H., Zhou, X., & Lu, J. (2024). The effects of parent-child separation on the digital literacy of children and adolescents: A bidirectional perspective study. *Heliyon, 10*(10), e22695. https://doi.org/10.1016/j.heliyon.2024.e31113

Hassan, S., Ahmad, R., Katuk, N., Ghazali, N. N., Aripin, J. A., & Ali, F. (2024). Staying one step ahead: Exploring protection motivation theory to combat cyber-fraud among e-services users. *Procedia Computer Science, 234*, 1364-1371. https://doi.org/10.1016/j.procs.2024.04.011

Hidayat, M. L., & Listiawati, V. (2018). *The urgency of parents' digital literacy to prevent their children from harmful effects of smart-mobile devices.* In Proceedings of the International Conference on Child-Friendly Education, (Vol. 4, pp. 618–624).

Hong, J. S., Kim, D. H., Thornberg, R., Kang, J. H., & Morgan, J. T. (2018). Correlates of direct and indirect forms of cyberbullying victimisation involving South Korean adolescents: An ecological perspective. *Computers in Human Behavior, 87*, 327–336. https://doi.org/10.1016/j.chb.2018.06.010

Hoskins, D. H. (2014). Consequences of parenting on adolescent outcomes. *Societies, 4*(3), 506–531. https://doi.org/10.3390/soc4030506

Hwang, Y., Choi, I., Yum, J. Y., & Jeong, S. H. (2017). Parental mediation regarding children's smartphone use: Role of protection motivation and parenting style. *Cyberpsychology, Behavior, and Social Networking, 20*(6), 362–368. https://doi.org/10.1089/cyber.2016.0555

Jang, Y., & Ko, B. (2023). Online safety for children and youth under the 4Cs framework—A focus on digital policies in Australia, Canada, and the UK. *Children*, *10*(8), 1415. https://doi.org/10.3390/children10081415

Kalkim, A., Korkmaz, E. K., & Toraman, A. U. (2024). Examining the relationship between digital parenting self-efficacy and digital parenting awareness of early adolescents' parents. *Journal of Pediatric Nursing*, *78*, 1-6. https://doi.org/10.1016/j.pedn.2024.05.028

Kanan, N., Arokiasamy, L., & Ismail, M. R. (2018). *A study on parenting styles and parental attachment in overcoming internet addiction among children*. In SHS Web of Conferences, (Vol. 56, p. 2002). EDP Sciences. https://doi.org/10.1051/shsconf/20185602002

Katz, I., Lemish, D., Cohen, R., & Arden, A. (2019). When parents are inconsistent: Parenting style and adolescents' involvement in cyberbullying. *Journal of Adolescence, 74*, 1–12. https://doi.org/10.1016/j.adolescence.2019.04.006

Kuppens, S., & Ceulemans, E. (2019). Parenting styles: A closer look at a well-known concept. *Journal of Child and Family Studies, 28*(1), 168–181. https://doi.org/10.1007/s10826-018-1242-x

Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*(2), 353–363.

Lazarus, R. S. (1993). Coping theory and research: Past, present, and future. *Psychosomatic Medicine, 55*(3), 234–247. https://doi.org/10.1016/j.dss.2011.09.002

Lazarus, R. S., & Folkman, S. (1987). Transactional theory and research on emotions and coping. *European Journal of Personality, 1*(3), 141–169. https://doi.org/10.1002/per.2410010304

Lee, S. J., & Chae, Y. G. (2007). Children's Internet use in a family context: Influence on family relationships and parental mediation. *Cyberpsychology & Behavior*, *10*(5), 640-644. https://doi.org/10.1089/cpb.2007.9975

Ling, C., Balcı, U., Blackburn, J., & Stringhini, G. (2021). *A first look at zoombombing*. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 1452–1467). IEEE. https://doi.org/10.1109/sp40001.2021.00061

Livingstone, S., & Helsper, E. J. (2008). Parental mediation of children's internet use. *Journal of Broadcasting & Electronic Media*, *52*(4), 581-599. https://doi.org/10.1080/08838150802437396

Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S., & Lagae, K. (2015). *How parents of young children manage digital devices at home: The role of income, education and parental style*. European Commission Joint Research Centre.

Lo, B. C. Y., Lai, R., Ng, T. K., & Wang, H. (2020). Worry and permissive parenting in association with the development of internet addiction in children. *International Journal of Environmental Research and Public Health, 17*(21), 7722. https://doi.org/10.3390/ijerph17217722

Lou, S. J., Shih, R. C., Liu, H. T., Guo, Y. C., & Tseng, K. H. (2010). The influences of the sixth graders' parents' internet literacy and parenting style on internet parenting. *Turkish Online Journal of Educational Technology-TOJET, 9*(4), 173–184.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Mallik, C. I., & Radwan, R. B. (2020). Adolescent victims of cyberbullying in Bangladesh-prevalence and relationship with psychiatric disorders. *Asian Journal of Psychiatry, 48*. https://doi.org/10.1016/j.ajp.2019.101893

Manoharan, S., Katuk, N., Hassan, S., & Ahmad, R. (2022). To click or not to click the link: the factors influencing internet banking users' intention in responding to phishing emails. *Information & Computer Security*, *30*(1), 37-62. https://doi.org/10.1108/ics-04-2021-0046

Marret, M. J., & Choo, W. Y. (2017). Factors associated with online victimisation among Malaysian adolescents who use social networking sites: A cross-sectional study. *BMJ Open*, *7*(6), e014959. https://doi.org/10.1136/bmjopen-2016-014959

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and online threat in general. *Computers in Human Behaviour*, *92*, 139-150. https://doi.org/10.1016/j.chb.2018.11.002

Mascheroni, G., Ponte, C., & Jorge, A. (2018). *Digital parenting: The challenges for families in the digital age.* Nordicom, University of Gothenburg.

