What works to prevent online violence against children?





What works to prevent online violence against children?



What works to prevent online violence against children?

ISBN 978-92-4-006206-1 (electronic version) ISBN 978-92-4-006207-8 (print version)

© World Health Organization 2022

Some rights reserved. This work is available under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 IGO licence (CC BY-NC-SA 3.0 IGO; https://creativecommons.org/licenses/by-nc-sa/3.0/igo).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited, as indicated below. In any use of this work, there should be no suggestion that WHO endorses any specific organization, products or services. The use of the WHO logo is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: "This translation was not created by the World Health Organization (WHO). WHO is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition".

Any mediation relating to disputes arising under the licence shall be conducted in accordance with the mediation rules of the World Intellectual Property Organization (http://www.wipo.int/amc/en/mediation/rules/).

Suggested citation. What works to prevent online violence against children? Geneva: World Health Organization; 2022. Licence: CC BY-NC-SA 3.0 IGO. https://creativecommons.org/licenses/by-nc-sa/3.0/igo/

Cataloguing-in-Publication (CIP) data. CIP data are available at http://apps.who.int/iris.

Sales, rights and licensing. To purchase WHO publications, see http://apps.who.int/bookorders. To submit requests for commercial use and queries on rights and licensing, see https://www.who.int/copyright.

Third-party materials. If you wish to reuse material from this work that is attributed to a third party, such as tables, figures or images, it is your responsibility to determine whether permission is needed for that reuse and to obtain permission from the copyright holder. The risk of claims resulting from infringement of any third-party-owned component in the work rests solely with the user.

General disclaimers. The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of WHO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted and dashed lines on maps represent approximate border lines for which there may not yet be full agreement.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by WHO in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by WHO to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall WHO be liable for damages arising from its use.

Cover image: Unsplash/Brooke Cagle

Design and layout by 400 Communications.

Contents

Preface	V
Acknowledgements	vi
Abbreviations	vii
Executive summary	viii
Overview	viii
Key findings	viii
Structural components	viii
Skill components	ix
What else is potentially promising?	х
1. Introduction	1
2. Online violence against children	3
2.1 Subcategories, types and dynamics	3
2.1.1 Online child sexual exploitation and abuse	5
2.1.2 Cyber-aggression and cyber-harassment	7
2.2 Three implications for prevention	9
3. Strategies to prevent online violence against children	10
3.1 Prevention education	10
3.2 Legislation	10
3.3 Law enforcement and regulation	11
3.4 Public awareness	11
3.5 Helplines and hotlines	12
3.6 Safer environments, technology-engineered solutions	12
3.7 Other strategies	12
4. A guide to the evidence	14

5. Evidence from effective prevention education programmes	15
5.1 Prevention education for violence against children	15
5.2 Core components of prevention education	18
5.3 Prevention education approaches needing more research	22
6. Evidence for effective online violence against children programmes	23
What currrent prevention education programs are actually saying and doing to address online violence against children	29
8. Effective messaging	36
9. Conclusion	42
10. References	43
Annex 1: Methodology	52

Preface

Violence is a major driver of poor health worldwide – both directly through the physical and psychological injuries it causes, and indirectly through its impact on families, communities, and society. Violence against children is particularly toxic form of violence because of its capacity to disrupt normal development and lead to a lifetime of poor physical and mental health.

Public health resources can be used effectively to prevent violence against children by providing direct assistance in four key areas: support for data collection on violence against children; research into the factors that can increase or decrease violence; the design, implementation and evaluation of interventions; and scaling up successful interventions and proving programme cost-effectiveness.

In recent years, as a result of technological change, violence against children has taken new forms and evolved in ways that need to be closely monitored and rapidly addressed. These forms include new environments for sexual exploitation and vehicles for aggression and interpersonal abuse. WHO is committed to contributing to existing efforts to understand these forms of violence and help guide international response.

One key to an effective international response is drawing lessons from the larger science of prevention. In this document, violence prevention researchers look broadly at the science of prevention and child health to draw implications for best practices for preventing online violence against children. They have identified a great deal of relevant research as well as major gaps in the literature. They have also looked critically at the content of existing prevention programmes targeted directly at online violence. They articulate some strong conclusions about merits of prevention education, but also some important needs for revisions to current practices. They also point the way to prevention strategies that require additional evaluation and support.

This document illustrates well how drawing on evidence from areas of public health can help make in-roads into some of the world's most pressing and challenging public health problems.

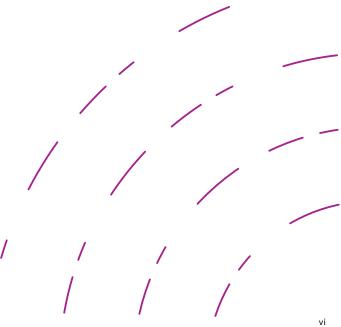
Acknowledgements

This report draws on the expertise of many individuals around the world dedicated to preventing and responding to violence against children. It was researched and written by David Finkelhor, Kerryann Walsh, Lisa Jones, Samantha **Sutton** and **Eugenia Opuda**. The preparation of this report was led by Alexander Butchart, Sabine Rakotomalala and Berit Kieselbach in the WHO Department for the Social Determinants of Health.

We gratefully acknowledge the advice and review of the text by Greta Massetti and Whitney Skowronski from the US Centers for Disease Control and Prevention (CDC), Daniel Kardefelt Winther and Afrooz Kaviani Johnson from UNICEF, Serena Tommasino from the Global Partnership to End Violence Against Children, Richard Wortley from University College London, Katie Edwards from University of Nebraska-Lincoln, Justin Patchin University of Wisconsin-Eau Claire, and Lorraine Radford and Amy Crocker as independent consultants. We would further like to thank the following individuals for inputs provided by email or through interviews: Patrick Burton, Jon Conte, Julia Davidson, Katie Edwards, Donald Findlater, Hannah Gaffney, Susan Kennedy, Daniela Ligiero, Larry Magid, Franceska Meinck, Janice Richardson, Melissa Stroebel, Amanda Third.



This publication has been produced with financial support from Safe Online initiative at End Violence. However, the opinions, findings, conclusions, and recommendations expressed herein are those of the author/organisation and do not necessarily reflect those of Safe Online or End Violence.



Abbreviations

CSAM child sexual abuse materials

OCSEA online child sexual exploitation

and abuse

UNESCO United Nations Educational,

Scientific and Cultural Organization

VAC violence against children

WHO World Health Organization

Executive summary

Overview

This report summarizes the scientific literature on what is currently known about the most effective strategies to prevent online violence against children (online VAC). While there is not yet a consensus on what types of violence and victimization should be included in online VAC, the following types were focused on for this review (in general alignment with the WHO policy brief: violence against children online):

- online child sexual exploitation and abuse (OCSEA), with its subcategories of online grooming, nonconsensual sexting and sexual extortion, child sexual abuse material production and distribution, and livestreaming of child sexual abuse;
- cyber-aggression and cyber-harassment, with the subcategories of cyberbullying and cyberstalking.

To summarize what we currently know, we conducted an evidence review in several areas: a best practice review of youth-focused prevention literature; a rapid review of evaluations of online safety programmes for children and adolescents; a desk review of online VAC programmes for children and adolescents.

Key findings

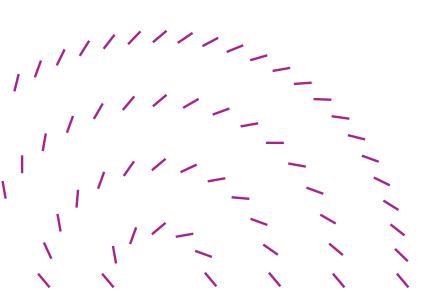
Educational programmes can work. Our review found strong evidence that prevention education for children can work, and that this is a key strategy for addressing online VAC. Educational programmes have been widely shown to increase safety and health in general. They are successful at preventing violence against children overall, and they are effective for preventing one form of online VAC in particular – cyberbullying (both victimization and perpetration).

Cyberbullying prevention works. There is a large body of evidence that educational programmes for children can reduce cyberbullying – one of the most prevalent forms of online VAC. Cyberbullying can be reduced both by traditional bullying prevention programmes and by programmes specifically targeted at cyberbullying.

Certain core components make for more successful educational programmes. Successful programmes have certain structural and skill components that should be generally adopted.

Structural components

- Multiple and varied learning strategies and tools. Reviews find that programmes are more successful when they use multiple and varied modalities for engaging children and promoting learning (1). These include, for example, videos, games, readings, posters and infographics, guided discussions, as well as leader instruction.
- Repeated exposure, greater intensity. Prevention programmes are more successful when they involve more lessons, more message exposures, more reminders, and follow-ups. The literature is less clear on exactly what amount is optimal (2). However, a single exposure like an assembly hall presentation, a film, play or puppet show is unlikely to be effective (3). Typical successful cyberbullying prevention programmes were delivered over an average of 22 weeks (4).



- Peer engagement, role-plays, interaction. The systematic reviews consistently find more success with programmes that actively engage young people with each other (5–8). When children actively engage with each other, it is likely that it increases attention from participants and may also activate and reveal peer norms against bullying and abusive behaviour.
- Whole-school environment involvement. The literature (9, 10) consistently finds that programmes are more successful when they get active engagement from the larger school or community, including support from school leadership (5, 10, 11).
- Parental involvement. The importance of parental involvement has been emphasized in many reviews (5, 6, 11–13). The most common modes of parental involvement are via homework materials and activity suggestions provided to parents. Informational gatherings tend to be sparsely attended and because of this have not been found to be effective (8).

Skill components

- Problem-solving skills. Reviews of successful prevention education programmes identify problem-solving skills as one of the most frequently included elements (14). These components engage children in thinking through situations of uncertainty, conflict, and crisis to choose modes of effective response using stories, role-plays or other methods. Some emphasize taking time to reflect and recognizing body signals and other signs of ambivalence.
- Assertiveness, self-efficacy, resistance to peer
 pressure. This is a very widespread component in
 safety training, used in nearly 80% of evidence-based
 programmes (15). It teaches the skills to resist peer
 pressure and problematic propositions, amplify
 internal hesitations, and to say no or to escape
 from problematic situations. It also teaches assertive
 body language and distinguishes assertive from
 aggressive responses.
- Empathy, perspective-taking, difference appreciation. This widespread (16) component helps children and adolescents to understand and accurately recognize the feelings and needs of other people, especially in situations of conflict (9, 17).
- Self-regulation, emotion management, impulse control. There are a variety of components to prevention programmes that teach self-regulation. These range from calming exercises, relaxation, deep breathing, and meditation, to self-distraction and monitoring emotional arousal (18, 19).
- Conflict resolution, de-escalation.

 These components teach children to identify escalating conflicts or threats and provide them with management tools such as withdrawal, acknowledgement of conflicting needs and the other person's point of view, avoidance of insults, reaching a compromise, and seeking a third-party's assistance (19–21).

- Help-seeking. Help-seeking (22) as a skill needs more than simply urging young people to seek help. It also generally includes training in identifying who their trusted helpers are, overcoming some of the barriers to help-seeking (such as embarrassment), and practicing the identification of problems that warrant help-seeking (22, 23).
- Bystander or defender mobilization.

 This component tries to teach other children who observe inappropriate behaviour or conflict to intervene to support and protect victims and discourage aggressors. It has been implemented in bullying prevention, dating violence, and sexual assault programmes (8, 24, 25).
- Social norm instruction. Social norm instruction is effective, particularly with adolescents (26). Injunctive norm instruction (what people believe others should do) tends to be more effective than descriptive norm instruction (what they actually do).
- Sex education. There is evidence (27, 28) that comprehensive forms of sex education can reduce physical and sexual aggression, in particular homophobic bullying, and dating and partner violence. The effectiveness of sex education has been confirmed in low- and middle-income countries, as well as in high-income countries (29).
- Substance abuse education. Substance abuse is associated with delinquent behaviour, violence perpetration and victimization, as intoxication goes along with reduced inhibitions and expectations of norm violation (19).

Evidence about the success of prevention programmes for online child sexual exploitation and abuse (OCSEA) is not yet available. Nonetheless, this report draws several conclusions on current educational efforts based on a review of the dynamics of online VAC and current online VAC-prevention programmes:

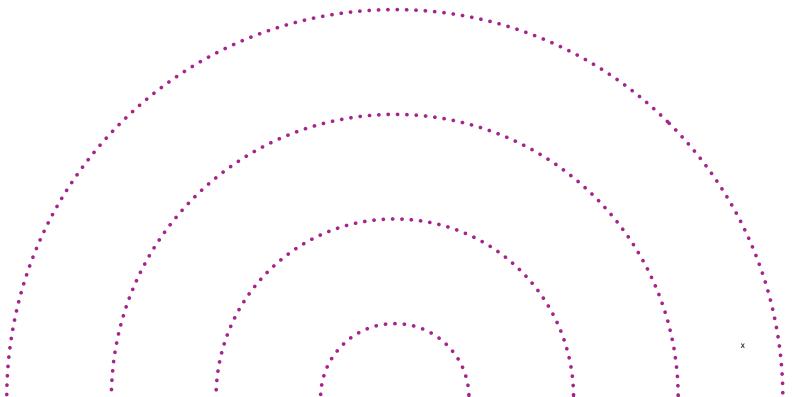
 More coverage is needed about acquaintance and peer perpetration. Acquaintances and peers (including intimate partners) make up a majority of online VAC perpetrators. This is true especially for the dynamics of cyberbullying, cyberstalking, but also many types of OCSEA. However, some online VAC programmes put an almost exclusive emphasis on the danger from strangers, adults, and people met online. Programmes need to provide more orientation to the knowledge and skills needed to prevent and respond to acquaintance and peer perpetration.

- More coverage is needed on healthy relationships.
 Much online VAC (both OCSEA and cyber-harassment) occurs as adolescents try to navigate their developing interests in romantic relationships and sexual intimacy. Online VAC prevention needs greater coverage of such topics as: 1) who is an appropriate romantic partner and why; and 2) reducing risks around sharing personal and intimate information, including images.
- Build online VAC prevention on the foundation of existing prevention programmes. There is an abundance of well-designed, widely disseminated and scientifically tested prevention education programming that addresses topics that are similar to online VAC – programmes about bullying, dating violence, sexual assault, and healthy relationships. Online VAC prevention can greatly benefit from building on the foundations of these programmes and working with their developers to add relevant online VAC knowledge and skills.

What else is potentially promising?

Many other initiatives aimed at preventing online VAC are under development. They include technologies to detect and remove online harmful content and behaviour, new legislation to deter abusers, increased police activity to disrupt criminal conduct, and regulations to force Internet platforms to make their environments less dangerous. However, there is far less scientific evaluation of these kinds of initiatives. Successful examples of similar strategies exist for other crimes, but evidence is sparse and their relevance to online VAC is not yet established. The conclusion is not that these strategies do not work – rather we need to find out if they do.

This report is a snapshot from 2022 in the midst of a rapidly changing digital environment. It provides guidance about some promising and successful strategies in which to invest efforts, though this is an emerging field. It is premature to rule out other especially novel ideas that may be worth developing and testing, and – given the rapid developments – this review will likely need to be updated in a few years.



1. Introduction

The rapid explosion of digital communications technologies and their use by young people has driven a re-orientation in the field of child protection and a fleet of new initiatives. Police, educators, physicians and mental health professionals have all found themselves responding to a variety of threats to children involving technology, some resembling versions of earlier, familiar threats, some with unique new dynamics. Many professionals have drawn on their experiences to design new strategies to protect children in the evolving technology realm. The result has been a wave of new child protection programmes with a digital focus.

Researchers, too, have been mobilized to assist in these efforts. There has been a dramatic growth in the research literature about the digital dangers and their dynamics. Researchers have also teamed with programme designers to scientifically evaluate programme designers' work.

