

THE UNIVERSITY OF QUEENSLAND

AUSTRALIA

Knowledge, control, and strangers: An analysis of resources for preventing self-generated imagery

by Shakira Memorey

School of Electrical Engineering and Computer Science,
The University of Queensland

Submitted for the partial fulfillment of the degree of Master of Cyber Security (Cyber Criminology)

May 2025

Assessable word count: [11,049]

Total word count: [17,004]

Contents

Acknowledgements	4
Abstract	5
Abbreviations	6
Chapter 1: Introduction	7
Chapter 2: Literature Review	11
Online child sexual exploitation offences	11
Online grooming offences	11
Online child sexual abuse material offences	12
Online sextortion offences against minors	12
The overlaps between grooming, CSAM, and sextortion	13
Impacts of victimisation	13
Factors influencing how young people use the internet	14
Developmental and cognitive factors	14
Social factors	15
The need for effective OCSEA prevention	16
Primary prevention	17
Effective and ineffective messaging for primary prevention resources	17
Theoretical framework: Protection motivation theory	18
Literature summary	19
Chapter 3: Data & Methodology	21
Data Collection	21
Data Analysis: Inductive Thematic Analysis	24
Limitations	26
Ethical Considerations	26
Chapter 4: Results	27
Theme 1: Knowledge is power	27
Sub-theme: Education and information are empowering	27
Sub-theme: Conversations break the stigma	29
Sub-theme: Beware of proactive and reactive red flags	30
Theme 2: To control or not to control?	32
Theme 3: Stranger, friend, or predator?	35
Theme 4: Using social media and online gaming for offending	37
Sub-theme: Using social media and online gaming to initiate contact	37

Sub-theme: Using social media and online gaming for identity obfuscation	38
Theme 5: Offenders transition across platforms throughout offending	39
Chapter 5: Discussion	41
Key findings as applied to developmental, cognitive, and social factors	41
Implications for future resource development	44
Implications for future research	45
Chapter 6: Conclusion	47
References	48
Appendices	60
Appendix A: Search terms	60
Appendix B: Websites selected to search for resources	62
Appendix C: List of analysed resources	63

Acknowledgements

Firstly, I want to thank my academic supervisor, Dr. Jonah Rimer, for the guidance, support, and encouragement provided throughout not only this project, but the classes which led me to taking this research journey. Your feedback and insights throughout this project were invaluable for the final output.

I would like to thank Ashley Carvalho and Dannielle Kelly from the International Centre for Missing and Exploited Children Australia for providing me with the opportunity to complete this project alongside an organisation making significant contributions to child protection. Ashley, I truly appreciated the advice and ideas shared throughout the completion of this project and I hope the findings are helpful for ICMEC Australia's work.

I would like to thank my work colleagues and friends, Mandy, Barbara, and Justin, for providing me with support, encouragement, and scheduling flexibility throughout my studies. The supportive work environment truly made a significant difference.

Finally, my sincere thanks go to Jordon, Jessica, Carlene, Lara, Isobel, Raphael, Lisa, and Sam for supporting me throughout all my university studies. Your unwavering support, the many sweet treat runs, and laughs got me through the intense study sessions.

Abstract

Online child sexual abuse and exploitation (OCSEA) has been exacerbated by the increasing presence of young people (YP) on the internet. Online grooming, child sexual abuse material (CSAM), and sextortion offenders take advantage of young peoples' presence in online spaces to receive self-generated child sexual abuse material (SG-CSAM) from victims. Recent increases in SG-CSAM have highlighted the need for initiatives to prevent the exploitation of YP from occurring, rather than responding once it has already occurred. YP's use of the internet is shaped by developmental, cognitive, and social factors, and offenders capitalise on children's internet use behaviours for successful exploitation; but little research has explored how such factors are addressed by primary prevention resources for self-generated imagery. As such, this thesis explores how primary prevention resources for the self-generated aspects of online grooming, CSAM, and sextortion offences align or not with the developmental, cognitive, and social factors influencing how YP use the internet, as well as how the same resources align or not with offender technology use. Inductive thematic analysis was undertaken on 150 primary prevention resources aimed at YP under 18, parents, and carers from Australia, New Zealand, the United States of America, and the United Kingdom. Analysis revealed primary prevention resources position knowledge as powerful to increase online safety behaviours, and provide confusion about controlling child internet usage and who offenders are. Some resources align with factors influencing young peoples' internet use; however, more could be done to increase alignment. The resources also align with how offenders use technology for initiating contact, identity obfuscation, and transitioning across platforms throughout offending.

Abbreviations

Abbreviation	Description
ACCCE	Australian Centre to Counter Child Exploitation
AUS	Australia
CSAM	Child sexual abuse material
CSEA	Child sexual exploitation and abuse
D&C	Developmental and cognitive
ICMEC Australia	International Centre for Missing and Exploited Children Australia
ITA	Inductive Thematic Analysis
IWF	Internet Watch Foundation
NCMEC	National Centre for Missing and Exploited Children
NZ	New Zealand
OCSEA	Online child sexual exploitation and abuse
PFP CSAM	Perceived first-person child sexual abuse material
PMT	Protection Motivation Theory
SG-CSAM	Self-generated child sexual abuse material
UK	United Kingdom
USA	United States of America
WHO	World Health Organisation
YP	Young people

Chapter 1: Introduction

Online child sexual exploitation and abuse (OCSEA) offences have proliferated on a global scale due to the increased accessibility of interconnected communication technologies (Ali & Paash, 2022; Walsh et al., 2025). OCSEA is a form of child sexual abuse that encompasses a combination of components such as power imbalances, manipulation, coercion, deception, fraud, force, threats, exchange, or status between an offender and victim (Rimer, 2024). By incorporating technology and the internet when committing child sexual exploitation and abuse (CSEA), offenders have increased accessibility to potential victims which, alongside increased internet use by children, has enabled the global proliferation of these offences (Bleakley et al., 2024; Martellozzo, 2017).

Online grooming, child sexual abuse material (CSAM), and sextortion are three OCSEA offences enabled by technology. Grooming is a modus operandi implemented by offenders to prepare a victim, their guardians, and their environment for CSEA (Martellozzo, 2017; Whittle et al., 2013a). Preparing a child for sexual abuse focuses on ensuring the offender has access to a child who will not disclose the abuse (Kloess et al., 2014; Peters, 2021; Ringenberg et al., 2022; Whittle et al., 2013b). CSAM includes images, videos, or depictions of children in a sexually explicit manner (Rimer, 2024). Sextortion is the coercion of a victim into fulfilling a request by threatening to distribute sexual media of the victim (Açar, 2016; Henry & Umbach, 2024; O'Malley & Holt, 2022; Ray & Henry, 2024; Rimer, 2024). These requests could be sexual, such as demanding more CSAM or the abuse of other minors by the victim, or financial, such as demanding a payment via bank transfer or gift cards (Henry & Umbach, 2024; O'Malley & Holt, 2022). These offences have been further shaped by the ability for people to capture and share images and videos of themselves via their devices (Bloxsom et al., 2024). Young people (YP) being able to create and share photos and videos has resulted in the

production of CSAM under the coercion of offenders (Bloxsom et al., 2024). This is referred to as "self-generated CSAM" (SG-CSAM).¹

This thesis aims to gain insight into the ways primary prevention resources from Australia (AUS), New Zealand (NZ), the United States of America (USA), and the United Kingdom (UK) involving the self-generated aspects of grooming, CSAM, and sextortion align or not with how YP use the internet. It further aims to explore how the same resources align or not with how offenders are using technology to abet offending. The following research questions will be answered:

- 1) Are current OCSEA prevention resources for the self-generated aspects of CSAM, grooming, and sextortion aligned with how YP use the internet?
 - 1a) If so, how do resources align with developmental, cognitive, and social factors that may impact the way YP use the internet?
 - 1b) If not, how could resources (including content, design, and the targeting of different audiences) be altered to align with relevant developmental, cognitive, and social factors?
- 2) Are current OCSEA prevention resources for the self-generated aspects of CSAM, grooming, and sextortion aligned with how offenders use technology to commit these offences?
 - 2a) If so, how do resources align with offenders' use of technology?

8

¹ Quayle (2022) has suggested the term "self-generated CSAM" places implied blame on victims, when the reality is these images are produced without the complete understanding or consent from the child. As such, they devise a shift to the term "perceived-first person CSAM" (PFP CSAM), however this thesis uses the term SG-CSAM because it is more well-known across literature and prevention resources.

2b) If not, how could resources (including content, design, and the targeting of different audiences) be altered to align with offenders' use of technology?

For the purposes of this project, the term "young people" refers to anyone under the age of 18, thus allowing for exploration of prevention resources aimed at any aged child, or their parents and carers.

Altogether, 150 primary prevention resources were analysed across the four countries by employing inductive thematic analysis (ITA). Analysis revealed prevention resources position knowledge and education as empowering for YP and offenders. Overall, the resources foster confusion about the best approach to controlling YP's internet use by parents and carers, however it is acknowledged that these approaches should vary by age. Cumulatively, the resources provide an unclear picture of *who* parents, carers, and YP should be weary of when trying to stay safe online and this is compounded by the manipulative ways offenders develop relationships with YP to prepare for sexual victimisation. Whilst some resources convey how YP will socialise with risky people online, others merely advise not to interact with "strangers" and "predators". Finally, the prevention resources portray that online grooming, SG-CSAM, and sextortion offenders mimic YP's technology use to initially engage with potential victims because they can identify social trends in interactive online environments, as well as platforms designed for YP. Then offenders will migrate abuse to a more private platform for threats and sexualisation, according to the resources.

This thesis begins by detailing current literature surrounding online grooming, CSAM, and sextortion offences, factors influencing YP's internet use, and effective OCSEA primary prevention. Then, the data and methodology are discussed, including how the resources were selected, collected, and analysed. This is followed by the results which are then contextualised

in the surrounding literature, using Protection Motivation Theory (PMT) to answer the research questions.

Chapter 2: Literature Review

This chapter begins by providing a brief background of OCSEA offenders and victims, the three focus offences, and areas where these offences converge. Then, the developmental, cognitive, and social factors contributing to how YP use the internet are discussed before moving onto the need for OCSEA prevention and applying PMT.

Online child sexual exploitation offences

OCSEA is significant because the dangers of CSEA extend beyond the physical barriers of offline spaces. There is not one OCSEA offender profile, however the most consistent findings are that offenders are typically male, white, and sometimes more highly educated than offline offenders (Babchishin et al., 2011; Henshaw et al., 2018; Kloess et al., 2014; Martellozzo, 2017; Shelton et al., 2016; Wolak et al., 2010). Victims of OCSEA do not come from homogeneous backgrounds; they range in socioeconomic status, geographic location, and ethnic and cultural background, but research highlights increased victimisation of females (Chauviré-Geib & Fegert, 2024; Choo, 2009; Villacampa & Gómez, 2017).

Online grooming offences

Online grooming offenders employ a variety of strategies to victimise YP. Online grooming commonly commences with enticements, where an offender attempts to build a 'special relationship' with a child by, for example, providing support and empathy, helping with homework, or complimenting the child (Ringenberg et al., 2022). The grooming process varies in duration, style, and intensity, but common elements include manipulation (e.g., flattery), accessibility, rapport building (e.g., learning about the victim's family and hobbies), risk assessments (to determine the likelihood of being caught) and sexual context, such as sharing pornography or CSAM (Choo, 2009; Kloess et al., 2019; Peters, 2021; Ringenberg et al., 2022; Whittle et al., 2013b). Offenders capitalise on the range of platforms available to complete the

grooming process by, for example, migrating conversations with a victim from online games or social media, such as Facebook, to encrypted communication applications, such as WhatsApp (National Society for the Prevention of Cruelty to Children, 2022; Peters, 2021; Thorn, 2017).

Online child sexual abuse material offences

Internet connected devices have allowed offenders to distribute and consume CSAM more swiftly and in higher volumes (Salter & Whitten, 2022). CSAM is circulated on the open web, including social media sites like X (formerly Twitter), and the dark web (e.g., Tor sites), and offenders seek contact with children for CSAM victimisation on encrypted messaging applications, social media, and online games (Lapsia, 2024). The majority of CSAM is created by offenders with physical access to children, such as family members or friends (Thorn, 2025), however, in 2024 the Internet Watch Foundation's (IWF's) Annual Report revealed 91% of the reports they received involved SG-CSAM content, making it the predominant type of reported CSAM (Internet Watch Foundation [IWF], 2024). This highlights a shift from offline production to SG-CSAM, and prevention resources need to consider this.

Online sextortion offences against minors

Sextortion initiation can be quick, for example an offender contacting a victim with immediate requests for CSAM, or slow, for example, threatening to release images when a victim tries to end an online or offline relationship (Ray & Henry, 2024; Thorn, 2017; Walsh & Tener, 2022). Ray & Henry (2024) conducted a scoping review to understand current literature on sextortion prevalence, finding victims of sextortion are most likely to be YP or sexual minorities. This was supported by Thorn's (2017) survey (with 2,097 respondents aged 13-25) which found younger victims are more likely to experience sextortion perpetrated by an offender met online. Most respondents were contacted by offenders on social media or chat

applications, including Kik, Facebook, Snapchat, Instagram, Skype, Gmail, Messenger, and Tinder (Thorn, 2017). Current literature has mixed results about the gender of sextortion victims; some state girls are more often victimised whilst others state males are, but generally girls are more likely to report victimisation than boys (O'Malley et al., 2023; Ray & Henry, 2024; Wolak et al., 2018).

The overlaps between grooming, CSAM, and sextortion

Grooming, CSAM, and sextortion offences are not mutually exclusive. Some grooming offenders use CSAM within the grooming process to, for example, make children feel more comfortable with providing images (Peters, 2021; Quayle, 2022; Thorn, 2017). Grooming can be committed as a precursor to sextortion, or sextortion can be committed after grooming to silence victims (Peters, 2021; Quayle, 2022; Ray & Henry, 2024; Thorn, 2017). For example, an offender builds a false, trusting relationship with a victim to obtain CSAM and then threatens to distribute the image if the victim discloses abuse (Peters, 2021). Additionally, sextortion is now a means for offenders to create SG-CSAM without having to be with the victim offline (Ray & Henry, 2024). These three offences can be committed in combination by OCSEA offenders who use technology to gain more information about victims, advance the longevity of their offending, and reduce the perceived risks of being caught by law enforcement (Peters, 2021). Victimisation, whether through a combination of offences or isolated to one, has detrimental impacts for YP.