Moreno–Ruiz, D., Martínez–Ferrer, B., & García–Bacete, F. (2019). Parenting styles, cyberaggression, and cybervictimization among adolescents. *Computers in Human Behaviour*, *93*, 252–259. https://doi.org/10.1016/j.chb.2018.12.031

Okeke, C. V., Obi-Nwosu, H., & Onuoha, O. C. (2024). Parental styles and moral disengagement as predictors of attitude towards online threat among undergraduates. *Zik Journal of Multidisciplinary Research, 7*(1), 207-222.

Pazarcikci, F. (2024). Risk factors for technology addiction in young children ages 2–5 years. *Journal of Pediatric Nursing*, *78*, e141-e147. https://doi.org/10.1016/j.pedn.2024.06.029

Plowman, L. (2015). Researching young children's everyday uses of technology in the family home. *Interacting with Computers*, *27*(1), 36–46. https://doi.org/10.1093/iwc/iwu031

Razali, N. A., & Nawang, N. I. (2022). An overview of the legal framework governing cyberbullying among children in Malaysia. *IIUMLJ*, *30*, 207. https://doi.org/10.31436/iiumlj.v30iS1.704

Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In: Cacioppo, J. and Petty, R. (Eds.), *Social psychophysiology*, 153-177, Guilford Press. https://ci.nii.ac.jp/naid/10017980757

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of Health Behavior Research 1: Personal and Social Determinants* (pp. 113–132). Springer. https://doi.org/10.1093/her/1.3.153

Rubis, A. B. (2024). *Successful strategies used by health care business managers to reduce data breaches* [Unpublished doctoral dissertation]. Walden University.

Sabillon, R., Cano, J. J., & Serra-Ruiz, J. (2016). Online threat and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165-176.

Samsudin et al. (2023). Prevalence of cyberbullying victimisation and its association with family dysfunction, health behaviour and psychological distress among young adults in urban Selangor, Malaysia: A cross-sectional study. *BMJ open*, *13*(11), e072801. https://doi.org/10.1136/bmjopen-2023-072801

Sciacca, B., Laffan, D. A., O'Higgins Norman, J., & Milosevic, T. (2022). Parental mediation in pandemic: Predictors and relationship with children's digital skills and time spent online in Ireland. *Computers in Human Behavior, 127*, 107081. https://doi.org/10.1016/j.chb2021.107081

Shin, W., & Lwin, M. O. (2022). Parental mediation of children's digital media use in high digital penetration countries: Perspectives from Singapore and Australia. *Asian Journal of Communication, 32*(4), 309–326. https://doi.org/10.1080/01292986.2022.2026992

Steinberg, L. (2008). A social neuroscience perspective on adolescent risk-taking. *Developmental Review, 28*(1), 78–106. https://doi.org/10.1016/j.dr.2007.08.002

Teimouri, M. (2015). *An integrated model to reduce online risks for children* [Unpublished doctoral dissertation]. Universiti Putra Malaysia.

Terry, G., Hayfield, N., Clarke, V., & Braun, V. (2017). Thematic analysis. *The SAGE Handbook of Qualitative Research in Psychology, 2*(17-37), 25.

Tomczyk, Ł., & Potyrała, K. (2021). Parents' knowledge and skills about the risks of the digital world. *South African Journal of Education, 41*(1). https://doi.org/10.15700/saje.v41n1a1833

UNICEF. (n.d.). *Protecting children online*. https://www.unicef.org/protection/violence-against-children-online

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

Waldman-Levi, R., Finzi-Dottan, R., & Weintraub, N. (2013). Attachment security and parental perception of competency among abused women in the shadow of PTSD and childhood exposure to domestic violence. *Journal of Child and Family Studies, 2*, 57–65. https://doi.org/10.1007/s10826-013-9813-3

Wechsler, B. (1995). Coping and coping strategies: A behavioural view. *Applied Animal Behaviour Science, 43*(2), 123–134. https://doi.org/10.1016/0168-1591(95)00557-9

Wegener, D. T., Petty, R. E., & Klein, D. J. (1994). Effects of mood on high elaboration attitude change: The mediating role of likelihood judgments. *European Journal of Social Psychology, 24*(1), 25–43. https://doi.org/10.1002/ejsp.2420240103

We Protect Global Alliance (2024). *The rise of sextortion and responses to a growing crime.* WeProtect Global Alliance. https://www.weprotect.org/thematic/sextortion/

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies, 98*, 95-108. https://doi.org/10.1016/j.ijhcs.2016.09.006

Wisniewski, P., Ghosh, A. K., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). *Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?* In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (pp. 51-69). https://doi.org/10.1145/2998181.2998352

Woon, I., Tan, G. W., & Low, R. (2005). *A protection motivation theory approach to home wireless security*. Proceedings of the 26th International Conference on Information Systems.

Yaman, F., Çubukçu, A., Küçükali, M., & Yurdakul, I. K. (2021). An investigation of parents' use of digital media. *Shanlax International Journal of Education, 10*(1), 76–88. https://doi.org/10.34293/education.v10i1.4327

Yusuf, M., Witro, D., Diana, R., Santosa, T. A., & Jalwis, J. (2020). Digital parenting to children using the internet. *Pedagogik Journal of Islamic Elementary School, 3*(1), 1–14. https://doi.org/10.24256/pijies.v3i1.1277

Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. *Frontiers in Public Health, 9*. https://doi.org/10.3389/fpubh.2021.634909