This report is an effort to better integrate these efforts, and to review the research literature and see how it can be used to improve prevention. We focus specifically on the harms to children from digitally mediated, malicious interpersonal relationships – what is termed "violence against children online" or online VAC (see Box 1 for more on terminology). The report does not address some of the other, non-interpersonal harms that may trace to digital environments, such as overuse, social isolation, sleep deprivation, misinformation, or self-image problems.

The report comprises:

- a review of online VAC types and dynamics as research describes them, and what clues this may offer for prevention;
- a summary of insights that can be gleaned from programme evaluation science, both from its extensive history with the prevention of youth problems in general, and also with its new and most relevant applications to online VAC;
- an analysis of the design details and messages of well-developed programmes built to teach children about online VAC (including a sense of the degree to which these programmes are in tune with existing scientific guidance);
- · key messages and a conclusion.

This report adopts a public health approach to the prevention of online VAC, consistent with the public health approach (30) to violence in general, with its emphasis on epidemiology informing primary prevention, refined by scientific evaluation.

What works - A Caution

This review looks at programmes and practices that have support in the research literature. However, the literature has paid much more attention to some practices than others. If programmes or practices do not have support or are not discussed in this review, it does not necessarily mean they are ineffective. In most cases, it means that they have not been well researched and evaluated.

Box 1. Online VAC terminology

Terminology in the field of online VAC is evolving. In addition to the term "online violence against children (online VAC)", which is used in this report, there are a variety of other terms used such as:

- · Internet crimes against children;
- · cybercrime against children;
- technology-facilitated abuse of children;
- technology-facilitated violence against children;
- online abuse of children.

It has been pointed out that "online" or "Internet" may be technically incorrect since much of the referenced violence occurs via texting or outside-the-Internet communications services. "Technology" for its part is an overly broad term because landline telephones and automobiles are also technologies.

The online sexual offence portion of the problem is also referred to with multiple terms such as:

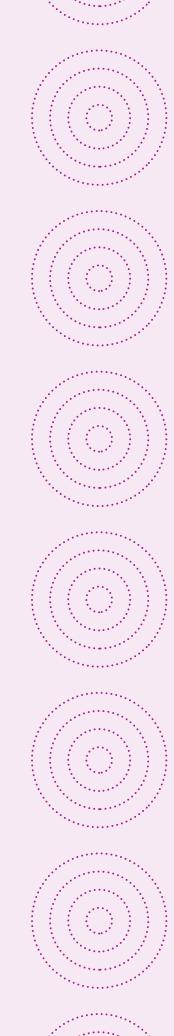
- online child sexual abuse;
- · online child sexual exploitation and abuse;
- image-based sexual abuse.

When it comes to prevention, most programmes that have online VAC prevention goals do not typically refer to themselves as "online violence against children programmes". They use a variety of other terms such as:

- · Internet safety;
- online safety;
- · digital citizenship;
- · cybersecurity;
- · esafety.

Unfortunately, this creates challenges when reviewing online VAC prevention strategies. Terms may confuse stakeholders about where to look or what goals and topics are being addressed by various programmes. In addition, many of the programmes have goals and components that go beyond online VAC concerns and touch upon topics such as how to set up accounts or turn off advertising. Other programmes restrict their coverage to a limited set of online VAC topics, such as cyberbullying. The lack of and clarity and consistency around terminology is likely to persist for a while and is a clear impediment to progress, the accumulation of knowledge, and programme development, adoption, and dissemination.

Note: this report uses the terms "children" or "children, youth, or young people" interchangeably to refer to persons under the age of 18 years.



Online violence against children

This section describes the main types of online VAC, their dynamics and the connections between them. Most of these topics have large literatures that cannot be fully summarized here (31). Instead, this review highlights the diversity of online VAC, and in particular the implications for prevention.

2.1 Subcategories, types and dynamics

Although definitions are sometimes cited, online VAC has primarily been defined in the literature by the list of issues considered to fall within this domain. The list has different versions (32).

A great deal of attention has been paid to online child sexual exploitation and abuse (OCSEA) – particularly in the fields of international law enforcement and advocacy. Comparable attention, particularly in the educational and child development domain, has been paid to cyber-aggression and cyber-harassment. This report covers both these domains and their several somewhat distinct subcategories.

In the OCSEA domain, we include:

Online sexual solicitation and grooming. Using digital devices to solicit children for sexual activity. Grooming is generally limited to adults who use technology to solicit and recruit children for online or offline sexual encounters or to obtain sexual images or videos. Solicitation can include non-adults.

Child sexual abuse materials (CSAM). Production, sharing, accessing or commercial use of sexual images and videos of children.

Live streaming of sexual abuse. Sexual activities that are transmitted ("streamed") live on the Internet for viewing. (Livestreaming could justifiably be incorporated into the CSAM category, as a live version of CSAM.)

Nonconsensual sexting and sexual extortion.

Making or disseminating sexual images without consent. Sexual extortion is using the acquired sexual images to extort money, favours or additional images.

In the cyber-aggression and cyber-harassment domain, we include:

Cyberbullying. The use of threats, hostility, denigration, and other attempts to cause harm in online communications.

Cyberstalking. Persistent unwanted contact via technology that directly or indirectly communicates a threat or creates fear in the victim.

Hacking, identity theft and fraud. Intentionally causing damage to a person's digital equipment, applications, accounts, websites, or other online representations. Intentionally impersonating another person online to cause harm to their interests or reputation. Deceiving a person to maliciously gain money or online assets. See Table 1 for a summary of types of online VAC.

3

Table 1. Online VAC – a summary of different types

Online VAC type and examples	Scope	Co-occurrences
Online child sexual e	exploitation and abuse (OCSEA	.)
 Online solicitation and grooming Unwanted requests for sexual favours or images Requests for sexual conversations Offenders manipulating children into sexual relationships 	According to a meta-analysis of international studies, 11.5% of survey participants had received unwanted online sexual solicitation (33) In a survey from the United States of America (USA), 5% of respondents had experienced online grooming before the age of 18 (34)	Production of sexual images, nonconsensual misuse of sexual images, sexual extortion, livestreaming sexual performances
 Child sexual abuse material (CSAM) The production of sexual images or videos of victims by face-to-face abusers Trading or selling of CSAM Downloading CSAM for sexual gratification 	In 2021, 29 million child sexual exploitation images were identified by electronic service providers (35)	Grooming, self-made sexual material, nonconsensual distribution of sexual material
 Livestreaming of child sexual abuse Using online video applications to view or share live video of children being sexually abused May be facilitated by an offender either remotely or in-person 	Little prevalence information	Grooming, CSAM
 Nonconsensual sexting and sexual extortion Sexual images taken or obtained without consent or under coercion Images consensually obtained, but then shared with others or posted without consent Images consensually obtained and then used to humiliate, denigrate, threaten, or extort money, favours or additional sexual images 	According to a meta-analysis of international studies, 8% of adolescents had a self-made sexual image forwarded without consent (36) In a survey from the USA, 5% of respondents reported that they had been the victim of sexual extortion (37)	Cyberbullying, sexual solicitation, livestreaming, CSAM
Cyber-aggressi	on and Cyber-harassment	
CyberbullyingThreats and hurtful messagesSexual harassmentSpreading rumours or lies	In a meta-analysis of international studies, 15% of children reported cyberbullying victimization (38)	Dating violence, nonconsensual sexting, cyberstalking, hacking online presence
Cyberstalking Frequent unwanted requests for communication or favours Persistent contact with victims through new platforms or identities after being blocked	In a survey from the USA, 24% of females and 19% of males experienced stalking when they were 17 or younger (39)	Cyberbullying, unwanted sexual solicitation, nonconsensual sexting
 Hacking and identity theft Attempts to steal personal or financial information through online means Vandalizing or misusing someone's social media account or website 	In a 19-country European survey, 11% of 9–16-year-olds, including 17% of 16–17-year-olds, had experienced misuse of their personal information or password, or theft of their digital identity (40)	Cyberbullying, production of nonconsensual sexual images, cyberstalking



2.1.1 Online child sexual exploitation and abuse

This domain has several major sub-types with substantial literatures.

Online solicitation and grooming

The key problem generally referenced on this topic is variously called Internet predation, online solicitation, online enticement, or online grooming (41,42). It can be divided into two main components:

- Solicitation for sexual activities: this may come from a wide variety of solicitors, including many peer solicitations that are unwanted, frightening and harassing (43–47).
- Grooming: this is generally limited to adults using technology to solicit and recruit children into online or offline sexual encounters or to obtain sexual images or videos (48). Online grooming offences can be perpetrated by adults encountered online and adults already known to the child from offline venues (49–51). Canadian police statistics find 61% of online grooming offenders are offline acquaintances or friends.

Importantly, studies of online sexual solicitation of youth show dynamics that are often more complex than widely held stereotypes. These crimes are sometimes depicted as involving younger children, deception, abduction and coercive violence at the hands of Internet strangers (48, 52–54). In studies of actual police-reported episodes, most of the victims of online adult sexual grooming were aged 12 years or older (48). Those arrested for online grooming crimes

were also not just online strangers, but acquaintances and friends from face-to-face environments who used technology to build trust and forge relationships that facilitated their crimes (49, 50). Deceptions about identity and sexual motives were sometimes present but were not the dominant offender strategies. Instead, victims were more typically teens drawn into sexual relationships with older partners because of flattery, gifts, attention, and offers of adventure, sexual instruction, or romance (51, 55). A majority had multiple sexual encounters with the offenders.

Scope: Several youth surveys have asked about online sexual solicitation (33, 56). A meta-analysis of nine studies on the prevalence of unwanted online sexual solicitation found a mean prevalence rate of 11.5% (33). One study that limited the count to aggressive or distressing solicitations estimated the past-year rate among a national sample from the USA of 10– to 17– year-olds as 3% for aggressive and 2% for distressing solicitations (57).

Surveys about grooming or online sexual interactions with adults include: from Germany, 22% of adolescents (only 10% of targets perceived the interactions as negative) (58); from Spain, 8% of female and 7% of male adolescents (53); and in the USA, 5% had experienced online grooming from an adult before age 18 (34).

Co-occurrence: Online solicitation and grooming are often the precursors to the production of sexual images, the nonconsensual misuse of sexual images, sexual extortion, the livestreaming of sexual performances, and offline sexual abuse (51, 55, 59).

Child sexual abuse materials (CSAM)

This online VAC category refers to the traffic in illegal images that depict children being sexually abused or displayed in a fashion to elicit sexual arousal and gratification. It includes face-to-face adult sexual abusers who produce the images of their victims for personal or commercial use. It includes online entrepreneurs who trade or earn money from the exchange of these images. It includes the audience of offenders who search for or download these images for sexual gratification or other motives. It increasingly also includes youth who post images of themselves or their acquaintances, which get diverted into this illegal trade. Some youth offenders are involved. Notably, in Canadian police statistics on criminal possession of CSAM, a quarter of the male offenders and three quarters of the female offenders were under the age of 18 years (50).

Scope: As systems to detect and report these sexual images of minors have been put into place, it has become possible to count the quantity of such images being downloaded or exchanged worldwide on some platforms over the course of a year. In 2021 after a decade of growth in detection efforts, the main international aggregating authority – Cybertypline – reported 29 million child sexual exploitation images identified by a subset of electronic service providers (35). It is not known how many distinct different children appear in these illegal images, because many of the reports may be of the same image or the same child. It is also not known how many new victims are added yearly to this available stream. But clearly these images are widespread and readily accessible.

Co-occurrence: For images to be in circulation, they need to be produced during the course of a sexual abuse episode, elicited through grooming, self-made and/or distributed nonconsensually. Thus, these offences overlap considerably with other online VAC types in the sex offence categories.

Livestreaming of child sexual abuse

Livestreaming is a form of online child sexual abuse in which sexual activities are transmitted ("streamed") live on the Internet for viewing remotely by potentially many people (41, 60, 61). Usually, viewers of live streaming pay facilitators or the children themselves. Viewers can request certain sexual acts in advance of the streaming or while it is underway. Live-stream performances have been subdivided in "voluntary self-produced," "induced self-produced," where grooming or coercion is applied, and "facilitated" performances (62) which an adult orchestrates. Livestreaming can pose law enforcement challenges when little or no trace of the performance remains, and offenders can avoid detection.

Scope: Population studies on livestreaming are sparse (31). A survey of international law enforcement found more evidence of the problem in the USA, Europe and the Philippines (63) than in other parts of the world.

Co-occurrence: Livestreaming may be best seen as a variation of other forms of child sexual exploitation and abuse described in this section. Much of it is an extension of grooming by adults, who as facilitators or audience induce juveniles to engage in sexual performances. It also clearly qualifies as the production of child sexual abuse materials, even if the images are ephemeral.

Nonconsensual sexting and sexual extortion

There is a large and growing literature on youth sexting (64) – defined as the creation, transmission or exchange of youth-produced sexual images via the Internet and mobile phones (36) - which is sometimes called "self-generated content" and "youth produced images". The growing literature shows sexting to be complicated, and not necessarily always victimizing (65). The nonconsensual forms of sexting that would be online VAC occur in several contexts. First are sexual images taken or obtained by other youth without consent or through coercion, pressure, deception or stealth. A second involves images consensually obtained, but then shared with others or posted without consent. A third context is when sexual images are consensually obtained and then used to humiliate, denigrate, threaten or extort money, favours or additional sexual images, what is termed sextortion or sexual extortion (41). Romantic relationships that end acrimoniously are often a context for these nonconsensual sexting and sextortion episodes (31, 66, 67). In police data about youth victims, 90–100% of the nonconsensual-distribution offenders were other youth (50). Similarly, in youth surveys (43-47), unwanted requests for and misuse of sexual pictures primarily come from youth acquaintances.

Scope: A meta-analysis of 39 studies found 8% of youth had a self-produced sexual image forwarded without consent (36). Another meta-analysis in Portugal (68) found the prevalence of abusive sexting was 4.3% (69). Among a nationally representative sample from the USA of 5568 middle and high school students, 5% reported that they had been the victim of sextortion (someone using their sexual image to try to obtain something) while 3% admitted to threatening others who had shared an image with them in confidence (70). In another national study from the USA that specifically looked at instances of threats of image misuse, 8% of respondents reported experiencing sextortion (34).

Co-occurrence: Nonconsensual sexting and sextortion overlap with cyberbullying (71) when friends, acquaintances and romantic partners use the images to humiliate and extort. They overlap with sexual solicitation and livestreaming, in which the young person produces images on request. These forms of online VAC also overlap with intimate partner abuse, where current or former romantic partners misuse the images (72). The images can migrate into the domain of online traded illegal images, and so it can overlap with CSAM as well (66).

2.1.2 Cyber-aggression and cyber-harassment

Cyberbullying

The term cyberbullying references verbal aggression. threats, hostility, and other attempts to cause harm in online communications (73). It encompasses terms such as flaming, outing, hate speech, online drama, and online harassment (74, 75). It can include the posting of false profiles, distributing defamatory information, and sometimes includes cyberstalking (76). Apart from physical threats and threats to home, family, and friendships, cyberbullying (like face-toface bullying) often includes sexual content, such as sexual harassment, sexual shaming, and homophobic and sexist insults (77). Hate communication, racial, ethnic and gender attacks are also common (78-80). Online bullying, harassment and aggression also often occur in the context of adolescent dating relationships, among school peers, as well as in relationships started online and through dating apps (76, 81). These topics are sometimes referred to separately as online dating or relationship abuse, but they fit within the definition of cyberbullying.

Scope: Rates of cyberbullying vary widely. A metaanalysis of 72 international studies found 15% of youth reported cyberbullying victimization compared to 36% reporting face-to-face bullying victimization (38). Cyberbullying occurred equally among both boys and girls, but there were differences by gender with respect to specific cyberbullying behaviours (82). Cyberbullying peaks between the ages of 13–15 years – somewhat older than conventional bullying (82–84) – an important consideration for prevention design.