Impacts of victimisation

The impacts of OCSEA victimisation must be considered when understanding the importance of prevention. CSAM victims face the possibility of their images being further distributed and continuously circulated online by offenders, threatening online permanence (Gewirtz-Meydan et al., 2018; Leonard, 2010; Martin, 2015; von Weiler et al., 2010; Whittle

et al., 2013a). This leads to prolonged feelings of shame, fear, anxiety, helplessness, powerlessness, blame, or guilt because victims know images may be circulated and viewed by unknown offenders continuously (Gewirtz-Meydan et al., 2018; Leonard, 2010; Martin, 2015; von Weiler et al., 2010; Whittle et al., 2013a). For example, Leonard (2010) conducted a study using two examples to understand how online and offline CSEA victimisation should be treated differently. They found SG-CSAM victims blame themselves because they believe they consented to sharing imagery with an offender as their "friend" (Leonard, 2010). It is evident from these impacts that OCSEA victimisation has detrimental outcomes which drives the need to understand the factors influencing YP's internet use.

Factors influencing how young people use the internet

Factors influencing how YP use the internet must be explored to understand how OCSEA primary prevention resources are aligned or not. Such factors can be divided into developmental and cognitive (D&C) factors (i.e., those depending upon a person's learning and experience) and social factors (i.e., social norms, pressure, and expectations for YP to follow in online environments).

Developmental and cognitive factors

D&C factors refer to elements of a child's learning, based on their age, that shape the way they understand, interact with, and utilise online environments (Borca et al., 2015; Danovitch, 2019; Johnson, 2006; Johnson, 2010; Munakata et al., 2004). D&C factors include phases of identity exploration, practicing independence, and practicing problem solving, particularly when gaining a sense of autonomy from parents (Borca et al., 2015; Given et al., 2016; Kennedy & Lynch, 2016; Throuvala et al., 2019). OCSEA offenders exploit these behaviours; for example, grooming offenders can understand a young person's desire for peer validation and will thus become a source of such validation to get closer to a victim

(Ringenberg et al., 2022). Furthermore, research suggests that despite being aware of risks, YP still partake in risky online behaviour (Liau et al., 2005; Livingstone et al., 2011; White et al., 2015). This suggests adolescents' ability to make decisions based on risk is limited by personal experiences and development, so being presented with negative experiences of other people resulting from risky behaviour is not necessarily effective (White et al., 2015). As such, D&C factors influencing how YP use the internet shift with both age and personal experiences, and should be considered by prevention resources aiming to deter risky online behaviour.

Social factors

Social factors influencing YP's internet use must be considered when creating prevention resources because they impact how YP choose to interact with content and people online. Social factors refer to social norms or expectations for internet use (Klobas & Clyde, 2021; Prievara et al., 2019). For example, the transition from childhood to adolescence often encompasses a desire to improve social status amongst peers which may impact online behaviours, including a propensity to overshare personal information online (Hayes et al., 2022; White et al., 2015; Wright, 2014) which offenders can utilise to target victims.

Social factors also include support from, and communication with peers, significant others, and family members (Kennedy & Lynch, 2016; Prievara et al., 2019; Tilleczek et al., 2019). For example, Kennedy & Lynch (2016) explored the nature of online social participation amongst 16 Irish nine to 16-year-olds and found all participants engaged in online social communication daily, including texting, tweeting, or posting as methods to expand and maintain social circles. Therefore, the desire for support and connection shapes the goals of accessing online environments, which determines online behaviour. Additionally, Kennedy & Lynch (2016) identified that YP seek online privacy from parents to avoid being embarrassed by posts considered to be "cringe-worthy", whilst others accept their parents monitoring for

appropriate behaviour, for example, not using "bad words" (p.162). This displays how YP's internet use is shaped by social expectations from both peers and parents.

Ignoring the social factors influencing internet use leaves gaps within OCSEA prevention resources, leaving YP more vulnerable. For example, offenders can understand the desires of adolescents to "fit in" with peers and utilise this to manipulate a child into creating SG-CSAM by sending another victim's CSAM (Choo, 2009; Peters, 2021). Furthermore, offenders can capitalise on the fears of YP becoming socially isolated to coerce them into creating more SG-CSAM with the threat of sharing their previous images with their friends and family (Peters, 2021; Walsh & Tener, 2022). Ultimately, the ways YP use online environments results in the need for effective OCSEA prevention initiatives.

The need for effective OCSEA prevention

Evidence-based prevention education for parents, carers, and YP is pertinent because it reduces the implementation of ineffective initiatives. For example, overly restrictive moderation and monitoring strategies do not prevent OCSEA victimisation, yet they are still implemented for online safety (Wang et al., 2021). Strict parental controls have been evaluated as ineffective at reducing risk of harm because YP seek out unrestricted environments, especially when exploring independence, and restrictions inhibit open and trusting communication between parents, carers and YP (Garmendia et al., 2012; Ghosh et al., 2018; O'Neill & Staksrud, 2012; Shin & Ismail, 2014; Wang et al., 2021). Additionally, law enforcement agencies do not have the capacity or resources to arrest and prosecute all OCSEA offenders because of the volume of reports being received, as showcased by NCMEC's 20.5 million reports of OCSEA in 2024 (Henry et al., 2018; NCMEC, 2024). These issues highlight the need for effective primary OCSEA prevention aimed at parents, carers, and YP.

Primary prevention

Primary prevention initiatives target an entire population to alter factors within the environment before an offence can occur (Brantingham & Faust, 1976). Primary prevention is proactive because it is not implemented in response to an offence. For example, the Australian Centre to Counter Child Exploitation's (ACCCE's) ThinkUKnow program provides educational resources for parents, caregivers, children, and education providers about preventing OCSEA (Australian Centre to Counter Child Exploitation [ACCCE], n.d.). Such resources have been created to intentionally deliver the same information to all audiences.

Effective and ineffective messaging for primary prevention resources

Successful offence prevention is the most desirable outcome to ensuring YP are not victimised, thus effective and ineffective messaging needs to also be considered. Literature on effective primary prevention programs for online and offline CSEA oftentimes use a measure of knowledge retention to judge effectiveness, however knowledge retention does not guarantee positive behavioural change to increase online safety (Ferragut et al., 2023; Finkelhor et al., 2021; Patterson et al., 2022). For example, Patterson and colleagues (2022) conducted a systematic review of nine studies from 2007-2019 on education and awareness interventions to determine effectiveness of primary OCSEA prevention. The researchers identified that initiatives which encourage active engagement from YP during the development process and respect youths' online activities are more effective for information retention, potentially due to children knowing what engages them better than adults creating interventions in isolation. Despite this, there was still no significant reduction in YP's risk-taking behaviour (Patterson et al., 2022).

Researchers have also suggested that "stranger danger" messaging is ineffective at reducing the risks of OCSEA victimisation for YP because it neglects the relationship built

between victims and offenders, so offenders no longer appear to be strangers (Finkelhor et al., 2022; Nurse, 2017; Sinclair et al., 2018; Weston & Mythen, 2020). Similarly, Nurse (2017) highlights how categorising offenders with terms like "evil" and "perverts" can leave YP vulnerable to offenders who are not perceived this way by parents and YP. Nurse (2017) also suggest prevention strategies should include deconstructions of offender categories to avoid reinforcing stereotypes, such as being able to easily spot offenders. Moreover, warnings to not share private information or meet strangers online are unlikely to be effective because they do not acknowledge how YP use online environments in alignment with social norms or to learn about sexuality and romance (Finkelhor et al., 2021; Wolak et al., 2004).

Researchers have also identified that effective prevention messaging should avoid inciting fear by, for example, presenting "worst-case" scenarios because it ignores everyday risks for YP, making the risk of OCSEA unbelievable (ACCCE, 2020; Davis, 2012; Finkelhor et al., 2021; Weston & Mythen, 2020). Effective prevention resources should acknowledge YP relate to and engage with prevention resources differently based on age and experiences (Topping & Barron, 2009; Weston & Mythen, 2020). This suggests the D&C factors influencing internet use are important to address when creating prevention resources because this will shape the relevance of resources for YP. Additionally, initiatives, such as Stop It Now's Internet Safety program, aimed at increasing knowledge for caregivers are beneficial for OCSEA prevention because they increase guardian comfort when discussing OCSEA risks (Patterson et al., 2022). This aids in reducing negative stigma surrounding OCSEA victimisation (Patterson et al., 2022; Prikhidko & Kenny, 2021).

Theoretical framework: Protection motivation theory

PMT is used to explain how communication can lead to changes in risk-taking behaviours to avoid a threat, thus it is suitable for understanding primary prevention resource content. PMT

is a general theory of persuasive communication aimed at eliciting behavioural change motivated by perceived vulnerability to risks (including severity and likelihood), the efficacy of the recommended response, and a person's self-efficacy (Boer & Seydel, 1996; Tsai et al., 2016). Self-efficacy refers to a person's belief in their ability to successfully change their behaviour or action advice (Boer & Seydel, 1996). PMT has been applied to offline CSEA education which aimed to understand parents' intentions to educate children about CSEA after engaging with prevention resources (Burgess & Wurtele, 1998; Campis et al., 1989). Campis and colleagues (1989) found that increasing a parents' self-efficacy to discuss CSEA with children increased their intentions to actually do so. Sturges & Rogers (1996) explored this theory with a developmental perspective to understand whether an explanation for adults' rational decision making could also be applied to children and adolescents. They conducted a study with a group of 10-year-olds, 15-year-olds, and 20-year-olds with smoking prevention resources and discovered resources need to consider the developmental stages of children by focusing more on uplifting their self-efficacy. This is because a child's belief in their ability to abstain from risk-taking behaviours is more easily reduced when compared to adolescents and adults (Sturges & Rogers, 1996). This means children are less certain in their abilities and more easily influenced by external pressure, so they require resources that focus on uplifting selfefficacy (Sturges & Rogers, 1996). These researchers suggest children can understand appropriate and encouraged behaviours once exposed to information, allowing this theory to be applied to children as well as adults. PMT allows insights to be gained into how and why prevention resources may or may not consider the developmental, cognitive, and social factors influencing YP's internet use.

Literature summary

This chapter showcased the significance of OCSEA prevention for safeguarding YP online. The impacts of OCSEA victimisation, particularly with CSAM elements, are carried by

victims throughout their lives, so the ultimate goal is to prevent abuse occurring at all. Research on effective primary prevention resources is inconclusive and confuses knowledge retention as an indicator for effectiveness, when this does not necessarily translate to increased online safety behaviour. This thesis adds to the literature by developing an understanding of if and how primary prevention resources for the self-generated aspects of online grooming, CSAM, and sextortion align with how YP use the internet, and how offenders use technology. Further research is required to comprehensively evaluate effective OCSEA prevention campaigns, and this thesis provides a stepping stone for organisations to consider the developmental, cognitive, and social factors when creating primary prevention resources in future.

Chapter 3: Data & Methodology

This chapter outlines the data and methodology used to complete this thesis. It will first discuss the data collection process and then the analytical methodology employed to answer the research questions before describing the limitations and ethical considerations.

Data Collection

Prior to commencing data collection, a list of inclusion criteria was established to ensure the resources originated from countries considered to be similar to Australia. These similarities included being democratic and having similar internet access restrictions (e.g., no country-wide filtering and blocking of popular social media applications). Resultingly, the following inclusion criteria were chosen:

- Is created by an organisation or government within any of the following countries:
 - o Australia
 - New Zealand
 - o USA
 - o UK
- Provides educational information or guidance for preventing online CSAM, grooming, or sextortion.
- Is a primary prevention resource.
- Is aimed at YP or parents/carers of YP who are under the age of 18.
- Is intended for public consumption.

- Is distributed via public websites hosted by government, non-government, charity, not-for-profit, or private organisations.
- If distributed via social media, it is posted via an organisation's public social media accounts (not an individual's account) and links to the organisation's website.
- Is in English.
- Is the most current version of the resource.
- Includes an aspect of SG-CSAM prevention.
- Is a written resource.

Google was selected as the preferred search engine for data collection. Firstly, keywords associated with the resource inclusion criteria were listed and then synonymised. For example, synonyms for "grooming", "CSAM", and "sextortion" were identified. These synonymised keywords were then used to devise search terms utilising Boolean operators (see Appendix A) to reduce the number of individual searches needing to be completed whilst maximising the potential return of relevant results. To further aid data collection, some organisations' websites were selected to specifically search within for prevention resources; these were selected based on their efforts and aims to combat OCSEA, or their work with YP. This involved searching for the website on Google, opening the site, and trying to identify eligible resources by navigating through the site (these sites are listed in Appendix B). All the collected resources were listed in an Excel spreadsheet with their details, including website/organisation, country of origin, and target audience.

Initially, the data was gathered with the intention of being divided into CSAM, grooming, and sextortion resources, however it became evident that most resources aimed to address two

or more offences, rather than one in isolation. Resultingly, the resources were not analysed in isolation. In total, 299 resources were collected across the four countries, which was then narrowed to 150 resources analysed (see Table 1 for the breakdown of resources per country and see Appendix C for the listed analysed resources).

Table 1: Total number of prevention resources collected and analysed across the four countries.

	Total number of prevention resources		
Country	Collected	Analysed	
Australia	127	69	
New Zealand	11	6	
USA	54	21	
UK	107	54	
TOTAL	299	150	

To ensure consistency, a spreadsheet was maintained which provided exclusion reasons for resources which may have met some criteria but not all; for example, news articles, resources aimed at classroom use, and resources requiring payment were excluded.

After all data was collected, the resources were reviewed again to confirm they fit the inclusion criteria. Then, the resources were either downloaded directly (if readily available as PDFs), printed from the webpage (if the PDF this produced rendered correctly without cutting content), or the content was copied into a Microsoft Word document. Each document was stored under the naming convention CRIME NUMBER COUNTRY, for example CSAM 04 AUS. Each resource was named using the offence which was its overarching focus, or the first offence it mentioned. However, to reiterate, due to the significant overlaps across the three offences, just because one resource is named with the offence of CSAM, grooming, or sextortion, this does not indicate the resource only targeted the named offence.

Data Analysis: Inductive Thematic Analysis

ITA was selected as the most appropriate analytical approach, guided by Braun & Clarke (2006), because the aims did not seek to test hypotheses or theoretical applications, but rather discover what the prevention resources contained. ITA is a type of thematic analysis involving analysing data without any preconceived agenda or theoretical perspectives to draw upon and fit the data within during analysis (Braun & Clarke, 2006). Instead, ITA allows a researcher to draw themes directly from the dataset, letting the resources themselves guide the themes composed by the researcher (Braun & Clarke, 2006). Correspondingly, for this project, ITA enabled the identification, analysis, and reporting of patterns (termed "themes") within the primary prevention resources. Notably, these themes were subjective to the meaning interpreted by the researcher for answering this project's research questions (Braun & Clarke, 2006).

Analysis commenced with familiarisation of the data by re-reading the resources collected. This was a crucial step which allowed the researcher to be immersed by actively conceptualising broad meaning and patterns presented in the prevention resources (Braun & Clarke, 2006; Nowell et al., 2017). These initial conceptualisations were recorded in a notebook as this was the researcher's preferred method of notetaking. This phase was followed by initial coding, whereby the researcher commenced a rigorous and systematic process of re-reading each prevention resource and selecting features of the raw data (Braun & Clarke, 2006) that provided advice, mentioned technology use, were repetitive, or appeared less frequently as potential anomalies. This was completed with the qualitative analysis software, Nvivo 15, as it allowed for file imports, interactive creation of codes and themes, and accessible quote retrieval. These initial codes covered content such as advice for parents to tell children, the applications and platforms used by offenders and YP, and how the resources provided information about the OCSEA offences. In this stage, the codes were sorted into those that could potentially be used for themes related to RQ1 (such as internet use behaviours of YP)

and themes related to RQ2 (such as mentions of offender technology and platform use) as this enabled the researcher to more easily identify when a code could be re-used or if a new code should be created. This dichotomy of codes was later shifted in theme development, so they were no longer divided between the two research questions. An additional categorisation was created to code where prevention resources linked to other prevention resources or more information because the researcher noticed this was occurring quite frequently across the data. Again, the researcher took notes about these codes.

Once the coding phase was completed, the researcher then commenced identifying themes from the initial codes generated (Braun & Clarke, 2006). Before merging any codes, the researcher read through all notes taken throughout the initial coding phase to ensure any significant observations were not overlooked during theme development. Next, the initial codes were grouped together based on similarities in meaning and frequency throughout the data. These groupings were then compared to the resources to ensure the codes were considered within the context of the resource they were extracted from, enabling the determination of themes without mis-representing the resources (Braun & Clarke, 2006; Nowell et al., 2017). This step was important to ensure a single theme was able to comprehensively capture opposing viewpoints, rather than just a single perspective. This was followed by defining and naming themes (Braun & Clarke, 2006). Theme names were representative of the whole theme, not just a single part. This step solidified the formation of sub-themes by providing internal structure for the main themes which covered varying perspectives presented by the resources (Braun & Clarke, 2006). These themes were reviewed twice more, and a final read-through of the prevention resources was undertaken to allow for alterations ensuring themes were adapted appropriately, as well as ensuring anomalous codes were not missed.

Limitations

This project does have some limitations. Firstly, only written resources were analysed, which means any interactive resources (e.g., ones that gamify learning) were excluded. Additionally, video resources were only included if they were embedded within a written resource which provided a readily available transcript. This was due to the timeframe allotted for the project and the volume of resources being discovered. Another limitation was the exclusion of primary prevention resources requiring payment; for example, eSafeKids had some resources which required payment to access. Moreover, this study was limited to prevention resources written in English which excluded resources written in other languages and does not reflect the multiculturalism of Australia, New Zealand, the USA, and the UK.

Whilst not a limitation, given thematic analysis can be considered a subjective analytical approach, there is a possibility for inherent analytical bias within the developed themes (Braun & Clarke, 2006). To mitigate this, the researcher ensured initial codes represented the raw data by refraining from seeking underlying meaning at this stage. Additionally, the author considered all coded advice without imposing bias about effectiveness.

Ethical Considerations

This thesis posed negligible risk because the data was gathered from government, non-governmental, charity, not-for-profit, and private organisations' publicly available websites. This research involved resources intended for broad public consumption with no human participation. An ethics exemption was received on September 16th, 2024 from the University of Queensland Research Ethics and Integrity (2024/HE001846).

Chapter 4: Results

This chapter details the themes identified in the prevention resources: 1) *Knowledge is power*; 2) *To control or not to control*?; 3) *Stranger, friend, or predator*?; 4) *Using social media and online gaming for offending*; and 5) *Offenders transition across platforms throughout offending*. All themes were represented across all three OCSEA offences. A notable observation was that 68% (102) of resources directed readers to additional resources, however, the additional resources were not analysed.² Note that some results are presented in quotes with ellipses inserted which is indicative of words being removed due to brevity or redundancy, but the meaning of the quotes has not been altered.

Theme 1: Knowledge is power

The theme of *knowledge is power* represents how the primary prevention resources suggest knowledge is crucial in disrupting and preventing an offence. This theme is represented across 96.0% (144) of the analysed resources and referenced 1,087 times. This theme is present throughout all three crimes and all four countries of analysis. Given this theme's breadth, it has been broken into three sub-themes: *Education and information are empowering; conversations break the stigma;* and *beware of proactive and reactive red flags*.

Sub-theme: Education and information are empowering

This sub-theme is represented across 79.3% (119) of the resources and referenced 451 times. *Education and information are empowering* includes educating about consent to empower YP to say "no"; for example, statements such as "it's important that youth know they

² This was noted because prevention resources may have been complimented by these additional resources. For example, some resources referred parents and carers to instructions for control settings but did not include any information about the OCSEA offences. The referenced resources were included for analysis only if the project collection criteria were met.

have the ability to say NO to anything that makes them uncomfortable or is unsafe" (CSAM 25 UK), and:

You can also discuss consent. Let young people know they have a right to say what happens to their body online and offline and talk about the importance of online safety practices like getting consent for sharing photos and videos. (GROOMING 095 AUS)

These examples explicitly state understanding consent enables informed decisions by young people, and gives them the power to express their desire, or lack thereof, to participate in something.

Some resources explicitly state education and knowledge equip YP with skills to defend against grooming, SG-CSAM, and sextortion. For example, "By focusing on educating children and young people can be equipped with the knowledge and tools to navigate these issues, while using the internet safely" (GROOMING 002 AUS). This highlights the importance primary prevention resources place on skill development through the imparting of knowledge, suggesting knowledge transfers to skill development. Some resources explicitly state knowledge is power or it empowers; for example "To help empower young people, it is important to build knowledge and critical thinking skills to help them navigate these issues" (GROOMING 006 AUS), and GROOMING 017 USA recommends for parents, carers, and children to engage with NCMEC's NetSmartz interactive educational program "to help empower children to make safer choices online." These examples articulate the positioning of knowledge as powerful for skill development to result in action to keep safe online, despite literature suggesting otherwise (Ferragut et al., 2023; Finkelhor et al., 2021; Patterson et al., 2022).

Sub-theme: Conversations break the stigma

This sub-theme is represented across 60.0% (90) of the analysed resources and referenced 259 times. The resources suggest stigma surrounding grooming, CSAM, and sextortion offences is compounded by offender manipulation tactics. For example, 26.0% (39) of resources emphasise how offender tactics make children feel like there is no way for them to prevent or stop abuse. Resources state offenders use fear, shame, coercion, and persistent contact to manipulate YP into feeling trapped. For example, "the shame, fear, and confusion children feel when they are caught in this cycle often prevents them from asking for help or reporting the abuse" (SEXTORTION 38 USA). This suggests offenders have knowledge of negative stigma surrounding SG-CSAM, and they capitalise on this to remain undetected by preventing YP from seeking help. Therefore, an offender's knowledge of YP's fear (through intimidation and threats), shame (through condemnation of sending SG-CSAM), and blame (by positioning the victim's actions as illegal) gives them power to silence victims, suggesting knowledge is power.

The prevention resources within this sub-theme recognise how stigma creates barriers for children which prevent help-seeking behaviours, and emphasise the importance of open communication between parents/carers and YP to prevent fear, shame, and stigma from trapping them into abuse. Amongst the analysed resources, 12.0% (18) suggest by removing the awkwardness between parents/carers and YP during conversations surrounding OCSEA, sex, or relationships, this breaks down barriers to recognising, preventing, and reporting grooming, SG-CSAM, and sextortion. For example, CSAM 18 UK and CSAM 36 AUS advise parents to remove awkwardness by avoiding sitting face-to-face during discussions, which acknowledges discomfort but also provides a method of alleviation so the conversation can take place. All of these resources emphasise awkward discussions need to take place regularly with revised information as YP grow up to begin to feel more "normal" and remove stigma,

because when parents and carers ensure YP have the knowledge that victimisation is never their fault, then YP have the power to report offenders.

Some resources also advise parents and carers to explicitly provide reassurance to YP when having conversations about online safety, grooming, SG-CSAM, and sextortion. 48.0% (72) of resources advise parents and carers to tell YP they will not be blamed, punished, judged, or dismissed when talking about their online activities and interactions. The resources suggest this explicit communication can break down barriers to recognising, preventing, and reporting these OCSEA offences. For example, GROOMING 087 AUS advises to "talk to your child without being judgemental or angry and make them feel like they can come to you with anything, without fear of being punished or criticised." Likewise, CSAM 95 UK advises to "let [children] know they can share their concerns at any time and you won't be upset or angry with them if something has happened." Conversations break the stigma encapsulates that prevention resources suggest regular conversations surrounding these offences and online safety make it easier for parents, carers and YP to discuss online experiences. In doing this, it is suggested dismantling the stigma relied upon by offenders to prevent abuse disclosure empowers YP with the knowledge that victimisation is not their fault and can be reported without fear of repercussions

Sub-theme: Beware of proactive and reactive red flags

The resources provide both proactive and reactive warning signs for identifying online grooming, SG-CSAM, and sextortion targeting YP. This sub-theme is represented across 46.0% (69) of the resources and referenced 341 times. Proactive signs are indicators which help YP identify OCSEA *before* an image is generated and sent to an offender so they can disengage and/or seek help. These occur across 30.7% (46) of the resources (referenced 158 times) with the most common advice to beware of:

- Requests to transition to more private platforms (12.7%).
- Persistent or early requests for information (10.7%).
- Being persuaded to keep communication a secret (9.3%).
- Offering of gifts, favours, or modelling roles (9.3%).
- Inconsistencies which could identify a fake profile (6.7%).
- Someone making excuses to avoid video chats, such as broken cameras (6.7%).
- Things seeming "too good to be true" (6.0%).

This approach of resources providing proactive red flags suggests YP can be empowered to disengage from uncomfortable and inappropriate online situations by gaining knowledge of the indicators of an offence. By providing examples of behaviour that could indicate an online contact is attempting to commit an offence, the resources intend for the audience to take preventative action. Thus, knowing the proactive and reactive red flags is positioned as powerful to prevent victimisation.

Comparatively, reactive warning signs are those informing parents and carers of the signs a child may *already be* experiencing victimisation. These occur across 26.0% (39) of the resources but are referenced more than the proactive warnings (183 references compared to 158 references). The most mentioned reactive warning signs were:

- Unexplained gifts or money (13.3%).
- Changes in mood, behaviour, or eating habits (12.7%).
- Secrecy surrounding devices and online activities (11.3%).

- Withdrawal from friends, families, or hobbies (6.7%).
- Changes in sexual knowledge, language, or behaviour (5.3%).

By providing reactive warning signs, the resources guide parents to maintain knowledge about their child's *normal* behaviours so they have the power to identify and intervene if their child does experience grooming, SG-CSAM, or sextortion victimisation which results in a shift in their child's behaviours. Overall, the theme *beware of proactive and reactive red flags* showcases how the resources indicate knowing the signs to look out for can empower parents, carers, or YP to identify, disengage from, or intervene in harmful online situations.

Theme 2: To control or not to control?

To control or not to control? represents resources advising parents on how to: use technical controls (including privacy settings, parental controls and monitoring software); choose a level of parental supervision for online activities; or choose rules that should be implemented by parents and carers. This theme is present throughout 48.7% (73) of the resources and referenced 228 times. The effectiveness of parental controls and monitoring software is a contentious issue for online safety of children (Ghosh et al., 2018; Shin & Ismail, 2014; Wang et al., 2021), and the prevention resources reflect the same trend. This is significant because the resources deliver inconsistent advice about if and how parents should be using parental control software. Resultingly, parents and carers may be left more confused about what steps they should be taking to keep their children safe from online grooming, SG-CSAM, and sextortion.

A minority of resources *advise against* the use of technical controls for keeping children safe online (4.7%; 7). These resources state such impositions create distrust, and five of these seven resources state if parents/carers do want to use them, they should explain the reasoning to their children to avoid defiance (Ghosh et al., 2018). The remaining two of these seven

resources state content filters either encourage YP to look for restricted content or hinder their ability to independently avoid online risks:

Avoid using filters or other online safety tools. If your child is using filters, they might not develop the skills they need to avoid inappropriate content. They might take risks either accidentally or on purpose when they go online in unfiltered environments. (GROOMING 068 AUS)

Contrastingly, 20.0% (30) of the resources advise parental control software should be implemented and does keep children safe online. For example, GROOMING 026 USA tells parents/carers to stay informed by using "helpful tools like monitoring apps for iPhones and Androids to track your child's call logs, text messages, and who they have access to – or who has access to them – online". A smaller portion of resources (8.0%; 12) advise parents to supervise their children online, and monitor online activities, but do not mention the use of control software. Four of these resources leave the method of monitoring open to the interpretation of the reader by providing no elaboration on how to implement supervision; thus, parents and carers could interpret this as a need for monitoring software, physical supervision, or something else. For example, CSAM 12 AUS tells parents and carers to "Supervise your child while they're on a connected device... [this] can prevent incidents of them sharing selfgenerated child abuse material." The remaining eight resources do provide more detail when advising parents to supervise children online, for example, GROOMING 034 AUS provides a brief list of supervision methods including being in the same room as the child when online and ensuring online gaming audio is played out loud via speakers. The resources providing further elaboration on how to supervise children when they are online give parents and carers direction on what they can do to increase online safety for YP compared to those offering no elaboration.

All resources within this theme provide parents with advice to shape their child's internet use in some way, thus leaving parents and carers to determine if they should control, or how much control they should have over, their child's internet use. Most of the resources within this theme (26.7%; 40) provide encouragement for the use of control software in some form. 13.3% (20) encourage the use of control software whilst simultaneously stating it is not 100% effective; these resources advise to maintain open communication and implement rules for internet use alongside technical controls. For example, CSAM 81 UK advises parents they can keep children safe by "[installing] filtering and parental controls...but remember these are never 100% effective...Talk to your child and be involved in their online life...Agree to clear rules with your child". An additional 13.3% (20) of resources suggest a combination of technical controls and rules also, but do not state control software lacks effectiveness. For example, GROOMING 094 AUS states:

It can be useful to set firm limits about use of devices. For example, apps and websites should be explored together. Make sure online interactions are only with people known to you and your child and that you trust them to keep your child safe.... listen to [a child's] thoughts on family rules, such as how much screentime is allowed. [Parents/carers] can also use parental controls to help prevent children seeing content that may be confusing or upsetting.