Co-occurrence: A well-substantiated finding is that much cyberbullying occurs in conjunction with offline bullying and harassment (85–87). One study found that two-thirds of online harassment episodes were connected to offline episodes (88). Victims and perpetrators of bullying are also at higher risk of being victims and perpetrators of other forms of violence exposure (89, 90) including dating violence, nonconsensual sexting, cyberstalking, hacking and various other delinquent and anti-social behaviours. This suggests bullying as a core element to online VAC. This is especially true because bullying in elementary and middle school appears to be a precursor to other forms of abusive behaviour online and offline in teenage and early adult years (91, 92).

Cyberstalking

Cyberstalking refers to persistent unwanted contact via technology that directly or indirectly communicates a threat or creates fear in the victim (93), and it can involve frequent unwanted requests for communication or favours. Even when they have been blocked, cyberstalkers, continue to contact victims through other platforms or under changed identities. Sometimes cyberstalkers threaten to appear in person or retaliate in social networks. Cyberstalking can be a mix of online and offline harassment and can have a sexual component in the form of persistent requests for sexual images or face-to-face sexual activities. The most common perpetrators of cyberstalking against both males and females are acquaintances or current and former intimate partners (39, 94), as well as internet contacts who want to establish or continue a relationship that is no longer wanted.

Scope: Cyberstalking is particularly common among young people of dating age, with girls victimized somewhat more than boys. One in four (24%) females and one in five (19%) males first experienced stalking when they were 17 or younger, according to one of the most comprehensive surveys of stalking conducted by the US Centers for Disease Control. Of these victims of stalking, 56% of females and 61% of males experienced their stalking via social media, such as unwanted texts and photos (39). In another national survey from the USA, victims said 61% of their cyber stalkers were intimate partners, friends or acquaintances, 28% were of unknown identity, and 10% were persons met online (95).

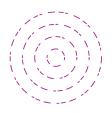
Co-occurrence: Cyberstalking overlaps considerably with cyberbullying or cyber-harassment, unwanted sexual solicitation, and nonconsensual sexting (93).

Hacking and identity theft

Programmes about online dangers frequently warn of identity theft, hacking, and malicious attacks on young people's computers, computer software, and smartphone applications. The attacks can be individually targeted or part of attacks on schools, or the databases of social media platforms (96, 97). Attacks against youth often originate from other youth. There is a considerable evaluation literature (98, 99) on prevention programmes in this domain, which is a sign of its extensive scope. While these topics dominate discussions of Internet dangers in general, they are less frequently included in online VAC discussions. That is unfortunate. Hacking, fraud, and identity theft are gross violations of children's rights and can cause considerable psychological as well as financial damage. Children may be particularly vulnerable because of inexperience and lack of security resources.

Scope: Some survey evidence about hacking and identity theft is available. In a 19-country European survey (40), 11% of 9–16-year-olds, including 17% of 16-17-year-olds, had someone misuse their personal information or password, take on their digital identity or create a hostile webpage. In one survey in the USA, 12% of 15–17-year-olds reported someone hacking into their accounts and stealing information, and 6% reported someone stealing or coercively obtaining their password (100). A survey of households in the USA by a private security firm claimed over 1 million children were affected by identity fraud resulting in losses totaling US\$ 2.6 billion and families paying over US\$ 540 million (101).

Co-occurrence: Much online hacking and identity theft can be conceptualized as a form of cyberbullying, where more powerful or technology-adept individuals, known and unknown, take advantage of children's vulnerability. Hacking and identity theft are also often part of the process of obtaining nonconsensual sexual images. They can also be part of harassment inflicted by cyberstalkers. Its frequent occurrence and connection with other online VAC domains, plus its routine coverage in Internet safety programmes, all warrant the inclusion of online fraud, hacking and identity theft as a type of online VAC.





2.2 Three implications for prevention

Literature on the dynamics of these various types of online VAC leads to conclusions that have important implications for the design of successful prevention strategies.

Acquaintances and peers are common perpetrators

Unknown adult perpetrators often predominate in descriptions of online VAC dynamics. However, as cited above, multiple studies from surveys and police records show that acquaintances outnumber strangers as perpetrators for most forms of online VAC. For example, among a nationally representative sample of grooming cases known to the police in the USA, a majority of offenders were offline acquaintances that their victims knew from their social networks (51, 55). In a national census of grooming cases gathered by Canadian police, 61% of perpetrators were acquaintances, friends, family or intimate partners (50). Surveys of youth from various countries, part of the Disrupting Harm in Online Exploitation initiative (43-47), confirm the primacy of acquaintance perpetrators even in sexual abuse offences, including unwanted solicitation, image requests, commercial sex offers and sextortion.

Peer perpetrators are also very numerous in online VAC offences. In the Canadian data about police-reported sexual image distribution crimes, 89% of the male offenders were under the age of 18 years. In solicitation cases, 21% of the mostly male perpetrators were also under the age of 18 years (50). Cyberbullying is also largely peer-perpetrated, although this is more widely recognized.

These insights about offenders are consistent with the history of awareness about violence and crime against children in general. Initial prevention efforts have often emphasized stranger dangers (for example, kidnapping or child molestation), even though acquaintances and intimates were found to be more numerous.

Prevention strategies that emphasize avoiding contact with strangers or unknown adults will have limited effect and perhaps give misleading guidance. Prevention strategies would do better to focus more broadly on inappropriate behaviours by both acquaintances and strangers, and both adults and youth. Programme developers should also keep in mind that prevention education targeted at youth, especially in schools, will potentially be reaching youth perpetrators in the audience as well as potential victims. Prevention education and messages directed at children may have positive outcomes through both deterring potential offenders as well as empowering potential victims.

There is significant overlap among types of online VAC

Different online VAC types overlap considerably one with another. For example, livestreaming is also a form of production and sharing of child sexual abuse material. Producing child sexual abuse material takes place through online grooming. Grooming can lead to sextortion. The overlap even involves sexual and non-sexual forms of online VAC. Cyberbullying takes sexual forms when bullies engage in nonconsensual sexting. Cyberstalking takes the form of unwanted sexual solicitations.

The literature is also clear that there is considerable overlap (87) between online and offline forms of violence against children (102). Studies find that two-thirds to three-quarters of cyberbullying episodes are connected with face-to-face bullying by the same harassers. Grooming victims often go to meet their groomers offline for sexual activities (88). Nonconsensual sexting is frequently connected to abusive face-to-face dating relationships. Cyberstalkers stalk victims in offline as well as online venues.

The relevance of this overlap is reinforced by a lengthy literature on youth problem interconnections. This literature confirms that multiple forms of risk-taking, aggression and delinquency cluster among some youth (103, 104) and also that multiple forms of victimization cluster in the lives of youth as well (105).

Prevention programmes should address the online VAC forms in an integrated way, both across online VAC types and along with offline forms of violence, as well. The extent of the overlap argues against a siloed approach to prevention (treating sexting, grooming, cyberbullying separately) in favour of a more holistic approach.

Bullying is a developmental precursor to online VAC

The literature shows that many forms of online VAC peak during adolescence. Victim vulnerability increases around puberty with the onset of interest in romance, dating, and sexual attraction. Groomers take advantage of adolescent interest in sex and relationships to engage victims. Cyberstalking, sextortion, and nonconsensual sexting all occur in contexts of troubled romantic relationships. By contrast, bullying perpetration and victimization, especially in the face-to-face environment, both have earlier onsets in elementary school (106). Studies have shown the connection between earlier, pre-adolescent bullying perpetration and victimization with later dating abuse and sexual abuse in adolescence and even adulthood (91, 92).

Summary

To address online VAC successfully, bullying prevention and its related respect-building skills should be a developmental cornerstone for the prevention of the later forms of offline and online violence. This approach (91, 107, 108) suggests an integrated prevention strategy that starts in pre-adolescence with offline respectful relationships and builds progressively into online VAC prevention in anticipation of adolescence.



3. Strategies to prevent online violence against children

Various prevention strategies have been proposed and deployed to address the domains of online VAC. Many are similar to strategies discussed in the INSPIRE framework (109), which addresses the broader problem of violence against children, and in the WeProtect Global Strategic Response Themes to eliminate child sexual exploitation and abuse online (110). Unfortunately, there is little evaluation on the impact of many of these strategies.

When a strategy for a particular prevention goal lacks evidence, the next best test is to see if there is evidence for that strategy's success with related problems. For example, it is not known if increased surveillance has deterred online sexual solicitation and grooming, or CSAM distribution, but have similar strategies been capable of reducing drug trafficking or property crime? It is also not known if prevention education has reduced OCSEA, but have similar prevention education efforts reduced sexual risk taking or HIV/AIDS transmission? Often these related problems share dynamics with online VAC. This approach is called testing the logic model of a strategy. In the absence of more direct evidence, it is the approach we draw on in the next two sections.

3.1 Prevention education

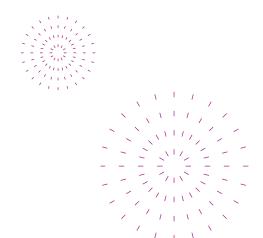
Most online VAC prevention efforts have focuses on providing education and information aimed at children and their parents. Internet safety programmes for these audiences have been developed all over the world, for online access, for home instruction and for use by schools. This strategy stands on the shoulders of other educational programmes with demonstrated success in a wide variety of prevention challenges related to youth, such as substance abuse and delinquency. This report focuses on this strategy the most, as it has a relatively large existing literature, and it has generated substantial insight about effective components and messages (this literature is reviewed in Section 4). Several other strategies that complement youth and family safety education are also summarized here and merit further study, though they have less of an evaluation record.

3.2 Legislation

New laws have been put in place that seek to prevent and reduce online VAC by criminalizing grooming behaviours, extending crimes to the online domain, or requiring technology companies to report online offences and take down illegal content (111). The INSPIRE package cites other examples of successful violence against children legislation, such as banning corporal punishment, restricting alcohol sales, and holding gun owners responsible for child access to weapons (109). However, we could find no evaluations of the impact of legislation on online VAC.

In general, it is hard to empirically assess the effects of legislation, but evidence suggests that enforcement and regulatory actions are more influential than legislation itself, and that new legislation is ineffective without serious enforcement.

In addition, legislation in this domain has sometimes provoked controversy and criticism for its potentially negative side effects. Examples include laws requiring juveniles to register as sex offenders (112, 113) and laws that criminalize sexting among youth. There are concerns that such laws can discourage victims from disclosing victimization because they are afraid that they or their friends could be prosecuted (114, 115) or placed on registries. Legislation is often a popular response, but it needs effective implementation and critical assessment.





3.3 Law enforcement and regulation

In response to online VAC there has also been a considerable mobilization of law enforcement and regulation, particular in the category of online sex crimes (116). Many countries have trained police on how to better detect and investigate online crimes against children. Special reporting centers and investigatory bodies have been created, and arrests and prosecutions have increased (50).

The prevention logic of these strategies is that the visibility of police activity deters offenders, who increasingly will recognize the potential for getting caught. Enforcement also reinforces norms and reminds the public of what is illegal, for example the downloading of child sexual images, when their criminality may have been unclear to some audiences.

Two elements of these law enforcement strategies are enhanced enforcement and surveillance. There is evidence in general for an enforcement strategy called "focused deterrence," which has been successful, for example, in reducing offending in a number of areas such as drug markets and gang activities (117, 118). Enforcement has also been successful at reducing corporate Internet security violations (119). Increased and targeted police activity has been statistically associated with overall reductions (120) in crime rates in the USA.

Surveillance in the online VAC arena has included greater efforts to monitor social media, Internet traffic, and websites for the presence of criminal activities against children. This has taken the form of content moderation and the use of artificial intelligence to flag suspicious communications that need more scrutiny.

There is research on surveillance, particularly the use of closed-circuit TV (CCTV) cameras in public places, and it has shown success in reducing crime in the areas targeted (121). Such situational crime prevention strategies do not simply displace crime to other areas (122) as some have argued. However, it is not clear to what extent surveillance works as well online where displacement is possibly easier.

Unfortunately, there are also examples where intensified police enforcement has had negative effects, such as increasing harm to domestic violence victims (123) as a result of regularly arresting offenders with whom they live. Increased police activity in schools (124) has also been found to drive up youth exclusion and disciplinary action without overall improvement in school safety. Increased Internet surveillance for criminal activity, as in terrorist monitoring, has been criticized for its potential intrusion on privacy of ordinary citizens (125). Questions have been raised about whether such intensification strategies work in low- and middle-income countries where policing can be particularly indiscriminate and brutal (126). There is an evident challenge in calibrating enforcement and surveillance to the right level so that deterrence is achieved without negative side effects. Police activity can be a deterrent to crime, but the possibility of negative side effects is real and needs to be monitored.

3.4 Public awareness

Some efforts have been made to prevent online VAC through direct communication with the community at large. These have included public awareness campaigns about children's online safety and targeted at potential offenders in various media environments. Other social marketing campaigns are designed as appeals to parents and users signing up for various technology privileges and applications to educate them about online dangers.

One example of a successful public awareness campaign is that of neighbourhood watch programmes (127). These can potentially deter offenders and mobilize neighbours or bystanders to take protective action, which mirror the goals for online VAC awareness. Media campaigns to prevent substance use, on the other hand, have had very mixed results, including some showing increases in substance usage (128).

Broadly targeted public awareness programmes are hard to evaluate. They also typically do not have the intensity and multi-modal features associated with successful prevention education. Their usefulness in the online VAC domain is being explored.

3.5 Helplines and hotlines

Considerable efforts have been put into developing helplines to address cybersafety and online VAC. These helplines, accessed by phone or online, provide help to child victims, concerned family members and friends, as well as to potential and actual offenders. Childhelpline International (129) is an international network of such hotlines. The INHOPE (130) network has also made an active effort to establish hotlines in European countries and around the world, specifically in regard to child sexual abuse material.

Helplines are widely revered by advocates and touted as successful by managers for the large number of people who get assistance and appear to be satisfied with it. Evaluations typically show reduced distress among, and positive reactions from, users. Helplines drive some offenders into counselling, but unfortunately, there is little research demonstrating that helplines prevent or reduce the types of ultimate outcomes of concern, such as suicide or sexual victimization (131-133). However, this should not be seen to judge helplines as unsuccessful, but rather to demonstrate the difficulty of evaluating programmes for which anonymity of the help-seeker is central. It is also important to note that helplines are not designed as a primary prevention strategy but are better viewed as a form of intervention or harm reduction.

3.6 Safer environments, technologyengineered solutions

A growing concept in online VAC prevention is "safety by design." This term refers to efforts to construct user platforms and technology environments that are inherently safer for children, cordoning off the dangers. The concept is still in development but draws inspiration from other engineered environments like automobiles or workplaces and their safety elements. Possible online VAC safety elements are efforts to automatically exclude certain kinds of content, certain categories of users (adults, strangers), or certain behaviour from youth-serving environments.

There are examples of multi-faceted efforts by technology companies to create safer platforms (134): these include limiting users' ability to search for child sexual abuse materials; posting warnings to searchers about illegal content and efforts to access it; facilitating and informing users about how to make reports; proactive artificial intelligence systems that try to disrupt grooming (135) and dissemination of dangerous new content; and flagging, reporting and removing known illegal images. Other examples include attempts by law enforcement to disrupt payment systems that enable the purchase and sale of child sexual abuse images and services (136). There have been signs of success but the field is waiting for evaluation of these environmental preventions.



The design strategy with the best supporting evidence is the use of warning messages. Experiments have shown that programme warnings surrounding searches for CSAM-type material can deter potential offenders from pursuing access to the images (137–139). There are also encouraging experiments showing the effects of warnings that deter perpetrators from hacking into the systems of potential victims (140–142).