Instead of mentioning the lacking effectiveness of parental controls, these resources rely on advising parents not to use parental controls in isolation. Whilst this attempts to guide parents and carers to consider more than one method of controlling their child's internet behaviours, it does not encourage them to consider the previously described drawbacks of technical controls. This is important because if parents and carers are unaware of the drawbacks then they may incorrectly believe their child is no longer exposed to online risks (Shin & Ismail, 2014; Wang et al., 2021). This theme displays how resources inconsistently advise parents to control YP's

internet use or not. Some resources advise parents that technical controls should not be the only method of online safety for YP, and rules should shift as children age. Other resources oppose this by advising against using monitoring software because it degrades trust, but become more confusing when saying to implement monitoring software *sometimes* because parents are left with contradicting instructions on how to move forward with online safety.

Theme 3: Stranger, friend, or predator?

The theme stranger, friend, or predator? showcases that prevention resources refer to offenders as strangers, friends, or predators inconsistently. This occurred across 63.3% (95) of the resources and was referenced 224 times. 32.0% (48) of resources reinforce "stranger danger" messaging to keep YP safe online and advise to never contact anyone a young person does not know offline. This messaging is conveyed using words like "stranger", "someone [parents/carers or YP] don't know", and "never met in real life". This is significant because the use of this messaging contradicts the research suggesting "stranger danger" narratives are ineffective for reducing YP's risks of OCSEA victimisation by failing to recognise the relationships formed between YP and offenders (Finkelhor et al., 2022; Sinclair et al., 2018; Weston & Mythen, 2020). For example, one resource defined a stranger as "someone we have never met in real life and don't know personally, therefore we can't trust to share private or personal information with" (CSAM 36 AUS). This definition fails to address how YP form personal connections with individuals online (whether legitimate or through offender manipulation), making it harder for YP to see an offender as a danger. Therefore, the effectiveness of the resources using this messaging can be called into question because they may misguide parents and carers about what to teach their children and fail to incite safer behaviours from YP during online interactions (Finkelhor et al., 2022; Nurse, 2017; Sinclair et al., 2018; Weston & Mythen, 2020; Wolak et al., 2004).

Some of the resources within this theme also acknowledge offenders can be known offline or considered online-only friends. 47.3% (71) of resources identify how offenders can be someone a young person knows offline or online-only; more than half (46) of these acknowledge online-only connections are not always strangers because of the formation of relationships and because interacting with people not known offline is inevitable. These resources align more with the literature surrounding ineffective "stranger danger" messaging and highlight inconsistencies across primary prevention resources. For example, CSAM 33 AUS states "online friends are different from the friends you see each day. You can't be certain who they are so be careful what you share and say." Opposing "stranger danger" messaging, CSAM 21 UK states:

Many young people receive friend or follower requests from people they don't know, and many view accepting these is part and parcel of being on social media...Banning a child from using all social media...or getting them to unfollow everyone they don't know in person – isn't the way to stop them being at risk. If you prevent them from accessing an essential part of their reality, and allowing them to connect with their friends, they will feel resentful, angry and alienated from you. They may also find other ways to keep connected, and become more private about their online lives.

This shows how, rather than prohibiting connections and relationships with people met online, these resources share the sentiment that children will interact with strangers online, so it is best to teach them how to do this safely. This is dichotomous to reliance on the term *stranger* which dismisses the formation of such relationships (Finkelhor et al., 2022; Sinclair et al., 2018; Weston & Mythen, 2020). Therefore, the prevention resources provide inconsistent messaging surrounding how parents, carers, and YP should perceive offenders to identify and avoid risky online interactions and victimisation.

Finally, 6.0% (9) of the resources label offenders as "predators", "pedophiles", "organised criminals", or "dodgy people". This messaging occurs across all three crimes, but only from AUS and USA-originating resources. These terms reinforce stereotypes, making it more difficult for parents/carers to educate YP, and for a young person to realise an "online friend" may be an offender (Nurse, 2017). For example, "Predators often pose as children to meet children or teens online" (CSAM 15 USA), and "They are a sexual predator (or 'paedophile') who is trying to trick you into sharing nudes or getting sexual online or in person" (CSAM 86 AUS). Overall, this theme showcases prevention messaging is inconsistent when teaching parents/carers and YP who to be weary of to prevent OCSEA victimisation. Strangers, friends, and predators are perceived differently by YP, parents, and carers; the terms "stranger" and "predator" are highly stigmatised and inhibit a potential victim's ability to identify if an online "friend" is truly a friend, or someone trying to harm them (Finkelhor et al., 2022; Nurse, 2017; Sinclair et al., 2018; Weston & Mythen, 2020).

Theme 4: Using social media and online gaming for offending

Given the use of online platforms is intrinsic for committing these offences, analysis focused on how resources stated they are being used and the mention of specific platforms. Overall, 66.7% (100) of the resources go beyond briefly mentioning that online platforms are used by delving into what offenders are doing with the platforms. This theme has been broken into two sub-themes: *Using social media and online gaming to initiate contact;* and *using social media and online gaming for identity obfuscation*.

Sub-theme: Using social media and online gaming to initiate contact

A portion of resources 28% (42) state a combination of social media sites, dating apps, gaming platforms, and online chat platforms are used for initial contact phases of online grooming, CSAM, and sextortion offences. Social media platforms mentioned for this phase include Snapchat, Instagram, Facebook, and TikTok. Private messaging platforms mentioned

include Facebook Messenger, Skype, or WhatsApp. Gaming platforms mentioned include Roblox, Discord, or Twitch. For example, GROOMING 023 AUS states:

Online grooming can happen just about anywhere children go online. All games, apps, website [sic] and platforms have the potential to be used by others to harm children. Any platform allowing communication with others, either written or verbal, has the potential to be used for online grooming, for example, gaming sites, social media platforms and messaging apps and platforms like Messenger, WhatsApp or Skype. Online child sex offenders use these platforms to initiate contact with a child and will then often invite the child to another, more private platform.

Additionally, 6.7% (10) of these resources mention the "scattergun" abuse tactic, where offenders target many victims at once to see who will respond. For example, "Perpetrators use a 'scattergun approach', contacting hundreds of children at once across platforms" (CSAM 18 UK). Therefore, the resources aim to inform parents, carers, and YP on the earliest possible signs of OCSEA in attempt to cultivate safer online behaviours from YP. Furthermore, by informing YP about the "scattergun" tactic, the resources attempt to encourage YP to consider red flag behaviours of OCSEA offenders and the potential that anyone making them feel a special connection online may also be contacting other YP in the same way.

Sub-theme: Using social media and online gaming for identity obfuscation

Across 30.0% (45) of the prevention resources, it is described that offenders use social media and online platforms for identity obfuscation or to appear more trusting to a victim. For example:

It is easy for someone with harmful intentions to pretend they are a child, a classmate or a friend's friend just by looking through a person's friend list and finding out what town they live in or school they go to. (CSAM 24 UK)

This quote shows how resources suggest an offender carefully selects a fake identity and by using information to appear as a mutual friend, a potential victim may believe any requests or messages are safe to accept.

In addition to appearing more trustworthy, some resources state offenders use identity obfuscation to reduce the likelihood of being identified as an offender due to the perceived anonymity of online environments. For example:

Among [the risks of romantic relationships in online spaces] is the threat posed by perpetrators intentionally leveraging the perceived anonymity of the internet to meet, manipulate, and abuse minors online... perpetrators take on a variety of online personas through which they connect with minors. (SEXTORTION 03 USA)

These quotes showcase how resources suggest offenders rely on identity obfuscation to abet OCSEA offending by increasing their perceived trustworthiness when interacting with victims and attempting to protect their offline identity. The resources attempt to encourage parents, carers, and YP to learn how to identify fake profiles so they can recognise unsafe interactions with the goal of influencing YP to actively assess account legitimacy.

Theme 5: Offenders transition across platforms throughout offending

The final theme showcases how resources state that offenders transition across platforms throughout offending. 16% (24) state grooming and sextortion offences do not occur in one place; instead, offenders are described as using one platform for initial contact and then convincing a victim to transition to a platform which offers more privacy. Resources state offenders transition to platforms including WhatsApp, Messenger, Discord, KIK, Telegram, and Snapchat. For example, SEXTORTION 57 USA states "These criminals commonly make first contact with a victim on one platform, then ask them to move to a second platform using encrypted messaging to make tracking their crimes more difficult." Likewise, GROOMING

070 NZ states "if [offenders] aren't already talking to the child using private or direct messages; groomers will try to move the conversation to a private platform where others can't see". Ultimately, these resources aim to establish that transitioning between platforms to increase privacy is a common tactic for online grooming and sextortion offenders, and as identified in theme 1, this can also be a warning sign for YP.

Chapter 5: Discussion

This chapter situates the key findings within the context of previous OCSEA prevention research by relating it back to the developmental, cognitive, and social factors influencing YP's internet use, and how these fit into PMT's suggested prioritisation of uplifting self-efficacy for parents, carers, and YP.

Key findings as applied to developmental, cognitive, and social factors

This project aimed to determine if current OCSEA prevention resources for the self-generated aspects of grooming, CSAM, and sextortion offences are aligned with how YP use the internet, and if the same resources are aligned with how offenders use technology to procure SG-CSAM. The results revealed some resources attempt to address the developmental, cognitive, and social factors which influence YP's internet use, however there is an overreliance on the stated power of knowledge to be successful in changing YP's online behaviours. Resultingly, the resources emphasise the importance of education over alignment with factors influencing how YP use the internet.

The literature states D&C factors are influenced by how the age of YP shapes the way they understand, interact with, and utilise online environments based on their exposure to knowledge and information (Borca et al., 2015; Danovitch, 2019; Johnson, 2010). However, increasing knowledge of risks does not necessarily cultivate a behavioural change for YP to make safer decisions online (Liau et al., 2005; Livingstone et al., 2011; Weston & Mythen, 2020; White et al., 2015). A significant finding from this project is that prevention resources position increasing a young person's knowledge as having the power to inherently cultivate changed online behaviour, thus reducing a YP's risk of victimisation. However, the literature suggests increasing awareness and education about these risks does not necessarily translate to reduced risk-taking behaviour (Finkelhor et al., 2021; Liau et al., 2005; White et al., 2015). As such, the prevention resources which state increasing YP's awareness of OCSEA risks will

reduce their susceptibility to victimisation do not align with current literature on the developmental factors which influence the risks taken by YP when engaging in online environments. Similarly, whilst the resources provide education and awareness about OCSEA tactics and red flags in attempts to encourage less information sharing, research suggests telling YP not to share personal information generally does not reduce their propensity to do so (Christofides et al., 2012; Finkelhor et al., 2021; Hayes et al., 2022). This is because this messaging fails to address the social norms shaping how YP interact in online environments (Christofides et al., 2012; Wolak et al., 2004; Wright, 2014). Resultingly, the emphasis that prevention resources place on the power of knowledge on OCSEA risks does not align with developmental, cognitive, and social factors which influence YP's online risk-taking behaviour.

The theme *to control or not to control?* highlighted that prevention resources are inconsistent with the advice given to parents about utilising technical parental controls. A minority of resources align with the literature that states restrictive controls are ineffective (Garmendia et al., 2012; O'Neill & Staksrud, 2012; Shin & Ismail, 2014; Wang et al., 2021). The most significant impeding factor for the effectiveness of these technical restrictions is when they are implemented with extreme restriction, such as constant activity monitoring and content blockers. This impedes a young person's ability to develop a sense of autonomy from parental oversight and discourages the development of skills to independently navigate unrestricted online environments (Borca et al., 2015; Garmendia et al., 2012; Shin & Ismail, 2014; Wang et al., 2021). Developing autonomy and independence are significant D&C factors impacting the behaviours of YP. Being prohibited from experiencing autonomy and independence has adverse effects for online safety, eliciting secrecy and risk-taking behaviour which discourages the disclosure of victimisation by reinforcing fears of repercussions (Garmendia et al., 2012; Ghosh et al., 2018).

Comparatively, the resources which provide advice for parents and carers to implement rules, such as using devices alongside parents, time limits, and devices used in common areas of the house, offer alternative and less-restrictive control for parents. Furthermore, allowing YP to be involved in the process of determining rules gives them a sense of autonomy over their restrictions, in comparison to parents just selecting and imposing rules (Finkelhor et al., 2021; Liau et al., 2005; Weston & Mythen, 2020; White et al., 2015). As such, resources which encourage parents and carers to give YP a say in their internet rules and guidelines support the D&C factors of autonomy and independence which shape internet use.

Another social factor presented within the resources stems from stranger, friend, or predator. Despite the research on effective prevention resources suggesting "stranger danger" messaging is ineffective at protecting YP from OCSEA victimisation (Finkelhor et al., 2022; Sinclair et al., 2018; Weston & Mythen, 2020), some prevention resources for grooming, SG-CSAM, and sextortion still implement it. Contrastingly, some resources do acknowledge YP will interact with others online without having met offline and thus develop seemingly legitimate relationships. These resources recognise YP will believe they have a true friend or partner and instead provide advice on practicing caution with online friends to indicate the potential threat, therefore aligning more with the social factors which lead YP to seek online relationships. Moreover, resources using more stigmatised terms like "predator" and "pedophile" inhibit a young person's ability to identify that someone they have already begun developing trust with may actually be an offender (Nurse, 2017; Weston & Mythen, 2020; Wolak et al., 2004). These inconsistencies cause confusion about who an online offender could potentially be. This is because a young person would not readily consider their online friend, whom they have developed trust with, to be a scary predator, or someone they don't know (Nurse, 2017). Aligning with PMT, these inconsistencies reduce a parent/carer or YP's selfefficacy in identifying potential unsafe interactions online, and coincidingly reduce the

perceived efficacy of the advice being provided because inconsistent messaging creates confusion rather than confidence. As such, PMT suggests parents and carers may be less likely to educate their children on these aspects of OCSEA, and YP may be less likely to be cautious when engaging with others online because the messaging does not resonate with them (Burgess & Wurtele, 1998; Campis et al., 1989; Sturges & Rogers, 1996).

Implications for future resource development

When developing primary prevention resources for OCSEA, organisations should look to support, rather than oppose or hinder the developmental, cognitive, and social factors influencing YP's internet use. Primary prevention resources targeting parents and carers should place more emphasis on guiding the development of age-appropriate online safety rules that consider the opinions of YP, rather than parental controls (Wurtele & Kenny, 2016). PMT suggests there should be a focus on uplifting YP's self-efficacy to increase their confidence to action the advice (Campis et al., 1989; Sturges & Rogers, 1996). By shaping prevention resources around the developmental, cognitive, and social factors that influence YP's internet use, this would also aim to increase self-efficacy by ensuring access to information relevant for different stages of their lives. For example, parents and carers could be better equipped to support D&C factors like autonomy and independence of their children by being taught strategies to prompt rule development from children, accompanied by scenarios that can be worked through together to practice how such rules would look during internet use. The target audience age of resources must also be made clear to both parents and YP so they can easily identify the relevance of resources, reducing the chance of becoming confused about who resources are aimed at, as well as ensuring the appropriate guidance is received by the intended audiences. This intends to aid the development of self-efficacy and resource-efficacy by providing actionable advice in alignment with YP's different cognitive, developmental, and social stages.

To support social factors influencing YP's internet use, it may be more beneficial for prevention resources to focus less on restricting access to particular platforms and condemnation of unknown people, and more on encouraging YP to identify and respond to feelings of uncertainty, concern, or discomfort when they experience it (Topping & Barron, 2009). This would enable understandings of distinctions between good versus bad online interactions, similarly to learning about healthy and unhealthy relationships (World Health Organisation, 2022). Given that developmental, cognitive and social factors influencing YP's behaviour are not exclusive to online activities and environments, organisations could consider identifying how offline CSEA prevention initiatives address these factors and assess whether there is potential for offline initiatives to inform the direction for OCSEA prevention initiatives.

Implications for future research

The analysed resources emphasised the importance of education and communication for parents, carers, and YP to help prevent online grooming, SG-CSAM, and sextortion offences. However, the resources relied a lot on referring the intended audience to additional resources to learn more about how to develop effective communication skills. Given these referenced resources were not within the scope of this project, future research could look into the resources which parents, carers, and YP are referred to for further developing their communication skills and overall knowledge of online safety practices. This would allow for a more well-rounded understanding of whether extended resources align with how YP use the internet and how they enable audiences to enhance prevention skills.

Future research could also extend this project by analysing primary prevention resources which are not text-based, such as videos and resources with gamification. Additionally, the scope of the research could be expanded beyond just resources with SG-CSAM elements. This would allow for insight into the ways of communicating that might be more engaging for YP

specifically, as well as build a more comprehensive picture of the primary prevention resource landscape for online grooming, CSAM, and sextortion offences.

Chapter 6: Conclusion

This thesis used ITA to gain understanding of how prevention resources with self-generated aspects for online grooming, CSAM, and sextortion from Australia, New Zealand, the USA, and the UK align or not with the developmental, cognitive, and social factors influencing how YP use the internet, and how they align or not with offender technology use. The prevention resources tend to align with the D&C factors influencing internet use when acknowledging prevention strategies need to shift as children age and as online independence increases. Some resources align with the social factors influencing how YP use the internet, like those recognising how YP do interact with people they have met online despite being told not to. Additionally, the resources align with offender technology use, suggesting offenders use social media platforms that are popular with YP, and migrate abuse across more than one platform. This was also supported by the literature.

Despite research suggesting the "stranger danger" messaging of prevention resources is ineffective, a notable portion of prevention resources still implement this messaging. Additionally, confusion exists surrounding the terminology resources use to refer to OCSEA offenders, which may be a roadblock for effective primary prevention. Highly stigmatised terms, such as "predator" and "stranger", align less with the social factors influencing how YP use the internet and whom they believe they communicate and develop relationships with online. Empowering YP to successfully independently navigate online environments and identify and disengage from potentially harmful situations supports the developmental, cognitive, and social factors of YP's internet use more than the maintenance of technical controls which may instead encourage risky online behaviour. Whilst some primary prevention resources do align with the developmental, cognitive, and social factors influencing YP's internet use, more needs to be done to support rather than hinder these factors to reduce OCSEA risks.

References

- Açar, K. V. (2016). Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology*, 10(2), 110–126. https://doi.org/10.5281/zenodo.163398/IJCC
- Ali, S. & Paash, S. A. (2022). A systematic review of the technology enabled child sexual abuse (OCSA) & its impacts. *Journal of Legal, Ethical and Regulatory Issues*, 25(5), 1–18. https://www.researchgate.net/publication/361866237_A_SYSTEMATIC_REVIEW_OF_TH E_TECHNOLOGY_ENABLED_CHILD_SEXUAL_ABUSE_OCSA_ITS_IMPACTS
- Australian Centre to Counter Child Exploitation. (n.d.). *ThinkUKnow: Our program*. https://www.thinkuknow.org.au/index.php/about/our-program
- Australian Centre to Counter Child Exploitation. (2020). Online child sexual exploitation:

 Understanding community awareness, perceptions, attitudes and preventative behaviours.

 https://www.accce.gov.au/sites/default/files/2021-02/ACCCE_ResearchReport_OCE_acc.pdf
- Babchishin, K. M., Hanson, R. K., & Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual Abuse: Journal of Research and Treatment*, 23(1), 92–123. https://doi.org/10.1177/1079063210370708
- Bleakley, P., Martellozzo, E., Spence, R., & DeMarco, J. (2024). Moderating online child sexual abuse material (CSAM): Does self-regulation work, or is greater state regulation needed? *European Journal of Criminology*, 21(2), 231–250. https://doi.org/10.1177/14773708231181361
- Bloxsom, G., McKibbin, G., Humphreys, C., Davidson, J., & Halfpenny, N. (2024). Five forms of coerced "self-produced" child sexual exploitation material: A critical interpretive synthesis.

- *Trauma, Violence, and Abuse, 25*(5), 4230–4244. https://doi.org/10.1177/15248380241271376
- Boer, H. & Seydel, E. R. (1996). Protection motivation theory. In M. Conner & P. Norman (Eds.), *Predicting Health Behaviour: Research and Practice with Social Cognitive Models* (pp. 95–120). Open University Press. https://ris.utwente.nl/ws/portalfiles/portal/5592716/K465_.PDF
- Borca, G., Bina, M., Keller, P. S., Gilbert, L. R., & Begotti, T. (2015). Internet use and developmental tasks: Adolescents' point of view. *Computers in Human Behavior*, *52*, 49–58. https://doi.org/10.1016/j.chb.2015.05.029
- Brantingham, P. & Faust, F. (1976). A conceptual model of crime prevention. *Crime & Delinquency*, 22(3), 284–296. https://doi.org/10.1177/001112877602200302
- Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
- Burgess, E. S. & Wurtele, S. K. (1998). Enhancing parent-child communication about sexual abuse: A pilot study. *Child Abuse & Neglect*, 22(11), 1167–1175.
- Campis, L. K., Prentice-Dunn, S., & Lyman, R. (1989). Coping appraisal and parents' intentions to inform their children about sexual abuse: A protection motivation theory analysis. *Journal of Social and Clinical Psychology*, 8(3), 304–316. https://www.proquest.com/scholarly-journals/coping-appraisal-parents-intentions-inform-their/docview/1292230550/se-2
- Chauviré-Geib, K. & Fegert, J. M. (2024). Victims of technology-assisted child sexual abuse: A scoping review. *Trauma, Violence, and Abuse*, 25(2), 1335–1348. https://doi.org/10.1177/15248380231178754
- Choo, K.-K. R. (2009). Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences. www.aic.gov.au

- Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on Facebook: The effect of having a bad experience on online behavior. *Journal of Adolescent Research*, 27(6), 714–731. https://doi.org/10.1177/0743558411432635
- Danovitch, J. H. (2019). Growing up with Google: How children's understanding and use of internet-based devices relates to cognitive development. *Human Behavior and Emerging Technologies*, *1*(2), 81–90. https://doi.org/10.1002/hbe2.142
- Davis, V. (2012). Interconnected but underprotected? Parents' methods and motivations for information seeking on digital safety issues. *Cyberpsychology, Behavior, and Social Networking*, 15(12), 669–674. https://doi.org/10.1089/cyber.2012.0179
- Ferragut, M., Cerezo, M. V., Ortiz-Tallo, M., & Rodríguez-Fernandez, R. (2023). Effectiveness of child sexual abuse prevention programs on knowledge acquisition: A meta-analytical study. *Child Abuse and Neglect*, *146*, 106489. https://doi.org/10.1016/j.chiabu.2023.106489
- Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of online sexual offenses against children in the US. *JAMA Network Open*, *5*(10), E2234471. https://doi.org/10.1001/jamanetworkopen.2022.34471
- Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2021). Youth internet safety education: Aligning programs with the evidence base. *Trauma, Violence, and Abuse*, 22(5), 1233–1247. https://doi.org/10.1177/1524838020916257
- Garmendia, M., Garitaonandia, C., Martínez, G., & Casado, M. Á. (2012). The effectiveness of parental mediation. In S. Livingstone (Ed.), *Children, risk and safety on the Internet:**Research and policy challenges in comparative perspective (pp. 231–244). Bristol University Press. https://muse.jhu.edu/book/79802.

- Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse and Neglect*, 80, 238–248. https://doi.org/10.1016/j.chiabu.2018.03.031
- Ghosh, A. K., Badillo-Urquiola, K., Guha, S., Laviola, J. J., & Wisniewski, P. J. (2018, April 21-26). Safety vs. surveillance: What children have to say about mobile apps for parental control. Conference on Human Factors in Computing Systems, Montreal, QC, Canada. https://doi.org/10.1145/3173574.3173698
- Given, L. M., Winkler, D. C., Willson, R., Davidson, C., Danby, S., & Thorpe, K. (2016).
 Watching young children "play" with information technology: Everyday life information seeking in the home. *Library & Information Science Research*, 38(4), 344–352.
 https://doi.org/10.1016/j.lisr.2016.11.007
- Hayes, B., James, A., Barn, R., & Watling, D. (2022). Children's risk and benefit behaviours on social networking sites. *Computers in Human Behavior*, 130, 107147.
 https://doi.org/10.1016/j.chb.2021.107147
- Henry, N., Flynn, A., & Powell, A. (2018). Policing image-based sexual abuse: Stakeholder perspectives. *Police Practice and Research*, 19(6), 565–581.
 https://doi.org/10.1080/15614263.2018.1507892
- Henry, N. & Umbach, R. (2024). Sextortion: Prevalence and correlates in 10 countries. *Computers in Human Behavior*, 158, 108298. https://doi.org/10.1016/j.chb.2024.108298
- Henshaw, M., Ogloff, J. R. P., & Clough, J. A. (2018). Demographic, mental health, and offending characteristics of online child exploitation material offenders: A comparison with contact-only and dual sexual offenders. *Behavioral Sciences and the Law*, *36*(2), 198–215. https://doi.org/10.1002/bsl.2337

- Internet Watch Foundation. (2024). *Annual Data and Insights Report 2024*. https://www.iwf.org.uk/annual-data-insights-report-2024/
- Johnson, G. (2006). Internet use and cognitive development: A theoretical framework. *E-Learning* and Digital Media, 3(4), 565–573. https://doi.org/10.2304/elea.2006.3.4.565
- Johnson, G. M. (2010). Internet use and child development: Validation of the ecological technosubsystem. *Educational Technology & Society*, *13*(1), 1176–3647.
- Kennedy, J. & Lynch, H. (2016). A shift from offline to online: Adolescence, the internet and social participation. *Journal of Occupational Science*, 23(2), 156–167. https://doi.org/10.1080/14427591.2015.1117523
- Klobas, J. E. & Clyde, L. A. (2021). Social influence and internet use. *Library Management*, 22, 61–67. https://doi.org/10.1108/01435120110358943
- Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process, and offender characteristics. *Trauma, Violence, and Abuse*, 15(2), 126–139. https://doi.org/10.1177/1524838013511543
- Kloess, J. A., Hamilton-Giachritsis, C. E., & Beech, A. R. (2019). Offense Processes of Online Sexual Grooming and Abuse of Children Via Internet Communication Platforms. *Sexual Abuse: Journal of Research and Treatment*, 31(1), 73–96. https://doi.org/10.1177/1079063217720927
- Lapsia, S. (2024). The tech platforms used by online child sexual abuse offenders: Research report with actionable recommendations for the tech industry. www.suojellaanlapsia.fi/en
- Leonard, M. M. (2010). "I did what I was directed to do but he didn't touch me": The impact of being a victim of internet offending. *Journal of Sexual Aggression*, 16(2), 249–256. https://doi.org/10.1080/13552601003690526

- Liau, A. K., Khoo, A., & Ang, H. (2005). Factors influencing adolescents engagement in risky internet behavior. *Cyberpsychology & Behavior*, 8(6), 513–520. www.liebertpub.com
- Livingstone, S., Haddon, L., Goerzig, A., Profile, S., & Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. https://www.researchgate.net/publication/50902989
- Martellozzo, E. (2017). Online sexual grooming. In E. Martellozzo & E. Jane (Eds.), *Cybercrime* and its victims (pp. 108–128). Routledge. https://doi.org/10.4324/9781315637198
- Martin, J. (2015). Conceptualizing the harms done to children made the subjects of sexual abuse images online. *Child and Youth Services*, *36*(4), 267–287. https://doi.org/10.1080/0145935X.2015.1092832
- Munakata, Y., Casey, B. J., & Diamond, A. (2004). Developmental cognitive neuroscience:

 Progress and potential. *Trends in Cognitive Sciences*, 8(3), 122–128.

 https://doi.org/10.1016/j.tics.2004.01.005
- National Center for Missing and Exploited Children. (2024). 2024 CyberTipline Report. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata
- National Society for the Prevention of Cruelty to Children. (2022, July 12). *Online grooming* crimes have risen by more than 80% in four years. https://www.nspcc.org.uk/about-us/news-opinion/2022/online-grooming-crimes-rise/
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1–13. https://doi.org/10.1177/1609406917733847