But key challenges remain. For example, users can get used to and then ignore routine warning messages. Users can also become frustrated with barriers and interruptions to easy access, prompting many to turn off or opt out of control options. The goal is to identify problem situations and interpose accurately targeted deterrents and blocks. At the moment, the evidence (143) for these strategies is still developing.

3.7 Other strategies

A variety of other strategies are being developed that are not forms of wide-scope primary prevention as such, but nonetheless may have some prevention effects. These include therapeutic support programmes for undetected or potential offenders (144) and interventions for children who display sexually problematic behaviour (145). Both of these have demonstrated reductions in offending behaviour.

Table 2 summarizes the prevention approaches of these different strategies and available evidence, mapped against the widely used INSPIRE: seven strategies for ending violence against children (109). It is important to note that research explicitly into what works to prevent online VAC is in its infancy. We currently know very little by way of findings from scientifically evaluated prevention programmes. This does not mean that these interventions do not work, only that our knowledge about what types of initiatives work for what problems is currently very limited.

Table 2. INSPIRE strategies

INSPIRE strategies	Intervention	Intended outcome(s)	Level of evidence
Implementation and enforcement of laws	Legislation	Prevent and reduce online VAC by criminalizing grooming behaviours, extending crimes to the online domain, or requiring technology companies to report online offences and take down illegal content	No evidence of effectiveness yet for online VAC prevention Related research suggests enforcement is key
	Law enforcement mobilization	Visibility of police activity will deter offenders and reinforce norms by reminding the public of what is illegal	No evidence of effectiveness for online VAC prevention, but "focused deterrence" has been found to work for other crimes
Norms and values	Public awareness	Prevent online VAC through direct communication messaging for parents, youth, potential offenders, and the community at large	No evidence of effectiveness yet for online VAC prevention
Safe environments	Technology engineered solutions	Prevent online VAC by excluding certain kinds of content, certain categories of users (adults, strangers), or certain behaviour from youth-serving environments	Emerging evidence that warnings about searches for CSAM may work. No evidence yet for online VAC prevention for other strategies
Response and support services	Helplines	Provide help to child victims, concerned family members and friends, as well as to potential and actual offenders	No evidence of effectiveness yet for online VAC prevention
Education and life skills	Prevention education programmes	Prevent online VAC via educational programmes about risks, and protection skills and strategies	Positive evidence for reducing cyberaggression but not yet for OCSEA; strong evidence for reducing related violence and risks
Parent and caregiver support			In actual practice, most child-focused prevention programmes have integrated parent components, and many parent education programmes engage children as well. These cross-over components are associated with better outcomes in both literatures

Summary

This section reviewed a variety of strategies for preventing online VAC. The only online VAC strategy that currently has a literature showing possible benefits in experimental designs was for warning messages aimed at those searching for CSAM. There was also indirect empirical support from other crime-reduction efforts behind the concepts

of "focused deterrence" through police mobilization and increased surveillance. Unfortunately, little generalizable research exists on crime-reduction strategies of the sort under consideration for online VAC. This does not mean that these initiatives should be abandoned, but that they need additional study before being universally promoted.

4. A guide to the evidence

In Chapters 4-7, we discuss "what works" in the way of programme types and programme components. In this report, something that "works", "is successful", or "is effective", means that:

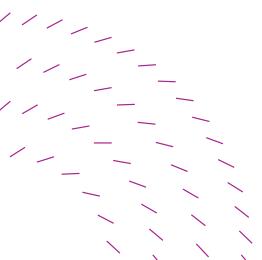
- the programme or programme component has been experimentally tested and the results compared between a group of children who received it and a similar group who did not;
- multiple evaluation studies have been aggregated together for this programme or programme component;
- the conclusion of positive effect is the result of a formal synthesis of all these studies, usually in a meta-analysis;
- the outcome being measured was a change in behaviour such as a reduction in victimization or perpetration, or an increase in bystander interventions;
- the change being measured was not limited to a change in knowledge, skills, attitudes, or selfefficacy (even though these can also be important).

However, there are serious limitations to almost all conclusions drawn from this evidence that must be kept in mind.

 Most of the studies have been conducted on populations in high-income countries, in regions such as north America and western Europe, so the conclusions may not apply to other country types or regions.

- Even when studies find positive effects, those effects may not necessarily apply to all subgroups of children in the studies. For example, the effects may not apply to children from groups unrepresented in the studies.
- The review summarizes findings published over a fairly long period – in some cases 20 or 30 years.
 Societal changes may render some of these conclusions obsolete.
- In most reviews with positive evidence of effects, there are some studies that do not show positive results. This means that some programmes or some programme components of this type do not always work or may work only in some designs or under particular conditions.
- There is a well-understood bias for publishing studies that show positive results, which reduces the ability to accurately summarize programme effects.

As a result, the conclusion that a programme or approach works must be regarded as conditional, contextual, and tentative. Nonetheless, given the infancy of online VAC programme evaluation, an approach that has been shown to work under some conditions has reasonable claims over programmes that have not yet been tested or shown positive outcomes at all.



Evidence from effective prevention education programmes

This section looks specifically at prevention strategies that aim to provide education and training for youth and their families. The large and detailed research literature on this topic merits such separate, intensive attention. The first section describes the strong endorsement given by the research to youth education programmes as a generically successful prevention, safety and behaviour-change strategy. The subsequent sections mine the literature for insights about what are the effective components of these successful educational programmes that should also apply to online VAC prevention.

5.1 Prevention education for violence against children

There is an enormous scientific literature behind prevention education for youth and families. This literature encompasses topics related to youth safety, physical health, mental health, and school performance. Particularly prominent topics are mental health promotion, substance abuse, and sexual risk behaviour. The scientific assessment of this field is rich in details and very optimistic in its conclusions. Large numbers of meta-analyses show consistently positive (even if modest) improvements and few negative effects across a wide range of problems.

A recent review of youth prevention education programmes summarized findings from over 1100 controlled empirical trials catalogued in 74 meta-analyses involving nearly half a million participants (146, 147). The most widely evaluated prevention education programmes were about substance abuse, externalizing problems (delinquency, bullying), and sexual behaviour, but many were multi-problem programmes. Virtually all the domains showed positive outcomes with practically no negative outcomes, although some impacts were small and varied by type of programme. This is an impressively consistent record of success.

This large prevention education literature is rich in positive findings about youth problems that bear similarities to online VAC – problems that require self-restraint in sexual contexts, refusal skills, peer-pressure resistance, and help-seeking. For example, there are positive outcomes for education to prevent risky sexual behaviour (148) (53 studies) and that conclusion has been substantiated in low- and middle-income countries (29) (33 studies). Youth education has yielded positive results for HIV-prevention outcomes (149) (67 studies) and it was the most consistently successful HIV-prevention strategy for youth (150). There were substantial positive outcomes for substance prevention education (151) (207 studies).

The supportive evidence for online VAC prevention from this broad literature can be broken down conceptually into three concentric circles (see Figure 1).

- The broadest universe is educational prevention for youth problems in general. The evidence cited above falls into that circle. It establishes that providing information and skills really does change behaviour and health outcomes across many serious problems – not always in every programme, but consistently.
- The middle circle designates the subset of programmes that address violence against children, though not necessarily online. Here there are meta-analyses that confirm success for educational problems that reduce bullying (9, 152), delinquency (146), dating violence (153), and sexual assault (154). For example, there are very consistent positive outcomes for bullying prevention in two large metaanalyses one of 77 studies and one of 100 studies (9, 152, 155). Since many of the drivers of online VAC are similar to the drivers of violence against youth in general and these drivers can be changed by violence-prevention programmes this appears very encouraging for similar successes with online VAC.
- Finally, there is a subset of educational programmes that addresses specific online
 VAC outcomes. These analyses are summarized in section 5. They are primarily confined to showing that educational programmes are effective to prevent cyberbullying, but they also confirm that borrowing approaches drawn from the practices in circles one and two have the potential to prevent offences in circle three, violence specifically online.

Figure 1. Layers of evidence for online VAC prevention education



There is a considerable body of direct and inferential evidence for the likely success of youth educational programmes to prevent online VAC. It strongly supports two of WeProtect's Global Strategic Response Themes to eliminate child sexual exploitation and abuse online: Capability 20 "Education and outreach" and Capability 23 "Research to understand children's online vulnerabilities and effective safety systems" (110).

Prevention programmes targeted at parents also have an encouraging literature (156–159) but considerably less than that relating to youth-focused programmes (160). Many of the parent education and training studies have been with parents of preschool children, however, which makes them less relevant to online VAC prevention (which has a later onset). However, review studies with parents of older children also show the

positive effects of parent education on problems like substance abuse, delinquency, bullying and sexual risk-taking.

In actual practice, many youth prevention programmes have integrated parent components, and many parent education programmes engage youth as well. These cross-over components are associated better outcomes in both literatures (8, 158). This report will refer to these as educational programmes for children and youth, since this is the predominant format.

The scientific literature on prevention yields a very strong conclusion. To improve outcomes for youth, education for children and youth has the most extensive and consistent record of success. The evidence spans multiple child and youth problems, and includes problems quite closely connected to online VAC. There is no other modality of prevention

that has a research evidence base of anywhere near comparable size and consistent results. Moreover, the literature on prevention education for youth is large enough and varied enough to yield important implications for which particular programme components create the most consistent positive outcomes. This evidence is exactly the kind of advice that programme developers seek (and is covered in subsequent chapters in this report).

For the purposes of preventing online VAC there are a number of other strong reasons, besides the sizeable evidence base, for making child and youth education a central component.

- These programmes are designed to be universally accessible to all children. This means that even small effect sizes can have large population-level effects because so much of the relevant population can be accessed.
- The cost is relatively modest for example, a schoolbased educational programme in the USA to combat child sexual abuse was assessed at US\$ 43 per student (161).
- These programmes address both potential victims and offenders, meaning that they have multiple avenues of influence. Reaching potential offenders early has generally been seen as a more effective strategy than waiting until they are on the brink of offending.

- These programmes are widely adapted to and disseminated in school environments, which has its own benefits. School environments are immersive and reach children and youth who might be out of reach to other modalities.
- Educational programmes are modalities that are familiar to children and build on conventional educational routines and practices that reflect enormous histories of use and refinement.
- In school environments, the programmes are often linked with professional, pedagogically trained staff, who are capable of providing assistance and referral should the programmes reveal victims or offenders who need more tailored attention.

Taken together, the evidentiary and practical arguments for child and youth education are very persuasive.

On the other hand, one frequent objection to child and youth-based education as a primary vehicle for online VAC prevention is the argument that this modality places too much of the safety burden on children and youth, and thus is morally deficient (161, 162). In this view, the priority should be on prevention strategies that put the safety burden on parents, technology companies, regulatory agencies, and societies – not children. But this argument is overly simplistic and does not in our view withstand other moral considerations.



- Why should online VAC prevention have a different moral standard than many other risks (for example, automobile safety, bicycle safety, physical and nutritional health, substance-use prevention, crime prevention and injury prevention) that are dealt with through youth education? All these risks have larger societal causes, such as badly designed roads, junk food marketing, criminal cartels, weak regulations and lax gun laws, which need to be addressed by adults. But youth education is still a very large and welcome component of a comprehensive and multisectoral strategy to prevent VAC (109, 110).
- When there are interventions that are known to work, it may be morally suspect and a violation of children's rights not to deploy them, even if they create unfair burdens. Would children, informed that education might protect them, still want adults to deprive them of that opportunity to shield them from burden? Many might contend that children have a right to such education.
- Moreover, it is mistaken to think that prevention education addresses young people only as potential victims, putting the burden on them to avoid their own victimization. Successful cyberbullying-prevention programmes, for example, address both victimization and perpetration by young people. Substantial quantities of cyberbullying, cyberstalking, hacking, sexual offending, and image abuse happen at the hands of other youth. Reductions of these behaviours require some burden of change and awareness from potential youth offenders. Education is a direct influence on them and is known to be effective (163).

Clearly, it would be morally infirm to present education of youth as the only prevention strategy when multiple other factors play important roles in the creation of risk. But given the abundance of evidence for the benefits of youth education, granting it a prominent role in prevention remains relevant.



5.2 Core components of prevention education

This section highlights components typically found (according to research) in more effective prevention education programmes.

One benefit of the large body of research on prevention education is that effective programmes can be compared with ineffective or less-effective programmes to identify the components that seem to be most helpful. This section highlights those components. Many of the conclusions that follow are based on meta-analyses of prevention education broadly, but they do include research on violence, bullying and online violence prevention.

Below we describe programme components in three groups. Structural components refer to how programmes are organized, their targets and their designs. Skill components refer to capabilities and behaviours that the programmes strive to develop. Knowledge components refer to particular information and messages that programmes strive to impart.

Structural components

Multiple and varied learning strategies and tools.

Reviews find that programmes are more successful when they use multiple and varied modalities for engaging youth and promoting learning (1). These may include, for example, videos, games, readings, posters and infographics, guided discussions, as well as leader instruction. Games have been shown in some specific reviews to augment effectiveness (1, 13, 164) but using games in the absence of other strategies may be less effective (165, 166).

Repeated exposure, greater intensity.

A widespread finding (6) from the reviews is that prevention programmes are more successful when they involve more lessons, more message exposures, more reminders, and follow-ups. This is a basic finding in educational research that sustained learning requires repetition. The literature is less clear on exactly what amount of exposure is optimal (2). However, a single exposure – such as an assembly hall presentation, a film, play or puppet show – is generally seen as ineffective (3). Typical successful cyberbullying programmes were delivered over an average of 22 weeks (4).

18 \

Peer engagement, role-plays, interaction.

The systematic reviews consistently find more success with programmes that actively engage young people with each other (9). This has been shown specifically in bullying and cyberbullying prevention research (5–8). When youth actively engage with each other, it is likely that it increases attention from participants and may also activate and reveal peer norms against bullying and abusive behaviour.

Whole-school environment involvement. The literature (9, 10) consistently finds that programmes are more successful when they get active engagement from the larger school or community, including support from school leadership, school-wide policies, and full staff training (5, 10, 11). This has been found in particular with anti-bullying and anti-violence programmes. The research finds less success when prevention efforts are limited to a single educator or classroom acting on their own. Priority should be placed on getting schools and school systems as a whole to adopt prevention programmes.

Parent/caretaker involvement. The importance of parental involvement has been emphasized in many reviews specific to violence, bullying and cyberbullying prevention (5, 6, 11–13). Presumably parent involvement generates additional reinforcement of messages and skills. It may help to affirm and disseminate antiviolence norms and increase supervision. The most common modes of parental involvement are homework materials and activity suggestions provided to parents. Informational gatherings for parents are sometimes included, but gatherings tend to be sparsely attended and have not been found to be effective (8).

Well-trained facilitators. A common sense finding in the literature is that trained facilitators, either specialists or teachers who have had more preparation, tend to do a better job (9, 167). One review found it particularly important in cyberbullying programmes that facilitators be competent and familiar with technology and the digital environment (168).

Quality-control mechanisms. All behaviour-change programmes suffer when adopters modify or adapt the content in ways that can impair successful components. Programmes that have detailed manuals outlining the curriculum, and mechanisms for ongoing supervision, reminders, facilitator booster trainings and evaluations tend to have more success (4, 169).

Attention to special and high-risk populations.

Some universal programmes also have components that address specific subpopulations – such as youth with disabilities, sexual minority youth, refugees and homeless youth. An analysis of 70 studies found this to be a best practice (10).



Skill components

Evidence is strong that programmes promoting concrete behavioural skills do considerably better than programmes primarily offering information and awareness (19). Programmes focused on social skills, for example, have been shown to be successful in youth violence reduction (4, 169). The following are some of the specific skills whose benefits have been most clearly associated with more successful prevention programmes (15).

Problem-solving skills. Reviews of successful programmes that prevent youth problems often identify problem-solving components as one of the most frequently included elements (14). These components engage children in thinking through situations of uncertainty, conflict and crisis to choose modes of effective response using stories, role-plays or other methods. Some emphasize taking time to reflect and recognize body signals and other signs of ambivalence.

Assertiveness, self-efficacy, resistance to peer pressure. This is a very widespread component in youth safety training, used in nearly 80% of evidence-based programmes (15). It teaches the skills to resist peer pressure and problematic propositions, amplify internal hesitations, and to say no or to escape from problematic situations. It also teaches assertive body language and distinguishes assertive from aggressive responses. The logic for online VAC situations is that, with practice, children and youth could, for example, resist peer pressure to share images with sexual content or extricate themselves from inappropriate interactions with adults. Assertiveness may also empower youth to set limits to cyberbullying or stalking behaviour.

that add with disa homeles to be a b

Empathy, perspective-taking, difference appreciation.

This widespread component helps children and youth to understand and accurately recognize the feelings and needs of other people especially in situations of conflict (16). It also helps them identify how differences in backgrounds and experiences can lead to different points of view. It encourages children to see value in differences, particularly differences like race, religion, disability, gender presentation and sexual orientation, which are often flashpoints of hostility, rejection, or diminution. A review of 18 randomized controlled trials found empathy training was effective in general but less so with children and youth than with university students (170). Another meta-analysis of 81 studies found that youth programmes with perspective taking and empathy promotion did reduce discrimination and prejudicial behaviour (9, 17).

Self-regulation, emotion management, impulse control. There are a variety of components to youth problem prevention programmes that teach self-regulation. These range from calming exercises, relaxation, deep breathing, meditation, self-distraction, to monitoring emotional arousal. The prevention logic is that such skills prevent angry responses to interactions or impulsive decision-making under emotive conditions. The model applies to both potential victims as well as potential perpetrators. A review of 41 studies found consistent improvements from self-regulation in programmes addressing substance abuse, conduct and behavioural problems and school suspensions (18, 19). Effects were positive across all age groups.

Conflict resolution, de-escalation. These skill-promotion components teach children to identify escalating conflicts, and provide them with management tools like withdrawal, acknowledgement of conflicting needs and the other person's point of view, avoidance of insults, compromise and seeking a third-party's assistance. The logic applied to online VAC is that if children can be equipped with such skills, disagreements and conflicts might not escalate to aggression, and potential perpetrators and victims could resolve or withdraw from escalating situations. Evidence from 36 studies found that programmes that included conflict-resolution skills improved anti-social behaviour, with larger effects for early- and midadolescents (19–21).

Help-seeking. Help-seeking as a skill implies more than simply urging young people to seek help with problems (22). It also generally includes training in identifying who their trusted helpers are, overcoming some of the barriers to help-seeking like embarrassment, and practicing the identification of problems that warrant help-seeking. Several studies (22, 23) show positive effects of educational programmes on help-seeking and stigma reduction.

Bystander or defender mobilization. This component tries to teach youth who observe conflict to intervene to discourage aggressors or to support and protect victims. It has been implemented in bullying prevention, dating violence and sexual assault programmes and is grounded in research that peers frequently witness bullying or know about friends' abusive and inappropriate relationships but are reluctant to comment or intervene (171, 172). Research also finds that aggressors are deterred when they perceive that their behaviour will cost them respect among peers. Bystander mobilization creates environments where peers articulate their opposition to bullying or cyberbullying and concerns about inappropriate or abusive relationships. Programmes teach bystanders how to identify abuse, how to overcome passivity, how to articulate opposition to aggressors and how to support victims (28). Programmes have been shown to increase bystander intervention (24). Peer and bystander mobilization has been successful in sexual assault prevention (25) and in bullying prevention (8). A review of a small number of studies on cyberbullying prevention found bystander components worked better with older youth when paired with empathy induction (25).

Knowledge components

Research suggests that information alone is not sufficient to change behaviour. However, specific types of information may help when included in better-designed programmes, particularly information that is accurate, convincing and new. These are several types of information that have been shown to be associated with more successful programmes.

Social norm instruction. Many programmes provide children and youth with information about what is considered appropriate or inappropriate, legal or illegal (called injunctive norms), and also information about what the rates of behaviours are in their community (called descriptive norms). For example, there are domains where children may be unaware about norms: around sexual touching, sexual consent, or age of consent laws. Youth also often have exaggerated ideas about how many of their peers engage in various behaviours – for example, sexting or sexual intercourse. A meta-analysis (26) finds social norm instruction effective, particularly with adolescents. In addition, injunctive norm instruction (what people believe others should do) tends to be more effective than descriptive norm instruction (what they actually do). Also, norm instruction is more effective in Asia and Latin America, more collectivist cultures, than in the USA.

An important caveat is that normative instruction can possibly backfire in rapidly changing environments and when it is at odds with strong youth perceptions. Telling youth that sexting will get them prosecuted may not work when they are aware that there is much sexting among peers but no prosecution. Such disjunctions may create cynicism among youth audiences about the credibility of a programme or its instructors (173).

Sex education. Sex education is challenging because parents and communities around the world are conflicted about what should be taught and who should do the teaching. It is complicated because there are many possible topics for sex education and disagreements about which are useful and appropriate for children of different ages. There is evidence (27, 28) however, that comprehensive forms of sex education can reduce physical and sexual aggression, in particular homophobic bullying, dating and partner violence. The effectiveness of sex education has been confirmed (29) in low-, middle- and high-income countries (148). This suggests that sex education is an evidence-based element that can play a role in reducing grooming, nonconsensual sexting, CSAM consumption, and livestreaming. But given cultural differences and sensitivities, sex education components to prevent online VAC may require more than the usual careful planning, as well as testing and customization in different contexts.

Substance abuse education. Many of the longest standing youth prevention programmes began by addressing substance abuse and refined and tested their components over several decades. Substance abuse is associated delinquent behaviour, violence perpetration and victimization, as intoxication goes along with reduced inhibitions and expectations of norm violation. A review of 158 studies found substance abuse education one of the most reliable components of successful programmes (19).



5.3 Prevention education approaches needing more research

Online-only programmes. Some prevention programmes are designed to be delivered entirely in a digital environment, through games or educational applications and have been shown in a meta-analysis of 16 studies to reduce bullying and cyber-bullying (174). But some of the findings in the review and in the larger literature suggest they may be less effective because they do not as reliably influence the whole-school environment, including teachers and peers.

Fear appeals. Much advice about what works in youth prevention has counseled against using fear. Indeed, there were earlier studies, particularly from the drug-awareness field, arguing that fear appeals were ineffective or even counterproductive (175). However, in recent years systematic reviews have found much evidence that certain types of fear appeals actually do work in many behaviour-change situations (176). Nonetheless, the challenge of designing successful messages using this approach is complicated. Unfortunately, there is little specific guidance about the best strategy for using fear appeals with youth populations, though blanket claims about its lack of efficacy are no longer warranted.

Youth leadership. The concept of engaging young people in the design and leadership of prevention education has a strong appeal. Young people provide a crucial knowledge of the target population and may be more influential than adults in changing peer attitudes and behaviour. Peer leadership programmes have been evaluated in prevention domains like sexual health but the evidence is still limited and inconclusive (177).

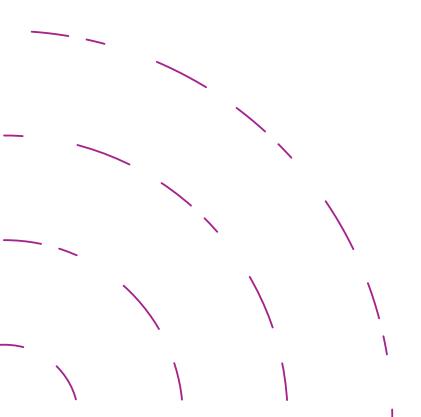
Cautions

This section has reviewed a large literature made up of systematic reviews drawing summary conclusions across a large number of studies in different domains. In interpreting its relevance, various cautions need to be observed:

- The studies emanate primarily from North America and Europe and may not apply to other regions.
- The studies often do not specify the applicability of their conclusions to specific populations like sex and gender minorities and racial and ethnic subgroups.
- The studies do not specify the applicability
 of their conclusions to the different stages
 of child development, and what modifications
 apply to these stages.

Summary

There is considerable guidance from the large prevention education literature about the components of successful programmes. Many of the conclusions drawn from the larger literature of safety and health have been reconfirmed as successful in the violence prevention field and even in some cases specifically in the field of online VAC prevention. As discussed in the next chapter, some of these components are widely included in online VAC and related programmes - such as multiple educational modalities and encouragement of help-seeking. Others are less widely included – such as emotion-management skills or trainer quality control. Nonetheless, this chapter's list provides a strong and broad foundation on which programmes can build and assess their own likelihood of success.



6. Evidence for effective online violence against children programmes

This section reviews the small but growing evaluation literature about programmes that either are designed to prevent online VAC or have been assessed for their influence on online VAC.

The evidence for online VAC-specific prevention programmes is still in its infancy. We conducted a search for evidence on the effectiveness of such programmes (see Annex 1, Methodology) across the various online VAC topics. There was considerable evaluation evidence for programmes that aim to reduce cyberbullying. There was some evaluation evidence about programmes to stop hacking, fraud, identity theft and generally improve cybersecurity. But there were few evaluations about programmes to address sexual online VAC domains.

Cyberbullying

Cyberbullying was the only online VAC domain with a strong collection of evaluation studies from which conclusions could be confidently drawn. That collection of studies was large and showed positive programme effects. There were at least eight systematic reviews and/or meta-analyses of this evaluation literature on cyberbullying prevention: among these, one reviewed 24 studies (9); a second reviewed 50 studies (4); a third reviewed 17 studies (168); a fourth reviewed 19 studies (5); and a fifth reviewed 30 studies (2, 11, 16, 20, 178). All reported positive outcomes from programme participation.

The reviews of cyberbullying-prevention programmes were extensive enough to yield some important additional conclusions:

- Programmes were successful at reducing both cyberbullying perpetration as well as victimization (4).
- The prevention effectiveness in relation to cyberbullying was equivalent in strength to the effectiveness for preventing conventional bullying.
- There were successful cyberbullying prevention programmes developed in a range of countries from different regions including Austria, Cyprus, Italy, Mexico, Spain, Taiwan, China, Turkey (see Table 3) (4).
- Cyberbullying was reduced by programmes that were totally focused on cyberbullying, and also by programmes with just some cyberbullying content (about a quarter of the programmes) (4).
- Programmes were successful when directed at both middle-school and secondary-school-aged children.
- Programmes were successful when delivered primarily from an online platform as well as when delivered face-to-face in conventional classroom lessons.
- Programmes were lengthy and multi-session, on average lasting 22 weeks (4).

Table 3. Evaluated cyberbullying prevention programmes^a

Country	Number of studies	Programme name (number of studies)
USA	17	Arizona Attorney General's Social Networking Safety Promotion and Cyberbullying Prevention (n=2) Cyberbullying: A Prevention Curriculum for Grades 6–12 HAHASO (Help – Assert Yourself – Humor – Avoid – Self-Talk – Own It) i-SAFE GREAT (Gang Resistance Education and Training) Second Step Middle School Programme Bulldog Solution Intervention Model Go Grrrls Programme Olweus Bullying Prevention Programme Stand Up: Virtual Reality to Activate Bystanders Against Bullying Department of Elementary and Secondary Education (DESE) lesson on bullying Restorative Practices Intervention
Spain	8	Cyberprogramme 2.0 (n=2) Asegúrate (n=2) ConRed TEI (Tutoria Entre Iguales) PREDEMA Prev@crib
Italy	4	Noncadiamointrappola! (Let's not fall into a trap) (n=2) No Trap! TABBY
Germany	3	Media Heroes (Medianhelden) (n=2)
Finland	3	KiVa
Austria	2	ViSC Social Competence Programme
Greece	2	TABBY
Turkey	2	NR
Belgium	2	Friendly Attac
Australia	1	Cyber Friendly Schools
Taiwan, China	1	WebQuest
Mexico	1	Internet Cyberbullying Prevention Program
Cyprus	1	ViSC Social Competence Program
Netherlands	1	Dutch Skills for Life

Source: (4)

^a This study included published and unpublished studies (1995 to August 2019), written in English, Spanish, or Turkish. It also included randomized and non-randomized evaluation studies with students in K-12. Included interventions for cyberbullying victimization and/or perpetration, and wider violence prevention interventions that measured at least one cyberbullying outcome.

Some of the successful cyberbullying prevention effects were programmes with long histories in the bullying prevention field, much research to back them up, and an international presence. They include programmes such as the Olweus Bullying Prevention Programme (179), KiVA (166), and Second Step (180).

But other successful programmes had a narrower cyberbullying focus, like the Spanish Cyberprogramme 2.0 (181, 182), which aimed to increase adolescents' antibullying skills through building interpersonal conflict-resolution abilities and self-esteem through 19 one-hour sessions in groups of approximately 20 adolescents.

An example of another successful programme, with web-based, online educators, was the Italian No Trap programme (183), which addresses face-to-face bullying and cyberbullying. WebQuest from Taiwan, China, is also an online curriculum that is composed of eight 45-minute sessions (184). This programme is delivered as a series of interactive "missions" that students must solve together in small teams regarding the dangers of cyberbullying.

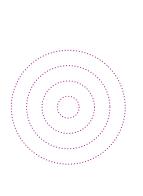
The evaluation research focused on cyberbullying has some encouraging news for online VAC prevention in general.

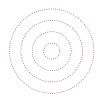
- At least one form of online VAC, cyberbullying, is clearly amenable to prevention.
- It worked well to take developed strategies from a non-online VAC domain such as bullying and apply them to the online VAC domain of cyberbullying.
- Varied formats and adaptations showed evidence of success, for example, classroom and web based.
- Successful programmes have been developed in different parts of the world in different cultural environments including some low- and middleincome countries.

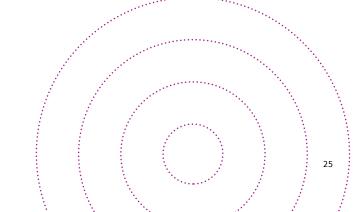
The apparent success of cyberbullying prevention, both for victimization and perpetration, prompts an important question: can that success be used as a foundation or template for the prevention of other types of online VAC besides cyberbullying? Several lines of evidence provide encouragement for this idea.

- There are strong, established connections (89, 92, 185–187) between bullying and other forms of violence against children such as dating violence, stalking, and sexual harassment. This means that effective cyberbullying programmes could be successful in preventing other online VAC types such as cyberstalking, unwanted sexual solicitation and perhaps also nonconsensual sexting, sextortion and sexual image abuse. This could be done by adding examples and scenarios from these domains.
- According to programme content analyses (108), bullying prevention and other violence-prevention programmes share many of the same messages and skill elements. Evaluations also have shown that traditional bullying-prevention programmes have positive influence on other forms of violence and vice versa as well (108). This suggests that successful extension to other online VAC domains may not require a great deal of added content.
- From a developmental perspective, bullying (which often begins in elementary school) can be addressed earlier than some of the teen-related online VAC domains such as stalking and sextortion. Thus, bullying programmes for pre-teens may introduce concepts like respect, empathy, and bystander mobilization that can become keystones for addressing other problems later on. There may be synergistic benefits when children begin early to acquire these skills and transfer them from one domain to another.

The consistent evidence for both bullying and cyberbullying prevention does suggest that such programmes could be good foundational programmes from which to extend successful prevention to other forms of online VAC.









Hacking, fraud, identity theft

There are many programmes aimed at youth to help prevent hacking and fraud and other generic cybersecurity dangers. These programmes include topics about privacy, phishing, passwords, security settings, and illegal content. One meta-analytic review found 56 studies on cybersecurity awareness programmes for children and youth (98). The evaluations primarily measured increased awareness and skill acquisition, for which the programmes were generally successful. However, no studies tested whether programmes actually reduced episodes of hacking, fraud, or other cybersecurity breaches. Another review examined 119 cybersecurity "tools" including games, films, modules, and comics (99). None of these was evaluated with regard to actual reductions of cybersecurity breaches (188).