- Nurse, A. M. (2017). Construction of the offender in child sexual abuse prevention training for adults. *Journal of Criminal Justice Education*, 28(4), 598–615.
 https://doi.org/10.1080/10511253.2017.1299423
- O'Malley, R. L., Holt, K., Holt, T. J., & Rodriguez, J. (2023). Minor-focused sextortion by adult strangers: A crime script analysis of newspaper and court cases. *Criminology and Public Policy*, 22(4), 779–801. https://doi.org/10.1111/1745-9133.12634
- O'Malley, R. L. & Holt, K. M. (2022). Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. *Journal of Interpersonal Violence*, *37*(1–2), 258–283. https://doi.org/10.1177/0886260520909186
- O'Neill, B. & Staksrud, E. (2012). Policy implications and recommendations: now what? In S. Livingstone (Ed.), *Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective.* (pp. 339–354). Bristol University Press. https://muse.jhu.edu/book/79802.
- Patterson, A., Ryckman, L., & Guerra, C. (2022). A systematic review of the education and awareness interventions to prevent online child sexual abuse. *Journal of Child and Adolescent Trauma*, 15(3), 857–867. https://doi.org/10.1007/s40653-022-00440-x
- Peters, R. J. (2021). Technology-facilitated child abuse. In R. Geffner, J. W. White, L.K. Hamberger, A. Rosenbaum, V. Vaughan-Eden, & V. I. Vieth (Eds.), *Handbook of Interpersonal Violence and Abuse Across the Lifespan* (pp. 953–973). Springer. https://doi.org/10.1007/978-3-319-89999-2 20
- Prievara, D. K., Piko, B. F., & Luszczynska, A. (2019). Problematic internet use, social needs, and social support among youth. *International Journal of Mental Health and Addiction*, 17(4), 1008–1019. https://doi.org/10.1007/s11469-018-9973-x

- Prikhidko, A. & Kenny, M. C. (2021). Examination of parents' attitudes toward and efforts to discuss child sexual abuse prevention with their children. *Children and Youth Services Review*, *121*. https://doi.org/10.1016/j.childyouth.2020.105810
- Quayle, E. (2022). Self-produced images, sexting, coercion and children's rights. *ERA Forum*, 23(2), 237–251. https://doi.org/10.1007/s12027-022-00714-9
- Ray, A. & Henry, N. (2024). Sextortion: A scoping review. *Trauma, Violence, and Abuse*, 26(1), 138–155. https://doi.org/10.1177/15248380241277271
- Rimer, J. R. (2024). Child Sexual Exploitation. In Oxford Research Encyclopedia of Criminology and Criminal Justice. Oxford University Press.
 https://doi.org/10.1093/acrefore/9780190264079.013.780
- Ringenberg, T. R., Seigfried-Spellar, K. C., Rayz, J. M., & Rogers, M. K. (2022). A scoping review of child grooming strategies: pre- and post-internet. *Child Abuse and Neglect*, *123*, 105392. https://doi.org/10.1016/j.chiabu.2021.105392
- Salter, M. & Whitten, T. (2022). A comparative content analysis of pre-internet and contemporary child sexual abuse material. *Deviant Behaviour*, 43(9), 1120-1134. https://doi.org/10.1080/01639625.2021.1967707
- Shelton, J., Eakin, J., Hoffer, T., Muirhead, Y., & Owens, J. (2016). Online child sexual exploitation: An investigative analysis of offender characteristics and offending behavior.

 *Aggression and Violent Behavior, 30, 15–23. https://doi.org/10.1016/j.avb.2016.07.002
- Shin, W. & Ismail, N. (2014). Exploring the role of parents and peers in young adolescents' risk taking on social networking sites. *Cyberpsychology, Behavior, and Social Networking*, 17(9), 578–583. https://doi.org/10.1089/cyber.2014.0095

- Sinclair, R., Duval, K., Ste-Marie, M., Bennell, C., & Pozzulo, J. (2018). Reframing stranger danger: Online child sexual exploitation. In J. Pozzulo & C. Bennell (Eds.), Working with Trauma-Exposed Children and Adolescents (pp. 149–182). Routledge. https://doi.org/10.4324/9780429423017-7
- Sturges, J. W. & Rogers, R. W. (1996). Preventive health psychology from a developmental perspective: An extension of protection motivation theory. *Health Psychology*, *15*(3), 158–166. https://psycnet.apa.org/record/1996-03679-002
- Thorn. (2017). Sextortion: Summary findings from a 2017 survey of 2,097 survivors. https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf
- Thorn. (2025). *Child sexual abuse material (CSAM)*. https://www.thorn.org/research/child-sexual-abuse-material-csam/
- Throuvala, M. A., Griffiths, M. D., Rennoldson, M., & Kuss, D. J. (2019). Motivational processes and dysfunctional mechanisms of social media use among adolescents: A qualitative focus group study. *Computers in Human Behavior*, *93*, 164–175. https://doi.org/10.1016/j.chb.2018.12.012
- Tilleczek, K., Bell, B., & Munro, M. (2019). Youth well-being and digital media. In K. Tilleczek & V. Campbell (Eds.), *Youth in the digital age: Paradox, promise, predicament* (pp. 39–59). Routledge. https://doi.org/https://doi.org/10.4324/9780429464751
- Topping, K. J. & Barron, I. G. (2009). School-based child sexual abuse prevention programs: A review of effectiveness. *Review of Educational Research*, 79(1), 431–463. https://doi.org/10.3102/0034654308325582

- Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016).
 Understanding online safety behaviors: A protection motivation theory perspective.
 Computers and Security, 59, 138–150. https://doi.org/10.1016/j.cose.2016.02.009
- Villacampa, C. & Gómez, M. J. (2017). Online child sexual grooming: Empirical findings on victimisation and perspectives on legal requirements. *International Review of Victimology*, 23(2), 105–121. https://doi.org/10.1177/0269758016682585
- von Weiler, J., Haardt-Becker, A., & Schulte, S. (2010). Care and treatment of child victims of child pornographic exploitation (CPE) in Germany. *Journal of Sexual Aggression*, 16(2), 211–222. https://doi.org/10.1080/13552601003759990
- Walsh, K., Mathews, B., Parvin, K., Smith, R., Burton, M., Nicholas, M., Napier, S., Cubitt, T.,
 Erskine, H., Thomas, H. J., Finkelhor, D., Higgins, D. J., Scott, J. G., Flynn, A., Noll, J.,
 Malacova, E., Le, H., & Tran, N. (2025). Prevalence and characteristics of online child sexual victimization: Findings from the Australian Child Maltreatment Study. *Child Abuse and Neglect*, 160, 107186. https://doi.org/10.1016/j.chiabu.2024.107186
- Walsh, W. A. & Tener, D. (2022). "If you don't send me five other pictures I am going to post the photo online": A qualitative analysis of experiences of survivors of sextortion. *Journal of Child Sexual Abuse*, 31(4), 447–465. https://doi.org/10.1080/10538712.2022.2067093
- Wang, G., Zhao, J., Van Kleek, M., & Shadbolt, N. (2021). Protection or punishment? Relating the design space of parental control apps and perceptions about them to support parenting for online safety. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1–26. https://doi.org/10.1145/3476084
- Weston, S. & Mythen, G. (2020). Working with and negotiating "risk": Examining the effects of awareness raising interventions designed to prevent child sexual exploitation. *British Journal of Criminology*, 60(2), 323–342. https://doi.org/10.1093/bjc/azz045

- White, C. M., Gummerum, M., & Hanoch, Y. (2015). Adolescents' and young adults' online risk taking: The role of gist and verbatim representations. *Risk Analysis*, *35*(8), 1407–1422. https://doi.org/10.1111/risa.12369
- Whittle, H. C., Hamilton-Giachritsis, C., & Beech, A. R. (2013a). Victims' voices: The impact of online grooming and sexual abuse. *Universal Journal of Psychology*, 1(2), 59–71. https://doi.org/10.13189/ujp.2013.010206
- Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013b). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*, 18(1), 62–70. https://doi.org/10.1016/j.avb.2012.09.003
- Wolak, J., Finkelhor, D., & Mitchell, K. (2004). Internet-initiated sex crimes against minors:

 Implications for prevention based on findings from a national study. *Journal of Adolescent Health*, 35(5), 424.e11-424.e20. https://doi.org/10.1016/j.jadohealth.2004.05.006
- Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2010). Online "predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. *Psychology of Violence*, *I*(S), 13–35. https://doi.org/10.1037/2152-0828.1.S.13
- Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 62(1), 72–79.
 https://doi.org/10.1016/j.jadohealth.2017.08.014
- World Health Organisation. (2022). What works to prevent online violence against children? https://iris.who.int/bitstream/handle/10665/364706/9789240062061-eng.pdf
- Wright, M. F. (2014). Longitudinal investigation of the associations between adolescents' popularity and cyber social behaviors. *Journal of School Violence*, *13*(3), 291–314. https://doi.org/10.1080/15388220.2013.849201

Wurtele, S. K., & Kenny, M. C. (2016). Technology-Related Sexual Solicitation of Adolescents: A Review of Prevention Efforts. *Child Abuse Review*, 25(5), 332–344. https://doi.org/10.1002/car.2445

Appendices

Appendix A: Search terms

(Online OR digital OR carriage service OR technology-facilitated OR internet-based OR technology-based OR internet-facilitated) AND (child sexual abuse material OR CSAM OR child sexual exploitation material OR CSEM OR child abuse material)

(Online OR digital OR carriage service OR technology-facilitated OR internet-based OR technology-based OR internet-facilitated) AND (CAM OR child porn* OR child exploitation material OR CEM OR image-based abuse OR image-based exploitation OR child abuse media OR child exploitation media OR indecent images of children OR digital child abuse imagery OR digital child exploitation)

(virtual OR cyber OR cyberspace OR social networking site OR social network OR e-Safety OR internet OR mobile OR phone OR technology OR tech OR social media OR digital media) AND (child sexual abuse material OR CSAM OR child sexual exploitation material OR CSEM OR child abuse material)

(virtual OR cyber OR cyberspace OR social networking site OR social network OR e-Safety OR internet OR mobile OR phone OR technology OR tech OR social media OR digital media) AND (CAM OR child porn* OR child exploitation material OR CEM OR image-based abuse OR image-based exploitation OR child abuse media OR child exploitation media OR indecent images of children OR digital child abuse imagery OR digital child exploitation)

(Online OR digital OR carriage service OR technology-facilitated OR internet-based OR technology-based OR internet-facilitated) AND (child luring OR child grooming OR grooming OR luring OR enticement OR child enticement OR groomed OR groom OR unwanted contact OR unsolicited contact)

(e-safety OR virtual OR cyber OR cyberspace OR social networking site OR social network OR internet OR mobile OR phone OR technology OR tech OR social media OR digital media) AND (child lur* OR luring OR sexually solicit OR child sexual solicitation OR approach* child*)

(Online OR digital OR carriage service OR technology-facilitated OR internet-based OR technology-based OR internet-facilitated) AND (child lur* OR luring OR sexually solicit OR child sexual solicitation OR approach* child*)

(e-safety OR virtual OR cyber OR cyberspace OR social networking site OR social network OR internet OR mobile OR phone OR technology OR tech OR social media OR digital media) AND (child luring OR child grooming OR grooming OR luring OR enticement OR child enticement OR groomed OR groom OR unwanted contact OR unsolicited contact)

(Online OR digital OR carriage service OR technology-facilitated OR internet-based OR technology-based OR internet-facilitated) AND (sextortion OR child sextortion OR youth sextortion OR youth sexual extortion OR sexual extortion OR child sexual extortion)

(Online OR digital OR carriage service OR technology-facilitated OR internet-based OR technology-based OR internet-facilitated) AND (child extortion OR extortion OR threats OR threatening OR threaten OR sexually threatening OR sex* extort*)

(Online OR digital OR carriage service OR technology-facilitated OR internet-based OR technology-based OR internet-facilitated) AND (sexual* brib* OR threaten OR blackmail OR ransom OR brib*)

(e-safety OR virtual OR cyber OR cyberspace OR social networking site OR social network) AND (sextortion OR child sextortion OR youth sexual extortion OR sexual extortion OR child sexual extortion)

(e-safety OR virtual OR cyber OR cyberspace OR social networking site OR social network) AND (child extortion OR extortion OR threats OR threatening OR threatening OR sexually threatening OR sex* extort*)

(e-safety OR virtual OR cyber OR cyberspace OR social networking site OR social network) AND (sexual* brib* OR threaten OR blackmail OR ransom OR brib*)

(internet OR mobile OR phone OR technology OR tech OR social media OR digital media) AND (sextortion OR child sextortion OR youth sextortion OR youth sexual extortion OR child sexual extortion)

(internet OR mobile OR phone OR technology OR tech OR social media OR digital media) AND (child extortion OR extortion OR threats OR threatening OR threatening OR sexually threatening OR sex* extort*)

(internet OR mobile OR phone OR technology OR tech OR social media OR digital media) AND (sexual* brib* OR threaten OR blackmail OR ransom OR brib*)

(resources OR resource OR initiatives OR initiative OR information OR education OR educate OR awareness OR response for OR response to OR guidance OR materials OR project OR guide OR materials OR program*) for (parent* OR caregiver* OR guardian* OR carer* OR caretaker* OR mum* OR dads* OR teen* OR child* OR tween* OR youth* OR adolesc* OR young person OR YP OR kid* OR mother* OR father*)

Appendix B: Websites selected to search for resources

eSafety	NTPOL	In The Know	Internetmatters.org	NCMEC
Kidshelpline	ACCCE	Ministry of Education NZ	Safer Internet Centre	ICMEC
ICMEC Australia	Education QLD	Charter School Agency	Pace	ISPCAN
Project Paradigm	Education NSW	Education Payroll (Rārangi Utu ā-Mātauranga)	Parents Protect	Internet Safety 101
Bravehearts	Education NT	Network 4 Learning (N4L)	ThinkUKnow	FBI
Daniel Morcombe	Department for	Teaching Council of	Association of Child	FTC
Foundation	Education SA	Aotearoa New Zealand (Te Tari Arotake Mātauranga)	Protection Professionals	
Scamwatch	Department of Education WA	Tertiary Education Commission (Te Amorangi Mātauranga Matua)	Virtual Global Taskforce	US Department of Education
AUSTRAC	Education Victoria	Education New Zealand (Manapou ki te Ao)	Department for Education	Thriving in Games Group
Department of Home Affairs	ACT Education Directorate	Education Review Office (Te Tari Arotake Mātauranga)	Department of Health & Social Care	RAINN
AFP	Raising Children Network	New Zealand Qualifications Authority	Department for Education (England)	kidzsmarts
QPS	Neighbourhood Watch	Te Kura (Te Aho o Te Kura Pounamu)	Department of Education (Northern Ireland)	
SAPOL	ThinkUknow	Ofcom	Education Scotland	
VICPOL	Netsafe	NSPCC	Department for Education and Skills (Wales)	
WAPOL	Keep it Real Online	Internet Watch Foundation	Childlight	
NSWPOL	NZ Police	Marie Collins Foundation	Federal Communications commission	