It is encouraging that cybersecurity programmes are being evaluated and reviewed in systematic reviews, but as yet there is no evidence on whether programmes increase cybersecurity for youth, or what strategies are most successful at doing so.

Online child sexual exploitation and abuse

The literature on what works to prevent online sexual exploitation and abuse (such as online solicitation and grooming, nonconsensual sexting, CSAM or livestreaming) is extremely thin (189, 190). We found one systematic review of prevention programmes aimed at online sexual abuse. The programmes were an assortment of mostly weak designs. None measured online behaviours (such as sending a sexual image without consent) or online child sexual exploitation and abuse risk behaviours (such as posting a selfgenerated intimate image). Two showed knowledge gains, one showed a paradoxical increase in risk behaviour, and one showed no change in safety-related attitudes. This weak track record should not necessarily be discouraging. It likely reflects the relative immaturity of programmes and their reliance on awareness raising strategies rather than strategies for behaviour change.

The weakness of evaluations in the online sexual exploitation and abuse domain is exacerbated by several factors. The most important is that the sexual victimization and perpetration outcomes, which need to be measured for evaluation purposes, are sensitive topics. Their disclosures are often difficult to elicit from programme participants and from their families and institutions in an exact and ethical way. So, such data are often not collected.

In addition, even if feasible to ask about, the sexual victimization and perpetration outcomes of interest to programmes are relatively rare, compared to the frequency of outcomes like cyberbullying, so evaluation studies need to be very large and to monitor participants for a long time in order to have enough cases to compare between experimental conditions. Such designs are expensive and time consuming, so they are usually not done.

Sex-related safety topics do pose major challenges for prevention, more than is the case for bullying or hacking. Cultures and subgroups within cultures have very different views on sexual behaviour norms and the proper contexts for talking about them. These are fraught topics for teachers as well as parents, who may feel ill-equipped to address them. These are also topics that may be embarrassing for children to openly discuss. The topics have different and sometimes problematic implications for children and adolescents of different genders and sexual orientations, which may require special designs. They are topics whose prevention content may need to shift rapidly over the course of development, as youth knowledge, experiences and norms change quickly with age. All these challenges have slowed the development, deployment, and evaluation of quality online sexual exploitation and abuse prevention programmes.

Borrowing from related evidence-based prevention domains

There is a need for a planned and concerted process of development and innovation to combat online child sexual exploitation and abuse. This process should include consultation with youth from different cultures and also developers in other safety domains.

There is a well-developed field of sexual abuse prevention education that has been refined through programme evaluation. While meta-analyses show that children exposed to these programmes acquire knowledge and skills (7, 191), it is unclear yet whether this yields a reliable reduction in abuse perpetration or victimization. One limitation is that most of these prevention programmes are directed at elementary and middle school-aged children. Many do not address the challenges and risk factors that emerge when youth become interested in romantic and sexual relationships that underlie considerable vulnerability to online sexual abuse.

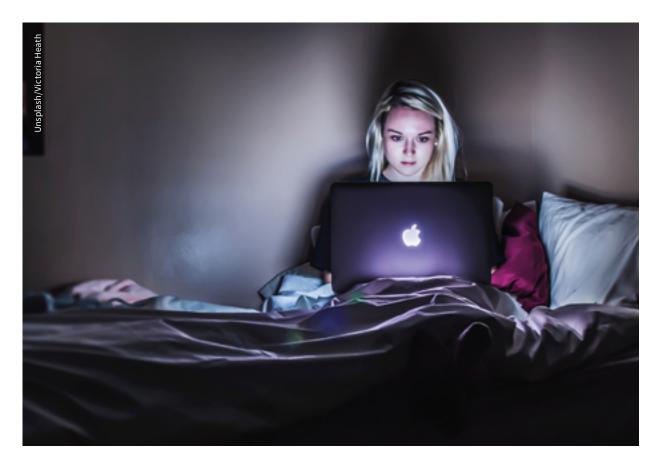
The sex education field (192) is another obvious place to turn for guidance (193, 194) about content and curricula relevant to online VAC. The components of comprehensive sex education have been shown (192) to have many positive outcomes that mitigate sexual violence. For curriculum specifics, UNESCO's International Technical Guidance of Sexuality Education (193) showcases many modules aimed at preventing online sexual abuse. It illustrates how to cover interrelated violence topics – bullying, dating violence, grooming, nonconsensual sexting, and sextortion – in an integrated comprehensive way. A systematic review of 22 school-based sex education curricula in

low- and middle-income countries found that 16 of these programmes were successful in reducing risky behaviour (195). The programmes delayed sexual debut, reduced sex frequency, decreased numbers of sexual partners, decreased unprotected sex and increased condom and contraceptive use.

Another very relevant source are the educational programmes developed as part of international HIV/AIDs prevention. HIV/AIDs prevention was a problem that also involved broaching sensitive sexual topics in a diversity of cultures and contexts (196) during an era of changing youth behaviour. HIV/AIDs education also experienced considerable challenges and setbacks, but it was assisted by strong public health orientation and deliberate efforts to build evaluations into programme development and dissemination

A final literature to be consulted and integrated is that which relates to relationships and dating violence. As indicated earlier, a considerable portion of online sexual abuse perpetration occurs by other youth who are former, current, or aspiring romantic partners. These dating violence programmes discuss topics such as consent and respect, the attributes of positive relationships, and signs of control and abuse. They have been shown to be effective at reducing sexual and relationship violence (197).

Despite these many opportunities for integration and borrowing, one of the most difficult challenges for online VAC prevention is how to reduce the generation and circulation of CSAM. While education programmes do currently make efforts to reduce teen sexting and self-produced sexual images – which can feed into supply

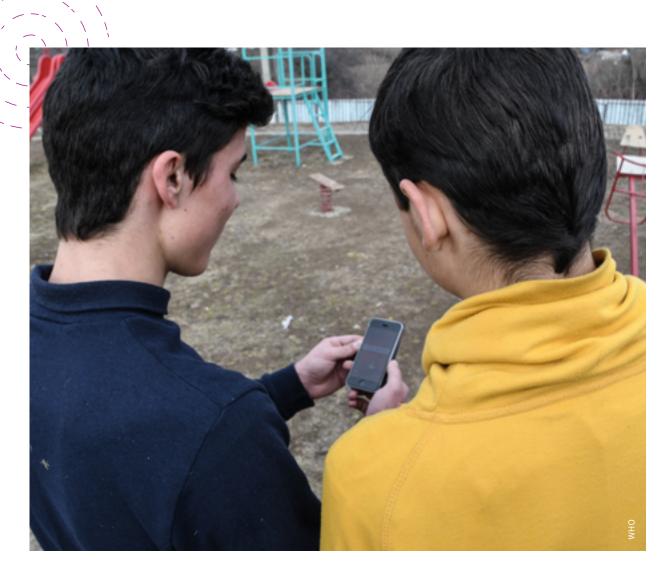


of and demand for CSAM – a large component of CSAM comprises images of young children that are made and consumed by adults, a group not readily accessible for the kind of education and skill-building approach that characterizes successful youth prevention.

Nonetheless, youth prevention education could play a larger role in CSAM. Pornography use and even access to CSAM begin during adolescence for a considerable portion of the user population, and youth-oriented sex education programmes might be successful at reducing this (198). Information about the criminal status of CSAM and the harm it causes to victims may be persuasive information for youth at this age, and they may benefit from learning how to avoid such images and what to do if encountered. Skills-related emotion management, improved interpersonal relationships and decision-making might also be relevant for this population to avoid harmful pornography and CSAM use (199). These skills may also work to protect against later adult involvement in CSAM. This approach to CSAM reduction is less direct than some of the approaches currently being promoted, but it may be worth evaluating.

Summary

The good news is that for one type of online VAC, cyberbullying, there is an extensive evaluation literature that finds prevention education in a variety of formats for a variety of ages is successful in reducing perpetration and victimization. The bad news is that the literatures on other forms of online VAC, especially sex offences, are lacking, and do not provide direct confirmation that prevention works or which educational strategies work best. For guidance around these topics, programme developers need to return to some developmental work with stakeholders – including children – and the experience of HIV/AIDS and other sexual risk-prevention literatures.



7. What currrent prevention education programs are actually saying and doing to address online violence against children

This section reviews an international sample of well-developed educational programmes with online VAC prevention content. It highlights the evidence-based elements and messages contained in those programmes.

An array of educational programmes and modules have been developed all over the world by organizations anxious to prevent online harms to children. These programmes come in a variety of forms. There are curriculum guides for teachers, websites for independent youth navigation, and compilations of videos and discussion prompts for general use. Some are targeted at elementary and middle school-age children. Some are targeted at younger and older teens.

In this section we examine the features and characteristics of some of these programmes. One goal is to make potential developers more familiar with the varieties and commonalities of these programmes. Another is to assess the degree to which they incorporate practices and messages that appear effective, based on our analyses of programme components and logic models.

We searched widely for programmes using multiple search terms and covering diverse regions and languages of the world. We restricted qualifying programmes to those characterized as well-developed, meaning that they needed to have:

- a multi-page website describing the programme and its components;
- educational modules for children and youth, delivered either via educators or designed for youth to engage with directly;
- · coverage of at least two or more online VAC topics.

Fifty-six different programmes were identified that met the above criteria and had enough details to review.

Online VAC programme features

Programmes have been developed all over the world. Well-developed examples were found in Malaysia, Czechia, Brazil, and Qatar, among other places. As expected, high-income and English-speaking countries hosted more of the programmes we could access (USA 21%, UK 17%, Canada 7%, and Australia 5%) but there were also programmes from many European countries (35%) as well as Asia (16%), including Cambodia, China, Indonesia, Malaysia, the Philippines, Thailand, and Vietnam (see Table 4).

Most of the programmes purported to be relevant to a broad spectrum of children from elementary to secondary school. Almost all covered ages 10–15 years, while 83% covered ages 6–9 years and 87% covered ages 16–17 years. Despite these broad coverage ambitions, most programmes did not have strongly customized content for different age groups. Thirty percent had uniform content for all age groups, 34% for two age groups and only 36% for more than two age groups.

All programmes reviewed covered at least two online VAC topics, but most programmes covered much more. Cyberbullying was almost universally addressed (98%), as was grooming (98%). Hacking, fraud, and identity theft were also reliably included (93%). Sexting was featured in 84% and sextortion in 62%; dating abuse and revenge porn in 71%. Livestreaming was broached in just half (51%) of programmes. Commercial sex abuse and trafficking were not widely addressed (only 15%). Interestingly, exposure to "sexually inappropriate" content, typically meaning pornographic images or sexual content deemed inappropriate for children, was featured in 80%. Some of the programmes covered

a very broad range of digital skills and might be better referred to as "digital citizenship" programmes, but in 80% of the programmes the majority of the content was about online VAC.

Most of the programmes had the potential for adequate levels of different content: 93% had five or more lessons or modules, and 43% had 10 or more. The availability of these multiple opportunities, however, does not ensure that all youth really got all these exposures. But the availability of multiple exposures confirms that many programme developers have moved beyond the single-session education model. As a caveat, we reviewed only well-developed programmes that had multiple online VAC topics and thus probably multiple exposures. It is likely that single-presentation programmes had fewer well-developed websites.

Moreover, most of the programmes in our sample were designed with evidence-based structural elements: 93% had skills-building practices for children, 85% had interactive activities, 88% had information for parents, 80% provided curricula for trainers and teachers and 63% had training materials. Only a third (35%) had materials for whole-school involvement (an element known to amplify effectiveness), but this reflects in part the fact that many programmes were designed for out-of-school administration and independent youth engagement.

Ninety percent made it possible for youth to access and engage with the programme independently without a school facilitation, and 13% used this design exclusively.

We reviewed the programmes to identify whether they included topics and content that have been shown to work in prevention education. All the reviewed programmes had content about help-seeking, 98% had content about refusal and disengagement, and 98% emphasized the harm that could be caused by cyberbullying and nonconsensual sexting. Bystander mobilization was promoted in 80% of programmes. Interestingly, statements to the effect that victims are never to blame (blame exculpation to promote help-seeking) were mentioned in only 45% of the reviewed programmes.

The overall pattern suggests that highly accessible programmes are internationally available, reliably cover several core online VAC topics and have sufficient content for multiple topic exposures. These programmes have also paid attention to the evaluation literature and have evidence-based features like skill-building exercises, interactive activities, information for parents, and guidance for educators. Some core messaging and training are universal about help-seeking and refusal-disengagement behaviours.

Table 4. Characteristics of programmes with online VAC content*

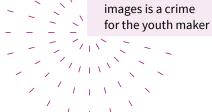
Region	Percentage (N=56)
USA	21
UK	18
Canada	7
Australia	5
Europe	36
Latin America	7
Africa	2
Asia	16
Middle East	4
Age range coverage	Percentage (N=47)
Age range coverage <6 years	Percentage (N=47)
	_
<6 years	43
<6 years 6–9 years	43 83
<6 years 6-9 years 10-12 years	43 83 98
<6 years 6–9 years 10–12 years 13–15 years	43 83 98 94
<6 years 6–9 years 10–12 years 13–15 years 16+ years Versions for multiple	43 83 98 94 87

Online VAC topics	Percentage (N=55)
Cyberbullying	98
Grooming/exploitation	98
Hacking/fraud/ identity theft	93
Dating abuse/relationship/ revenge porn	71
Stalking/cyberstalking	49
Online solicitation/ unwanted solicitation	58
Sexting	84
Sextortion	62
Commercial sexual abuse/ trafficking	15
Livestreaming/webcam	51
Sexually inappropriate content	84
Majority of content safety topics	80

Programmes identified in a desk review of online VAC programmes for children and adolescents

Number of modules or lessons	Percentage (N=56)
>5	7
5-10	50
11-20	30
20+	13
Structural elements of programmes	Percentage (N=56)
Skills-building practices	93
Parental information	88
Parent engagement linked to youth modules	85
Materials for whole school	35
Interactive activities for groups	85
Curriculum available to help trainers	80
Training available for trainers	63
Independent online child/ youth engagement	
• Not possible	9
• Possible	78
• Solely	13

Generic skills	Percentage (N=55)	
Help-seeking	100	
Bystander mobilization	80	
Refusal/disengagement	98	
Harmfulness	98	
Blame exculpation ("it was not your fault")	45	
Grooming messages	Percentage	Sample size
No reference to grooming, sexual exploitation, sextortion	5	(N=56)
Grooming as primarily stranger danger	65	(N=52)
Grooming emphasizes adult identity deception	57	(N=51)
Uses "no interaction with unknown persons"	43	(N=54)
Uses "no meeting offline with online friends"	58	(N=52)
Uses "no sharing personal information"	54	(N=54)
Sexting messages		
Discusses the dangers of sexting	96	(N=47)
Any acceptable context for sexting	34	(N=47)
Uses "never make sexual images"	30	(N=47)
Warns that making images is a crime	63	(N=48)



Content about online sexual exploitation and abuse

Online sexual abuse is one of the dominating online VAC concerns. Ninety-five percent of programmes covered at least one aspect of this topic (see Table 4). But the topic is challenging because of varied norms across communities in relation to talking to children about sex. It is important to know how the content on these topics is being conveyed and whether the information being provided is accurate and useful. So, we reviewed how the prevention programmes were handling topics such as grooming and sexting. There was a mixture of contrasting approaches.

Sexual perpetrator identity messages

We coded programme messages to examine whether they characterized the grooming problem primarily in terms of stranger perpetrators: 64% had that orientation, but 36% did not. Thus, an emphasis on stranger perpetrators was widespread but not the sole emphasis in this sample of well-developed safety programmes.

These were examples of the common messages about not talking online to strangers:

"Students should avoid talking to strangers online and should only connect with people they have met face-to-face." eSafety Commissioner

"Most of us talk to people online – it's a great way to stay connected. It can even be a good way of making new friends sometimes. But it's really important to understand the dangers of talking to someone you don't know." Childline

In these messages the danger is being associated with fact that someone is unknown (they have not met face-to-face), when online sexual abuse and exploitation dangers are also very common among known persons, and the dangers may be better characterized as inappropriate behaviours by anyone – known or unknown, stranger or acquaintance.

Many programmes (57%) also emphasized identity deception (fraudulently assuming another identity) as a key element in their description of the problem. For example,

"Grooming describes a process in which an adult, anonymously or under a false identity, builds up a relationship of trust with a minor on the Internet over a longer period of time." Bee Secure

It is not fully known how frequently identity deception occurs in the dynamics of online grooming and sexual abuse and exploitation. But it is clear that most nonconsensual image sharing and much of the adult grooming of youth occurs with known acquaintances. Whether victims really know the true identities of perpetrators may be less important than children recognizing the trust manipulations that offenders use. Some programmes gave a more detailed account of those trust-building ploys without a primary emphasis on identity deception. For example:

"Grooming is the strategy with which an adult solicits and manipulates a minor for sexual purposes. Groomers are generally very manipulative and take time to gain trust and bond. Gradually, they incite sexual acts. Groomers gain trust by playing the understanding adult friend and giving compliments. This is how they try to induce the victims to strip naked. The perpetrator can also be a known person, such as a family member. Most victims know the perpetrators are adults." Child Focus

Another programme mentioned deception as one strategy among others and named these other strategies, opening the door to deeper understanding:

"They may use fake accounts and photos or say they enjoy the same hobbies and interests as the young person they are grooming. Others may pretend to be modelling scouts, sports coaches, celebrities, or influencers. However, not all groomers will choose to hide who they really are, and some may try to build a connection or develop a 'mentor' type relationship based on their true identity." Childnet

Another facet of the emphasis on strangers is the use of typical warnings against interacting with unknown persons (43%), sharing any personal information (50%), and going to meet in person anyone you first met online (58%). This was an example of a meeting warning:

"No matter how long they've been talking to a friend they met online, they are still strangers that they shouldn't share personal information with or arrange to meet in person." Safe Internet UK

And here are examples of very blanket advice about personal location information that implied strangers were the main perpetrators:

"Remind children that they should never post sensitive information online as it could help predators locate them." Monique Burr Foundation

"There are also some things you shouldn't share with others online like: your age, your address, where you go to school, email address." Netsmartz

By contrast, some programmes cautioned specifically against an overemphasis on strangers and discussed, even if briefly, the variety of possible perpetrators. Here are some examples:

"Online groomers are not always strangers. In many situations, they may already have met them through their family or social activities and may use the Internet to build rapport with them. Sometimes children don't realize they've been groomed and think that the person is their boyfriend or girlfriend." Internet Matters

"Warn young people that there are people online who target adolescents to engage in sexual conversations. Make sure they understand that this is not limited to people they have met online: people they know offline may try to use digital platforms as a private space for grooming them." Media Smarts

"One of these outdated techniques is the oftenrepeated phrase, 'Don't talk to strangers'. The term 'stranger' is an ineffective concept for teaching safety to children as the term itself is too abstract for younger children. Often, once a child has met an individual who has been nice to them and does not appear scary in appearance, they no longer perceive the individual as a stranger. Also, since the majority of children are victimized by someone they know, the term 'stranger' is truly ineffective." Kids in the Know

"The image presented by the media of an older male deceiving and preying on a young child does not paint an accurate picture of the nature of the majority of sexual solicitations and Internet-initiated offline encounters." Netsafe

These programmes are presenting more nuanced information about the variety of offenders and avoiding simplistic rules about stranger avoidance. But it is quite apparent that online VAC education has not arrived at a consensus on how to characterize for children or their families the key elements of the online sexual abuse and exploitation problem. This is a crucial issue to resolve.



Sexting messages

Sexting was also a topic treated in contrasting ways by different programmes. Most of the programmes (96%) had some content about the possible dangers of sexting, with an emphasis on future career-damaging outcomes.

"Do you want to risk having sleazy teen photos surface when you're job hunting? Or how about when your kids are online 10 or 15 years from now researching family history for a school project?" Cybersafe Malaysia

Some programmes (23%) had a strong orientation that full abstinence from sexting was the proper course of conduct.

"Do not send any revealing photos/videos, either to people you trust or to strangers!" Bee Secure

"For maximum safety and peace of mind, don't share nude or sexually suggestive photos of yourself or anyone else, especially if under 18." Connect Safely

By contrast, some programmes (34%) acknowledged that sexting might have a positive role to play in romantic relationships but explained under what conditions it becomes problematic.

"Sexting can be part of a healthy relationship but could also become abusive if one partner pressures the other to send sexts." Media Smarts

"Sexting can also be without consequences and does not have to be evaluated negatively per se. It can be part of modern intimate communication if the participants are old enough, know each other well enough, behave fairly and respectfully, and observe some important cautions." Klicksafe

Quite a few programmes (54%) also gave stern warnings to youth about the illegality or criminality of a youth making sexual images.

"Sexting between children is still illegal even if they are in a relationship." National Online Safety

"Creating, possessing or sharing nude images of people under 18 may be a crime, even if it's a nude selfie." eSafety Commissioner

"Sexting is sexual abuse and illegal especially if the messages, photos, or videos are of someone below the age of 18. Even if children below the age of 18 share such information with each other it is sexual abuse." Arpan

"It's against the law to ask someone who's under 18 to send a nude image, even if you're under 18 as well." Childline

As discussed earlier, these unqualified warnings about illegality could deter victims of sextortion or nonconsensual sexting from reporting their victimization because they first created the image themselves.

By contrast, other programmes gave a more nuanced reading of the criminality issue.

"The police recognize that young people may create and share nude selfies because of natural curiosity about sex and exploration in a healthy relationship. The law was created to protect young people, not punish them." Think U Know

"Nude images of anyone under the age of 18 are illegal in the UK. The law does not want to criminalize young people who share nudes consensually in relationships, but if nude images of young people are shared without consent, there's a possibility the police could get involved." Think U Know

"It is illegal to share photos of others in private situations unless you have obtained permission, also called consent, from the person in the photo. It is illegal to share photos and movies that humiliate others or violate their privacy. It is illegal to share a picture of a person under the age of 18 if it shows sexual acts. It belongs to child pornography. However, you may share a picture of yourself with sexual acts with your boyfriend or close friend if you are over 15 – but it may not be shared on to others." Media Counsel for Children and Young People

How much legal information is useful and comprehensible to children? How can developers, instructors and parents stay on top of changing laws and practices? These are hard questions. It may be better to avoid using information about youth criminal exposure as a warning or motivator, because the information may be wrong or prone to misinterpretation.

There are obviously quite contrasting approaches being taken by the messages about online sexual abuse and exploitation. These are inherently very sensitive and complicated topics to discuss effectively. But caution is warranted in disseminating these messages because these contrasting approaches pertain to some of the key concepts that orient youth to the problem. Youth who receive messaging primarily about stranger danger may just fail to recognize grooming from an acquaintance perpetrator. Youth who believe they may go to prison for a sext they made could have a considerably more traumatic outcome to a nonconsensual usage. The field clearly needs a great deal of additional guidance rooted in more research, testing, and debate about how to design effective messages about online sexual abuse for different audiences.



Box 2. Indecent image and pornography exposure

Our findings show that exposure to indecent images or conventional pornography is a topic covered by many Internet safety programmes. The primary issue addressed under this topic is not CSAM, but how children and youth can avoid exposure to more conventional sexual images and content that are inappropriate for their age.

This is not a topic that we have reviewed for this report, primarily because it has not been deemed a form of violence against children.

Some types of indecent image exposure have aspects similar to online VAC, for example, when children are sent unwanted graphic images with the intent to shock or sexually engage them. But other types of indecent image exposure are less like online VAC, as when children seek out material from curiosity, when they come across sites accidentally or when peers share material for notice or comment.

Moreover, research on this topic is still undeveloped. There is a recognition that forms of pornography exposure can be harmful to youth (200) and there are recently developed educational programmes teaching pornography "literacy" to reduce negative effects (198, 201). Online VAC education programme developers who wish to include content on this topic should pay attention to this developing area.

Summary

Our search revealed over 50 well-developed, multitopic online VAC educational prevention programmes for children from around the world, including several from low- and middle-income countries. Most of these programmes had evidence-based components like multiple exposures, skills-building and interactive activities, information for parents and guidance for teachers and trainers - all of which are hallmarks of effective prevention. Training children in help-seeking, disengagement and bystander mobilization were also common. Messaging around perpetrators often had a primary focus toward strangers encountered online, with less attention to known acquaintance offenders. Some messages around sexting counseled abstinence and emphasized the possibility of criminal sanctions against youth. Others acknowledged sexting as acceptable in some contexts and under conditions of consent, and tried to assuage victims that they would not be treated as offenders.

8. Effective messaging

This section discusses several possible problems with messages currently conveyed in many online VAC programmes. They involve disconnects between the messages and the realities of online VAC dynamics and youth social behaviour in general. These problems include: the lack of adequate emphasis on acquaintance perpetrators in online sexual abuse and cyberstalking, the recognition of reasonable contexts for face-to-face meetings, and a harm-reduction approach to sexting, given the growing pattern of intimate image-sharing as part of dating.

One way to assess prevention programmes is to check whether their messages correspond with the reality of the problem they are trying to solve. Telling people to wear a scarf to avoid catching a cold is not the best advice if colds are primarily acquired from viruses on surfaces and in the air. In the online VAC field there are such mismatches. Many of the prevention programmes were designed before definitive research existed about online VAC dynamics and risk factors. Research is still scarce and evolving on many issues. But the developing research has demonstrated that online VAC problems are different from and more complicated than early stereotypes that informed messaging. As a result, messages may be missing important realities.

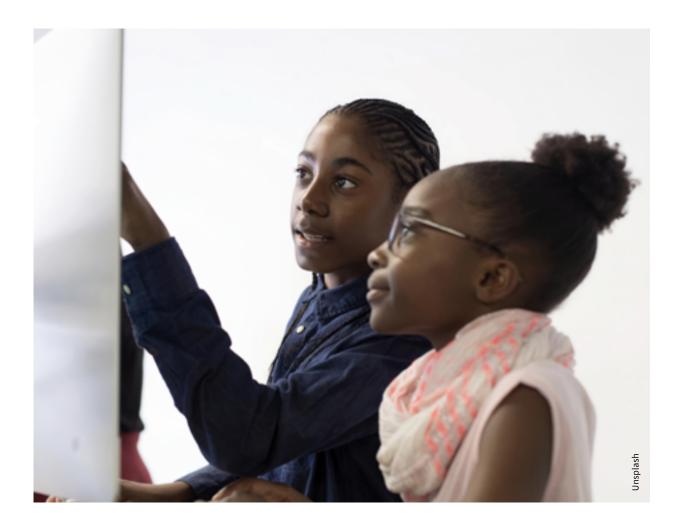
Neglecting the prevalence of acquaintance perpetrators

Strangers are not the sole or even the predominant offenders in online VAC. Studies show that adult online sex offenders are as likely to be acquaintances as strangers (50, 51). Victimization by acquaintances is very typical for unwanted solicitation, nonconsensual sexting and sextortion offences (43–47). The "acquaintance offender" reality is widely accepted about cyberbullying – but it is also true about online sexual abuse.

Stranger danger overemphasis is a mistake that has been made repeatedly in crime prevention. Child molesters were thought to mostly be strangers until research identified that family members, neighbours, teachers, and ministers were often the ones sexually abusing children. Assaulters were typified as street thugs until we recognized the ubiquity of abusive parents, intimate partners, and school bullies, who were less likely to draw police attention. The Internet is only the latest venue where we are allowing the stranger archetype to predominate.

Consider the many stranger-oriented messages that are widespread in Internet safety programmes:

- "Do not communicate with strangers you meet online"
- "People aren't who they pretend to be"
- "Never meet in person with someone you only know online."



Even if these messages help in some instances, the focus on strangers as the main type of perpetrator misses the mark in many ways.

- a. If these are the only, or main, messages in discussions about online VAC (or even just its sexual abuse components) they create complacency toward about a large part of the problem.
- b. These messages invoking stereotypes about criminals and stranger molesters also focus children's attention on what may be extraneous risk issues. The danger lies not in the fact that you do not know someone, but in the inappropriate behaviour they exhibit. Knowing someone's identity does not preclude the grooming, aggression, animosity, betrayal, and exploitation that are the dangers.
- c. Some of these stranger-oriented messages are so broad and categorical as to be impossible to truly comply with. For example:
 - "Don't share personal information": Many websites require users to provide some personal information. You cannot get an account or participate without it. Many people legitimately need some personal information to get in touch with you, for example a cousin who wants to send a present.

- "Don't communicate with someone you do not know": But some of the help sources we urge youth to consult – such as digital helplines – require them to communicate with someone they do not know.
- d. The concept of "stranger" or "person you met online" is nebulous and possibly hard to apply as online social interaction becomes more encompassing. What about your new teacher who is teaching online because of COVID-19 restrictions?
- e. What is really needed is good judgment about which strangers and which acquaintances are reasonable to communicate and share personal information with, under what circumstances, and, by contrast, what information in what situations needs to be guarded. No simple rule applies.

Virtually the whole online VAC programme universe needs a thoughtful reorientation to confront the large portion of the risks from friends, acquaintances, and actual and would-be romantic partners. The concerns about identity need to take second place to concerns about inappropriate behaviour.

Meeting online acquaintances in person

This message "don't go to meet in person someone you only know online" is common to many prevention programmes. Yet there is considerable and reasonable debate about how useful and effective this message is. The problems with this message emerge from two findings from the research. One is that frequently youth have justifiable reasons for and positive experience of meeting face-to-face people they first contact online. Another is that youth embarking on such risk taking will find this warning meaningless and irrelevant.

Many youth interact with and go to meet people that they (so far) have only known online. Safety advocates, immersed in danger narratives, have difficulty recognizing the vast number of situations where meeting someone like this is appropriate: for example, to find a drummer for your band or a recruit for your basketball team. To sell a piece of equipment. To finally meet your friend's friend who was part of a long-standing group conversation. In surveys (202) covering 19 countries (40), 16% of youth aged 9-16 years (including 33% of youth aged 15-16 years) met such a person in the past year. Importantly, 70% were happy and another 22% neutral about those meetings. Only 3% were fairly or very upset, but this could be for many non-threatening reasons (maybe the equipment they bought from the Internet contact did not work). Moreover, consider how many youth get upset after going to meet a typical offline friend or acquaintance. Upset is not the same as criminally victimized.

The ordinary norms of routine social life undercut the meaning or applicability of these broad, warning messages about stranger meetings. What youth need in reality is help in making discriminating judgments about when such meetings might be risky. One big risk context is around romance-motivated meetings.

The research on technology-facilitated criminal encounters raises other concerns about the "don't meet face-to-face" warnings. Studies of online grooming for criminal sexual relationships have several important conclusions about their dynamics (48, 203). Youth and perpetrator often communicate for a considerable time before they meet, during which the perpetrator comes to be seen as a friend rather than a stranger (204, 205). By the time the meetings are arranged, the youth know that romance and sex are on the agenda. The possibility of such outcomes may be a key part of the attraction. They may be online looking to experiment with relationships. They may see the relationships as an antidote to depression and low self-esteem. The youth generally do not want parents to know and often mislead them to avoid detection. For the many adult groomers who are offline acquaintances, the dynamics are similar. The abusers play on youth vulnerabilities and curiosity about sex and romance. What these potential victims need are not necessarily warnings about meeting strangers, but warnings about the risks and likely bad outcomes from sexual and romantic relationships with adults.