Appendix C: List of analysed resources

Resource	Publishing entity	Resource title	Link	Country
CSAM 04 AUS	ACCCE	What is online child sexual exploitation?	https://www.accce.gov.au/sites/default/files/2021-06/Factsheet%20- %20What%20is%20online%20child%20sexual%20exploitation%3F. pdf	AUS
CSAM 05 AUS	ACCCE	What is online child sexual exploitation?	https://www.accce.gov.au/help-and-support/what-is-online-child-exploitation	AUS
CSAM 07 AUS	eSafety	Sending nudes and sexting	https://www.eSafety.gov.au/parents/issues-and-advice/sending-nudes- sexting	AUS
CSAM 08 AUS	Bravehearts	Covid-19 and online child exploitation: Understanding and responding to risks associated with young people's increased online activities	https://bravehearts.org.au/covid-19-and-online-child-exploitation-understanding-and-responding-to-risks-associated-with-young-peoples-increased-online-activities/	AUS
CSAM 09 UK	internetmatt ers.org	Protect children from sexting	https://www.internetmatters.org/issues/sexting/protect-children-from-sexting/	UK
CSAM 10 AUS	Kids Helpline	Sexting	https://kidshelpline.com.au/teens/issues/sexting	AUS
CSAM 11 AUS	Kids Helpline	Sexting and the impacts on young people	https://kidshelpline.com.au/parents/issues/sexting-and-impacts-young-people	AUS
CSAM 12 AUS	ThinkUKno w	Self-generated child abuse material	https://www.thinkuknow.org.au/find-advice/self-generated-child-abuse-material#need-to-know	AUS
CSAM 13 AUS	ThinkUKno w	Self-generated sexual content or personal image sharing	https://www.thinkuknow.org.au/sites/default/files/2020-10/Fact%20sheet%20Self-%20generated%20sexual%20content%20or%20personal%20image%20sharing.pdf	AUS
CSAM 14 AUS	ThinkUKno w	Sexting, selfies and pics	https://www.thinkuknow.org.au/find-advice/sexting-selfies-and-pics	AUS

CSAM 17 UK	CEOP Education	#AskTheAwkward	https://www.CEOP Education/parents/ask-the-awkward/	UK
CSAM 18 UK	Internet Watch Foundation	Make sure your home doesn't have an open door to child sexual abusers	https://Internet Watch Foundation.uk/wp-content/uploads/2023/08/Parent_Resource_UpdatedJuly2023.pdf	UK
CSAM 19 UK	CEOP Education	Sending nudes	https://www.CEOP Education/11_18/lets-talk-about/nudes/sending-nudes/	UK
CSAM 20 UK	Childnet	Nudes	https://www.Childnet/help-and-advice/nudes-11-18-year-olds/	UK
CSAM 21 UK	Internet Watch Foundation	Online Child Sexual Abuse	https://Internet Watch Foundation.uk/what-you-need-to-know/	UK
CSAM 22 UK	Childnet	Sexting	https://www.Childnet/help-and-advice/sexting/	UK
CSAM 24 UK	Stop It Now	Tip Sheet: Keeping children and youth safe online	https://www.stopitnow.org/ohc-content/keeping-children-and-youth-safe-online	UK
CSAM 25 UK	Stop It Now	How do people sexually exploit children and youth online?	https://www.stopitnow.org/ohc-content/how-do-people-sexually-exploit-children-and-youth-online	UK
CSAM 30 USA	NCMEC	Talking to Teens About Sexting	https://www.missingkids.org/content/dam/netsmartz/downloadable/tipsheets/Talking%20to%20Teens%20About%20Sexting.pdf	USA
CSAM 31 USA	NCMEC	Think before you send	https://www.missingkids.org/content/dam/netsmartz/downloadable/tipsheets/Think%20Before%20You%20Send.pdf	USA
CSAM 32 AUS	Victoria Department of Education	Sexting	https://www.education.vic.gov.au/Documents/about/programs/bullyst oppers/smsexting.pdf	AUS

CSAM 33 AUS	ACCCE	Jack Changes the Game	https://www.thinkuknow.org.au/sites/default/files/2022-10/eBook%20-%20Jack%20Changes%20the%20Game_0.pdf	AUS
CSAM 36 AUS	Cape	Conversations with kids	https://s3.amazonaws.com/kajabi-storefronts-production/file-uploads/sites/2147658237/themes/2159596452/downloads/66445e-3a72-e3f5-a1a4-f0d76c0bdf32 Online Safety Series 6 - 11yo.pdf	AUS
CSAM 37 UK	NSPCC	Talking to your child about the risks of sharing nudes	https://www.nspcc.org.uk/keeping-children-safe/online-safety/sexting-sending-nudes/	UK
CSAM 40 UK	Children's commission er	Parents Guide: Talking to your child about online sexual harassment	https://assets.childrenscommissioner.gov.uk/wpuploads/2021/12/cco talking to your child about online sexual harassment a- guide for parents dec 2021.pdf	UK
CSAM 42 UK	Childnet	Supporting your child with SEND to thrive online: Nudes	https://www.Childnet/wp-content/uploads/2022/05/Nudes-Thrive-online.pdf	UK
CSAM 43 AUS	raisingchild ren.net	Sexting: talking with teenagers	https://raisingchildren.net.au/teens/entertainment- technology/pornography-sexting/sexting-teens	AUS
CSAM 45 AUS	Headspace	Understanding sexting and image-based abuse - for families	https://headspace.org.au/explore-topics/supporting-a-young-person/sexting-and-image-based-abuse/	AUS
CSAM 46 AUS	Michelle Mitchell	They sent a nude: Thoughts to prevent, understand and respond to sexting	https://michellemitchell.org/parentingteens-sendingnudes/?srsltid=AfmBOopVf_ryBNy3qCboOvlI6Rty2yqMT5 NnjigK5cbP45KREezlogul	AUS
CSAM 47 AUS	ReachOut	How to talk to your teenager about sexting	https://parents.au.reachout.com/friendships-and-dating/sex/how-to-talk-to-your-teenager-about-sexting	AUS
CSAM 50 UK	Catch 22	Is someone asking you for a nude picture	https://d1mdc3nx9zxju4.cloudfront.net/prod/uploads/2024/02/Issomeone-asking-you-for-a-nude-picture-2024.pdf	UK
CSAM 51 AUS	Safe on Social	Safe on Social: Sexting & Child Pornography cheat sheet	https://www.lynehamhs.act.edu.au/ data/assets/pdf_file/0018/44041 5/SoS_Cheat_SheetSexting_and_Child_Pornography.pdf	AUS

CSAM 57 NZ	Press Pause	Sexualised images	https://presspause.co.nz/sexualised-images	NZ
CSAM 59 USA	Connected kids guide	Key online safety messages to share with children	https://connectedkidsguide.com/section-11-key-online-safety-messages-to-share-with-children/	USA
CSAM 60 UK	Childline	Sexting and nudes	https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/	UK
CSAM 63 UK	Think before you share	We're here to help	https://www.thinkbeforeyoushare.org/teenagers	UK
CSAM 64 UK	Think before you share	Let's talk about nudes	https://www.thinkbeforeyoushare.org/parents-and-carers	UK
CSAM 65 UK	internetmatt ers.org	What parents need to know about sexual image-sharing among kids	https://www.internetmatters.org/hub/research/parents-guide-child-sexual-image-sharing/	UK
CSAM 73 UK	internetmatt ers.org	Teens and online dating: Advice and support for parents	https://www.internetmatters.org/wp-content/uploads/2020/02/Inernet- Matters-Online-Dating-Guide-v3.pdf	UK
CSAM 75 UK	internetmatt ers.org	Learn about sexting	https://www.internetmatters.org/issues/sexting/learn-about-sexting/	UK
CSAM 76 UK	CEOP Education	7 Questions parents ask about nude selfies	https://www.CEOP Education/parents/articles/7-questions-parents-ask-about-nude-selfies/	UK
CSAM 78 UK	internetmatt ers.org	How can vulnerable young people be protected from the risks of online dating	https://www.internetmatters.org/hub/expert-opinion/how-can-vulnerable-young-people-be-protected-from-the-risks-of-online-dating/	UK
CSAM 79 UK	internetmatt ers.org	So you got naked online	https://www.internetmatters.org/wp-content/uploads/2020/10/SWGfL-SYGNO-SEND-guide-for-young-people_v2.pdf	UK
CSAM 81 UK	Parents Protect	Internet safety Useful information for parents and carers	https://www.parentsprotect.co.uk/files/Leaflet%20for%20parents%20 Oct%202014%20WITHOUT%20BEATBULLYING.pdf	UK

CSAM 86	eSafety	I'm being pressured to send	https://www.eSafety.gov.au/young-people/being-pressured-to-send-	AUS
AUS	- 0	nudes	nudes	
CSAM 87	eSafety	Young people's guide to	https://www.eSafety.gov.au/sites/default/files/2022-	AUS
AUS		dealing with online sexual	01/Online%20sexual%20harassment%20and%20image-	
		harassment and image-based	based%20abuse%20-	
		abuse	%20Young%20People%20Guide.pdf?v=1741839339959	
CSAM 88	Project	The online risks of child	https://projectparadigm.com.au/userfiles/files/PDF_Resources/PP_On	AUS
AUS	paradigm	sexual exploitation	line%20Risks%20of%20CSE_Resource%20Sheet.pdf	
CSAM 89	Raising	How to talk with children	https://raisingchildren.net.au/school-age/media-technology/online-	AUS
AUS	Children	about sexting: 6-11 years	safety/sexting-early-conversations	
	Network			
CSAM 90	Netsafe	Online relationships	https://cdn.sanity.io/files/8y8wsx0z/production/a969972a69cb8e9a4ff	NZ
NZ			db6a3fcb9b87fcc8d3044.pdf	
CSAM 91	Netsafe	Nudes #thebarefacts	https://barefacts.Netsafe.org.nz/	NZ
NZ				
CSAM 94	UK Safer	Helping parents and carers	https://saferinternet.org.uk/online-issue/coerced-online-child-	UK
UK	internet	keep their children safer	<u>sexualabuse</u>	
66.115.05	Centre	online		* ***
CSAM 95	Parents	Nudes and sexual selfies	https://www.parentsprotect.co.uk/nudes-sexual-selfies-sexting.htm	UK
UK	protect UK	(sexting)	1 // OPODE1 / 1.11.1 1	T 177
CSAM 97	CEOP	Younger children sharing	https://www.CEOP Education/parents/articles/Has-your-child-shared-	UK
UK	Education	pictures or videos online	a-picture-or-video-online-/	T 177
CSAM 98	CEOP	Online/offline: Different	https://www.CEOP Education/globalassets/parents	UK
UK	Education	worlds?	carers/pdf/asktheawkward-parentscarers-help-sheets-updated-2.pdf	
CSAM 99	Internet	Online predators: Child sex	https://interNetsafety101.org/CSAM	USA
UK	Safety 101	abuse material (CSAM)		
CSAM	eSafety	The hard-to-have	https://www.eSafety.gov.au/parents/issues-and-advice/hard-to-have-	AUS
100 AUS		conversations	<u>conversations</u>	
SEXTOR	ThinkUKno	Myth buster	https://www.thinkuknow.org.au/sites/default/files/2020-	AUS
TION 02	W		10/Fact%20sheet%20Image%20based%20abuse%20and%20sexual%	
AUS			20extortion.pdf	

SEXTOR TION 03 USA	Thorn	Grooming & Sextortion	https://www.thorn.org/research/grooming-and-sextortion/	USA
SEXTOR TION 04 UK	CEOP Education	Online blackmail	https://www.CEOP Education/11_18/lets-talk-about/sexual-abuse/online-blackmail/	UK
SEXTOR TION 05 UK	internetmatt ers.org	What is sextortion?	https://www.internetmatters.org/resources/what-is-sextortion/	UK
SEXTOR TION 06 AUS	ThinkUKno w	Sexual extortion	https://www.thinkuknow.org.au/find-advice/sexual-extortion	AUS
SEXTRO RTION 08 USA	Connect Safely	Parent's Guide to Teen Sextortion Scams	https://connectsafely.org/wp-content/uploads/2022/07/Guide-to-Teen-Sextortion-Scams.pdf	USA
SEXTOR TION 10 USA	NCMEC	Sextortion: What parents should know	https://www.missingkids.org/content/dam/netsmartz/downloadable/tipsheets/sextortion-what-parents-should-know.pdf	USA
SEXTOR TION 13 UK	SWGfl	So you got naked online	https://swgfl.org.uk/assets/documents/so-you-got-naked-online-2024.pdf?_=1732893848	UK
SEXTOR TION 15 UK	Childnet	Sextortion	https://www.Childnet/help-and-advice/sextortion/	UK
SEXTOR TION 16 UK	Childnet	Sextortion	https://www.Childnet/help-and-advice/sextortion-2/	UK
SEXTOR TION 21 USA	Meta	Stop sextortion - caregivers	https://about.meta.com/actions/safety/topics/bullying- harassment/stop-sextortion/caregivers	USA

SEXTOR TION 24 AUS	eSafety	Someone is threatening to share my nudes	https://www.eSafety.gov.au/young-people/someone-threatening-to-share-my-nudes	AUS
SEXTOR TION 26 AUS	ACCCE	Sextortion	https://www.accce.gov.au/sextortionhelp	AUS
SEXTOR TION 27 AUS	ACCCE	Online blackmail and sexual extortion response kit	https://www.accce.gov.au/sites/default/files/2023- 03/Online_blackmail_and_sexual_extortion_response_kit_March202 3.pdf	AUS
SEXTOR TION 28 AUS	ACCCE	This is sextortion	https://www.accce.gov.au/sites/default/files/featured_images/2023-07/sexotrtion%20yellow%20poster%20screenshot%20-austrac.JPG	AUS
SEXTOR TION 34 AUS	ACCCE	Sextrotion: Messaging Kit	https://www.accce.gov.au/sites/default/files/2023- 11/Sextortion_messaging_kit_October2023.pdf	AUS
SEXTOR TION 35 AUS	Victoria Police	Sextortion (sexual extortion)	https://www.police.vic.gov.au/sextortion	AUS
SEXTOR TION 38 USA	FBI	Sextortion	https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion	USA
SEXTOR TION 41 USA	FBI	Financially motivated sextortion	https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion/financially-motivated-sextortion	USA
SEXTOR TION 48 UK	National Crime Agency UK	Financially Motivated Sexual Extortion (Sextortion)	https://www.nationalcrimeagency.gov.uk/what-we-do/crimethreats/kidnap-and-extortion/sextortion	UK
SEXTOR TION 49 AUS	Headspace	Understanding sexual extortion over nude images	https://headspace.org.au/explore-topics/for-young-people/sextortion/	AUS

SEXTOR TION 50 AUS	Bendigo Bank	What are sextortion scams?	https://www.bendigobank.com.au/security/scams/sextortion/	AUS
SEXTOR TION 54 AUS	Kids Helpline	Sextortion: What it is and what to do about it	https://kidshelpline.com.au/teens/issues/sextortion-what-it-and-what-do-about-it	AUS
SEXTOR TION 56 USA	eSafeKids	Sextortion: What you need to know	https://www.esafekids.com.au/post/sextortion	AUS
SEXTOR TION 57 USA	ICE	Sextortion: It's more common than you think	https://www.ice.gov/about-ice/hsi/news/hsi-insider/sextortion	USA
SEXTOR TION 58 USA	SAFE - Stop Abuse For Everyone	Online safety for children and teens: Detecting and preventing sextortion and sexploitation	https://www.safeaustin.org/online-safety-for-children-and-teens-detecting-and-preventing-sextortion-and-sexploitation/	USA
SEXTOR TION 59 USA	Center for Online Safety	Sextortion - What Parents Need to Know	https://www.dropbox.com/scl/fi/oj0dc2hvo8d5s69tv48f6/Sextortion-what-parents-need-to-know.pdf?rlkey=zafainnozkxx5zamudm14ks3t&e=1&dl=0	USA
SEXTOR TION 60 USA	Center for Online Safety	Sextortion and What Parents Need to Know	https://www.centerforonlineSafety.com/blog/sextortion-what-do-i-do	USA
SEXTOR TION 64 UK	NSPCC	Young people's experiences of online sexual extortion or 'sextortion'	https://learning.nspcc.org.uk/media/ylbobz5i/young-people-experiences-sextortion.pdf	UK
SEXTOR TION 71 UK	Childline	Trusting others online	https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/trusting-others-online/	UK
SEXTOR TION 73 UK	Internet Watch Foundation	Sextortion' or sexually coerced extortion help & support	https://www.Internet Watch Foundation.org.uk/resources/sextortion/	UK

SEXTOR TION 76 USA	Internet Safety 101	Sextortion 101: a quick guide for parents and educators	https://interNetsafety101.org/objects/EIE_Sextortion_101.pdf	USA
SEXTOR TION 79 AUS	Project Paradigm	Sextortion	https://projectparadigm.com.au/userfiles/files/PDF Resources/PP SE XTORTION_Online%20Resource%20Sheet.pdf	AUS
SEXTOR TION 81 NZ	Netsafe	Sextortion	http://Netsafe.org.nz/scams/sextortion	NZ
SEXTOR TION 82 UK	CEOP Education	Online blackmail	https://www.CEOP Education/parents/articles/online-blackmail/	UK
GROOMI NG 002 AUS	ThinkUKno w	Myth Buster	https://www.thinkuknow.org.au/sites/default/files/2020-10/Fact%20sheet%20Online%20grooming.pdf	AUS
GROOMI NG 003 AUS	ThinkUKno w	Myth Buster	https://www.thinkuknow.org.au/sites/default/files/2020-10/Fact%20sheet%20Online%20gaming.pdf	AUS
GROOMI NG 004 AUS	ThinkUKno w	Myth Buster	https://www.thinkuknow.org.au/sites/default/files/2020-10/Fact%20sheet%20Instant%20messaging_1.pdf	AUS
GROOMI NG 005 AUS	ThinkUKno w	Myth Buster	https://www.thinkuknow.org.au/sites/default/files/2020- 10/Home%20learning%20activity%20Learning%20about%20safer% 20gaming%20and%20smart%20user%20names.pdf	AUS
GROOMI NG 006 AUS	ThinkUKno w	Myth Buster	https://www.thinkuknow.org.au/sites/default/files/2020-10/Home%20learning%20activity%20Learning%20about%20safer%20online%20%20interactions%20and%20online%20grooming.pdf	AUS
GROOMI NG 007 AUS	ThinkUKno w	Not everyone online is who they say they are	https://www.thinkuknow.org.au/find-advice/not-everyone-online-who-they-say-they-are	AUS

GROOMI NG 008 AUS	Child Safety	Grooming	https://www.childsafety.gov.au/about-child-sexual-abuse/grooming	AUS
GROOMI NG 011 AUS	eSafety	Every online conversation matters	https://www.eSafety.gov.au/sites/default/files/2024-06/Every-Online-Safety-Conversation-Matters-parents-advice-sheet-ENG.pdf?v=1739083688839	AUS
GROOMI NG 012 AUS	eSafety	Child Grooming	https://www.eSafety.gov.au/parents/issues-and-advice/grooming-or-unwanted-contact	AUS
GROOMI NG 013 AUS	eSafety	Someone is contacting me and I don't want them to	https://www.eSafety.gov.au/kids/I-want-help-with/someone-is- contacting-me-and-i-dont-want-them-to	AUS
GROOMI NG 014 AUS	eSafety	Unsafe contact and 'grooming'	https://www.eSafety.gov.au/young-people/unsafe-contact	AUS
GROOMI NG 015 AUS	eSafety	Things to watch out for with online friends	https://www.eSafety.gov.au/kids/I-want-help-with/things-to-watch- out-for-with-online-friends	AUS
GROOMI NG 017 USA	NCMEC	Online Enticement	https://www.missingkids.org/theissues/onlineenticement	USA
GROOMI NG 018 AUS	Education Victoria	Online Grooming	https://www.education.vic.gov.au/Documents/about/programs/bullyst oppers/smgrooming.pdf	AUS
GROOMI NG 019 AUS	eSafety	Privacy and your child	https://www.eSafety.gov.au/parents/issues-and-advice/privacy-child	AUS
GROOMI NG 022 AUS	Kids Helpline	Understanding online grooming	https://kidshelpline.com.au/parents/issues/understanding-online-grooming	AUS

GROOMI NG 023 AUS	eSafeKids	Online Grooming: Minimising opportunity, minimising risk	https://www.esafekids.com.au/post/online-grooming-minimising-opportunity-minimising-risk	AUS
GROOMI NG 026 USA	socialmedia victims.org	Social Media and Online Grooming	https://socialmediavictims.org/sexual-violence/online-grooming/	USA
GROOMI NG 027 AUS	Queensland Police	Who's chatting to your child?	https://www.police.qld.gov.au/policelink-reporting/reporting-cybercrime/children-and-the-internet/whos-chatting-to-your-kids	AUS
GROOMI NG 029 UK	internetmatt ers.org	Learn about online grooming	https://www.internetmatters.org/issues/online-grooming/learn-aboutit/	UK
GROOMI NG 030 UK	CEOP Education	Online grooming	https://www.CEOP Education/11_18/lets-talk-about/sexual-abuse/online-grooming/	UK
GROOMI NG 031 AUS	Kids Helpline	What is online grooming?	https://kidshelpline.com.au/teens/issues/what-online-grooming	AUS
GROOMI NG 032 AUS	Kids Helpline	Social Media and safety	https://kidshelpline.com.au/parents/issues/social-media-and-safety	AUS
GROOMI NG 034 AUS	ThinkUKno w	Learning about online supervision	https://www.thinkuknow.org.au/sites/default/files/2020- 10/Home%20learning%20activity%20Learning%20about%20online %20supervision.pdf	AUS
GROOMI NG 036 NZ	Netsafe.org. nz	Online child grooming: safeguarding on social media and at home	https://Netsafe.org.nz/online-abuse-and-harassment/grooming	NZ
GROOMI NG 039 UK	Childnet	Grooming	https://www.Childnet/help-and-advice/grooming-11-18-year-olds/	UK

GROOMI NG 043 AUS	eSafety	eSafety Early Years Online safety for under 5s	https://www.eSafety.gov.au/sites/default/files/2020- 05/eSafety%20Early%20Years%20booklet_0.pdf?v=1740453563014	AUS
GROOMI NG 046 USA	NCMEC	Protecting your kids online 2.0	https://www.missingkids.org/content/dam/netsmartz/downloadable/tipsheets/Protecting%20Your%20Kids%20Online%202_0.pdf	USA
GROOMI NG 047 UK	Childline	Grooming	https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-grooming/	UK
GROOMI NG 048 USA	Children and Screens	Online sexual exploitation, grooming, and extortion of youth	https://www.childrenandscreens.org/learn-explore/research/online-sexual-exploitation-grooming-and-extortion-of-youth/	USA
GROOMI NG 049 USA	Children and Screens	Teaching online safety to prevent sexual grooming	https://www.childrenandscreens.org/learn-explore/research/teaching-online-safety-to-prevent-sexual-grooming/	USA
GROOMI NG 051 UK	Shorespace	What to do if you think someone has tried to groom you	https://shorespace.org.uk/what-to-do-if/you-think-someone-has-tried-to-groom-you/	UK
GROOMI NG 057 UK	CEOP Education	Sexual Pressure Online	https://www.CEOP Education/11_18/lets-talk-about/sexual-abuse/sexual-pressure-online/	UK
GROOMI NG 058 UK	CEOP Education	What is a catfish	https://www.CEOP Education/11_18/lets-talk-about/relationships/catfishing/	UK
GROOMI NG 063 AUS	ACCCE	Parent & carer social media starter kit: preventing online child sexual exploitation	https://www.accce.gov.au/sites/default/files/2022-02/20220202%20Parents-Carers_SM_v0.3.pdf	AUS
GROOMI NG 066 AUS	Raising Children Network	Online safety: children 6-8 years	https://raisingchildren.net.au/school-age/safety/online-safety/internet-safety-6-8-years	AUS

GROOMI NG 067 AUS	Raising Children Network	Online safety: pre-teens 9-11 years	https://raisingchildren.net.au/pre-teens/entertainment-technology/cyberbullying-online-safety/internet-safety-9-11-years	AUS
GROOMI NG 068 AUS	Raising Children Network	Online safety: teenagers	https://raisingchildren.net.au/teens/entertainment- technology/cyberbullying-online-safety/internet-safety-teens	AUS
GROOMI NG 070 NZ	Keep it real online	Online grooming and sextortion	https://www.keepitrealonline.govt.nz/parents/online-grooming	NZ
GROOMI NG 072 UK	NSPCC	Chat Apps	https://www.nspcc.org.uk/keeping-children-safe/online-safety/social-media/chat-apps/	UK
GROOMI NG 074 UK	NSPCC	Child sexual exploitation	https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/child-sexual-exploitation/	UK
GROOMI NG 075 UK	CEOP Education	Play, Like, Share: Keeping 8- 10 year olds safe online	https://www.CEOP Education/parents/playlikeshare/	UK
GROOMI NG 076 UK	internetmatt ers.org	How to protect children from online sexual harm	https://www.internetmatters.org/hub/news-blogs/how-to-protect-children-from-online-sexual-harm/	UK
GROOMI NG 077 UK	internetmatt ers.org	Online issues impacting neurodivergent children	https://www.internetmatters.org/advice/neurodivergent-children/neurodivergent-online-safety-issues/	UK
GROOMI NG 078 UK	internetmatt ers.org	Online Grooming	https://www.internetmatters.org/wp-content/uploads/2023/01/Internet-Matters-Online-Grooming-guide-Jan23.pdf	UK
GROOMI NG 081 UK	Internet Watch Foundation	Make sure your home doesn't have an open door to child sexual abusers	https://Internet Watch Foundation.uk/	UK

GROOMI NG 086 USA	ICMEC	Connected Kids: A comprehensive guide to ensuring online safety and well-being	https://cdn.icmec.org/wp-content/uploads/2024/04/Connected- Kids_Online-Safety-Guide.pdf	USA
GROOMI NG 087 AUS	eSafety	Keeping children safe online - advice for parents and carers	https://www.eSafety.gov.au/sites/default/files/2022-03/Keeping%20children%20safe%20online%20-%20advice%20for%20parents%20and%20carers%20%28English%29.pdf	AUS
GROOMI NG 094 AUS	eSafety	Talking about child sexual abuse online with 0-12 year olds	https://www.eSafety.gov.au/parents/issues-and-advice/protecting-children-from-sexual-abuse-online/talking-with-0-to-12	AUS
GROOMI NG 095 AUS	eSafety	Talking about online child sexual abuse with 13 to 18 year olds	https://www.eSafety.gov.au/parents/issues-and-advice/protecting-children-from-sexual-abuse-online/talking-with-13-to-18	AUS
GROOMI NG 096 AUS	eSafety	Protecting children from sexual abuse online	https://www.eSafety.gov.au/parents/issues-and-advice/protecting-children-from-sexual-abuse-online	AUS
GROOMI NG 097 AUS	Bravehearts	Online child exploitation	https://bravehearts.org.au/about-child-sexual-abuse/online-child-expoitation/	AUS
GROOMI NG 099 AUS	Daniel Morcombe Foundation	A guide for children and young people: Recognise online grooming	https://danielmorcombe.com.au/wp-content/uploads/2022/09/Recognise_online_grooming_For_children_and_young_people.pdf	AUS
GROOMI NG 100 AUS	Daniel Morcombe Foundation	What do groomers look like?	https://danielmorcombe.com.au/wp-content/uploads/2022/09/What-do-groomers-look-like.pdf	AUS
GROOMI NG 101 AUS	Daniel Morcombe Foundation	Stages of grooming	https://danielmorcombe.com.au/wp-content/uploads/2022/09/Stages_of_grooming.pdf	AUS
GROOMI NG 106 UK	internetmatt ers.org	Protect children from online grooming	https://www.internetmatters.org/issues/online-grooming/protect-your-child/	UK

GROOMI	CEOP	What is sexual grooming?	https://www.CEOP Education/parents/articles/What-is-sexual-	UK
NG 107	Education		grooming/	
UK				
GROOMI	CEOP	Online contacts and staying	https://www.CEOP Education/parents/articles/online-contact-and-	UK
NG 108	Education	safe	staying-safe/	
UK				
GROOMI	Crime	Fact sheet for parents and	https://nsw.crimestoppers.com.au/wp-	AUS
NG 109	Stoppers	carers	content/uploads/2023/12/Crime-Stoppers_Child-Protection_Fact-	
AUS			Sheet 2023-V4.pdf	