Grooming prevention for youth that addresses these complexities might include information about:

- age of consent laws and why they exist (206);
- why relationships with adults do not work, and the problems that they can create, including criminal prosecution of the adult;
- why adults might seek inappropriate relationships with youth;
- the kinds of strategies groomers use to befriend, isolate and seduce, including gifts, exaggerated flattery, guilt induction, insisting on secrecy, and denigrating friends and family;
- red flags for grooming such as someone rushing to ask a lot about your body and sexual experiences, and requesting sexual pictures, and putting you under pressure;
- the key deceptions, which are not about identity, but about the declarations of love, admiration, loyalty, and exclusivity;
- skills in how to refuse demands and extricate yourself from such relationships;
- skills for helping friends extricate themselves from such relationships (207).

These kinds of messages align better with the diversity and reality of much online grooming and may provide a better knowledge base and skillset for preventing bad outcomes.

Exchanging sexual images

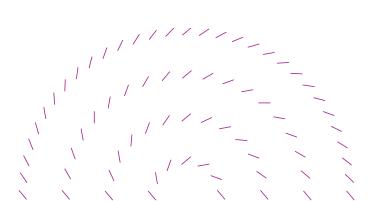
A common message intended to prevent sextortion and nonconsensual image sharing is the advice to simply avoid making or sharing images that are sexual, or images that you wouldn't want everyone (including your grandmother) to see (208). This message is likely persuasive to some youth, but increasing numbers of youth are nonetheless making and sending sexual images. A recent review suggested the sexting rates were about 20% for teens and even higher for older youth (68). The practice is described by researchers and sex educators in some parts of the world as a sometimes risky but increasingly accepted part of sexual exploration, which in so many of its facets tends to involve risks (65).

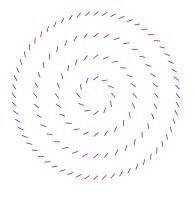
Education about sexual risk taking has long debated whether strict abstinence should be the primary message or whether it is important to also to promote additional harm-reduction strategies for those who decide to experiment (208). Advocates for harm reduction make the analogy with sex education and condom use. It is possible to have messages that both discourage early sexual debut and also provide information about how to stay safe if engaging in sexual activities.

Some sexting harm-reduction practices have been proposed (64, 209–212), including:

- only share images with someone you trust fully and make sure you know what the indicators of trustworthiness are;
- do not send images under pressure or when intoxicated;
- only share your own images with someone who has fully consented to receiving your images, by being asked beforehand – consent is crucial;
- teach safe sexting with strategies such as:
- Consider sharing images that may be revealing but stop short of showing your private parts.
- Do not include your face or other details in the images that may reveal your identity.
- Turn off location services and automatic tagging.
- Use apps that automatically and securely delete content after a period of time, and via sharing services with end-to-end encryption.
- Delete or be very careful about storing the images on your own devices where they may be seen or found by someone for whom they were not intended (173).
- If you receive images or videos from someone else, do not send them or show them to others, and consider whether they need to be reported.

Some other sexting messages may be useful. Since nonconsensual sexting and sextortion often grow out of abusive behaviour from intimate partners or those seeking such relationships, online VAC prevention programmes could do much more to alert teens to signs of healthy and unhealthy relationships, in particular relationships where trusting someone with an image may not be merited (28).







Some of the relevant signs of healthy and unhealthy relationships highlighted by evidence-based dating safety programmes include (213–215):

Healthy relationships:

- · Asks permission
- · Keeps commitments and promises
- · Apologizes for mistakes
- Feels respectful
- · Treated equally

Unhealthy relationships:

- Frequently angry or hurt
- Is controlling about who you spend time with and what you do
- Frequently jealous
- Tries to make you feel guilty
- · Has more allegiance to friends than to you
- Makes threats
- · Puts you down

Since programmes with messages such as these have been found to reduce teen relationship abuse, they may help youth make better judgments about sharing images and reduce nonconsensual sexting and sextortion.

Such harm-reduction educational messages are still under debate within segments of the prevention community and they are clearly not feasible in many cultural contexts. There is also not yet direct evidence about the efficacy of such messages, and likely it will be a while before they can be tested in a rigorous evaluation. Possibly the strongest indirect evidence for such an approach is that youth sex education has been found to increase contraceptive usage among teens (29, 193) meaning harm-reduction education around sexual behaviour does have strong empirical support.

Sexting as criminal behaviour

Many cybersafety programmes take pains to inform youth that making and sharing sexual images of themselves and their peers violates the law and can embroil them in criminal prosecution. This information is factual (210) in many locales, even though some countries have taken steps to decriminalize consensual sexting among youth. In most places, prosecution of youth for self-production is rare. But it poses a dilemma that educational programmes must address.

A message about criminal statutes may be new information to some youth with potential to dissuade them from making or sharing sexts (216) but it may have problematic effects as well. The most serious would be if it frightens victims of grooming and sextortion enough to deter them from reporting their victimization to authorities. Some victims, having heard the message, fear that they may also be charged with an offence because they originally created or shared their image (217). Even bystanders who viewed the images might be deterred from reporting. An additional problem is if the message promoting fear of prosecution sounds to some youth like an alarmist scare tactic that diminishes the credibility of the educator. This reaction may be especially true when teens know many peers who have made and exchanged sexts without being prosecuted in any way.

The utility of criminal warnings is an issue that begs for evaluation and clarification. Perhaps the message needs to be qualified by the reassurance that prosecution is rare and never mounted against a victim or a good-faith reporter. Perhaps its utility varies by age and local context. More discussion and research are badly needed because of the widespread use of this message and its potential for negative effects.

Cyberstalking dynamics

Messaging around cyberstalking, like grooming, also often has a stranger focus to it, with prevention emphasis on not giving out personal information or talking to strangers (218). This may be useful for some portion of the cyberstalking threat. But stalking and cyberstalking are also offences that more frequently occur at the hands of friends and former intimate partners – the most persistent and dangerous of offenders (219, 220).

More comprehensive and accurate stalking-prevention education (221) has a somewhat different emphasis. Its messages include:

- information about the wide variety of forms that stalking can take;
- establishing and reinforcing social norms so that potential victim and offenders will recognize when stalking is occurring and be deterred;
- empathy promotion so that offenders and bystanders can understand why some stalking behaviours are intimidating and upsetting;
- bystander mobilization, so that friends react sympathetically and supportively to other youth who are encountering stalking;
- help-seeking, dispelling self-blame, and explaining options for blocking, reporting to police and Internet providers.

These messages also seem very relevant to cyberstalking, which often overlaps with face-to-face stalking and cyberbullying.

Summary

The key point from this section is that many core messages in online VAC prevention need more nuance, critical discussion, and refinement. The current messages may not fully or accurately describe the nature of the problems they address. They may not be understood or capable of implementation by their young audience. It would greatly benefit the field of online VAC prevention to review and adapt messages and frameworks from the evidence-based educational programmes in the related domains of dating violence, bullying, sexual abuse and sexual risk prevention.

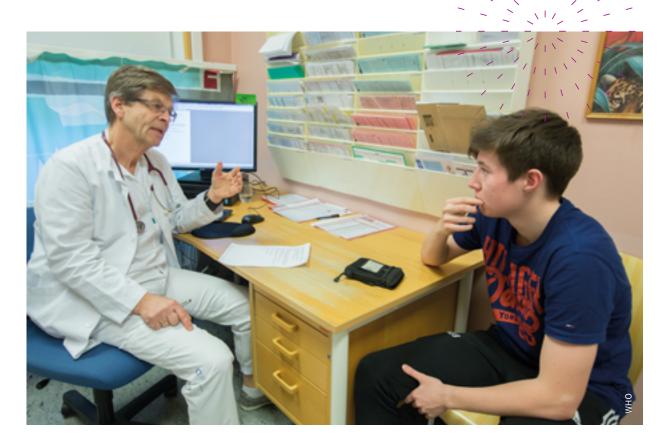
9. Conclusion

This section is a summary of key messages based on the evidence gathered as part of this review.

- Resources should be confidently and generously committed to child safety education programmes that have content that addresses online VAC and related topics.
- Priority should be given to building content about online VAC into existing evidence-based educational programmes, particularly about bullying, because of their well-developed content and design.
- Programmes need to have multiple sessions and multiple modalities and should emphasize acquiring and practicing skills, particularly in the areas of problem solving, assertiveness, empathy, emotion management, self-efficacy, conflict resolution, help-seeking and bystander mobilization.

 More programme content and messaging is needed to prevent abuse by acquaintances, peers and romantic partners, including content about healthy romantic relationships and how to avoid and terminate unhealthy ones.

This report is a snapshot from 2022 in the midst of a rapidly changing digital environment. It provides guidance about some promising and successful strategies in which to invest efforts. But it is still early in a growing field. It is premature to rule out other especially novel ideas that may be worth developing and testing. Given the rapid developments, this review should be updated in a few years as evidence emerges.



10. References

 Doty JL, Girón K, Mehari KR, Sharma D, Smith SJ, Su Y-W et al. The dosage, context, and modality of interventions to prevent cyberbullying perpetration and victimization: A systematic review. Prevention Science. 2021;23(4):523–537.

- Doty JL, Girón K, Mehari KR, et al. The dosage, context, and modality of interventions to prevent cyberbullying perpetration and victimization: A systematic review. Prevention Science. 2021;23(4):523–537.
- Jones LM, Mitchell KJ, Walsh WA. A systematic review of effective youth prevention education: implications for internet safety education. Durham, NH: Crimes against Children Research Center (CCRC), University of New Hampshire; 2014.
- 4. Polanin JR, Espelage DL, Grotpeter JK, Ingram K, Michaelson L, Spinney E et al. A systematic review and meta-analysis of interventions to decrease cyberbullying perpetration and victimization. Prevention Science. 2021:1–16.
- Lan M, Law N, Pan Q. Effectiveness of anticyberbullying educational programs: a socioecologically grounded systematic review and meta-analysis. Computers in Human Behavior. 2022;130:107200.
- Mertens E, Deković M, Leijten P, Van Londen M, Reitz E. Components of school-based interventions stimulating students' intrapersonal and interpersonal domains: a Meta-analysis. Clinical Child and Family Psychology Review. 2020;23(4):605–631.
- Zhang H, Shi R, Li Y, Wang Y. Effectiveness of School-based child sexual abuse prevention programs in China: a meta-analysis. Research on Social Work Practice. 2021;31(7):693–705.
- Gaffney H, Ttofi MM, Farrington DP. What works in anti-bullying programs? Analysis of effective intervention components. Journal of School Psychology. 2021;85:37–56.
- Gaffney H, Ttofi MM, Farrington DP. Evaluating the effectiveness of school-bullying prevention programs: an updated meta-analytical review. Aggression and Violent Behavior. 2019;45:111–133.

- Sood S, Kostizak K, Mertz N, Stevens S, Rodrigues F, Hauer M. What works to address violence against children (VAC) in and around schools. Trauma, Violence, & Abuse. 2021:1–13.
- Cantone E, Piras AP, Vellante M, Preti A,
 Danielsdóttir S, D'Aloja E et al. Interventions on
 bullying and cyberbullying in schools: a systematic
 review. Clinical practice and Epidemiology in
 Mental Health. 2015;11(Suppl 1 M4):58.
- Burrus B, Leeks KD, Sipe TA, Dolina S, Soler R, Elder R et al. Person-to-person interventions targeted to parents and other caregivers to improve adolescent health: a community guide systematic review. American Journal of Preventive Medicine. 2012;42(3):316-326.
- 13. Gubbels J, van der Put CE, Stams G-JJ, Assink M. Effective components of school-based prevention programs for child abuse: a meta-analytic review. Clinical Child and Family Psychology Review. 2021;24(3):553–578.
- 14. Boustani MM, Frazier SL, Becker KD, Bechor M, Dinizulu SM, Hedemann ER et al. Common elements of adolescent prevention programs: minimizing burden while maximizing reach. Administration and Policy in Mental Health and Mental Health Services Research. 2015;42(2):209–219.
- Lawson GM, McKenzie ME, Becker KD, Selby L, Hoover SA. The core components of evidencebased social emotional learning programs. Prevention Science. 2019;20(4):457–467.
- Hutson E, Kelly S, Militello LK. Systematic review of cyberbullying interventions for youth and parents with implications for evidence-based practice. Worldviews on Evidence-Based Nursing. 2018;15(1):72–79.
- 17. Beelmann A, Heinemann KS. Preventing prejudice and improving intergroup attitudes: a meta-analysis of child and adolescent training programs. Journal of Applied Developmental Psychology. 2014;35(1):10–24.
- 18. Pandey A, Hale D, Das S, Goddings A-L, Blakemore S-J, Viner RM. Effectiveness of universal self-regulation-based interventions in children and adolescents: a systematic review and meta-analysis. JAMA pediatrics. 2018;172(6):566–575.

- 19. Skeen S, Laurenzi CA, Gordon SL, du Toit S, Tomlinson M, Dua T et al. Adolescent mental health program components and behavior risk reduction: a meta-analysis. Pediatrics. 2019;144(2):e20183488.
- Evangelio C, Rodriguez-Gonzalez P, Fernandez-Rio J, Gonzalez-Villora S. Cyberbullying in elementary and middle school students: a systematic review. Computers & Education. 2022;176:104356.
- 21. Garrard WM, Lipsey MW. Conflict resolution education and antisocial behavior in US schools: a meta-analysis. Conflict Resolution Quarterly. 2007;25(1):9–38.
- 22. Xu Z, Huang F, Koesters M, Staiger T, Becker T, Thornicroft G, et al. Effectiveness of interventions to promote help-seeking for mental health problems: systematic review and meta-analysis. Psychological Medicine. 2018;48(16):2658–2667.
- 23. Aguirre Velasco A, Cruz ISS, Billings J, Jimenez M, Rowe S. What are the barriers, facilitators and interventions targeting help-seeking behaviours for common mental health problems in adolescents? A systematic review. BMC Psychiatry. 2020;20(1):1–22.
- 24. Polanin JR, Espelage DL, Pigott TD. A meta-analysis of school-based bullying prevention programs' effects on bystander intervention behavior. School Psychology Review. 2012;41(1):47–65.
- Kettrey HH, Marx RA. Effects of bystander sexual assault prevention programs on promoting intervention skills and combatting the bystander effect: a systematic review and metaanalysis. Journal of Experimental Criminology. 2021;17(3):343-367.
- 26. Rhodes N, Shulman HC, McClaran N. Changing norms: a meta-analytic integration of research on social norms appeals. Human Communication Research. 2020;46(2-3):161–191.
- 27. Goldfarb ES, Lieberman LD. Three decades of research: the case for comprehensive sex education. Journal of Adolescent Health. 2021;68(1):13–27.
- 28. Rivera AIV, Mondragón-Sánchez EJ, Vasconcelos FKA, Pinheiro PNdC, Ferreira AGN, Galvão MTG. Actions to prevent sexual violence against adolescents: an integrative literature review. Revista Brasileira de Enfermagem [Brazilian Journal of Nursing]. 2021;74(suppl 4):e20190876.
- 29. Fonner VA, Armstrong KS, Kennedy CE, O'Reilly KR, Sweat MD. School based sex education and HIV prevention in low-and middle-income countries: a systematic review and meta-analysis. PloS one. 2014;9(3):e89692.
- 30. Global status report on violence prevention. Geneva: World Health Organization; 2014.

- 31. Davidson J, Aiken M, Gekoski A, Phillips K,
 Farr R. Research on protection of minors:
 a literature review and interconnected
 frameworks. Implications for VSP regulation
 and beyond (https://www.researchgate.
 net/publication/350358831 Research on
 Protection of Minors A Literature Review
 and Interconnected Frameworks Implications
 for VSP Regulation and Beyond, accessed 12
 October 2022).
- 32. Fernando N, Hakeem MAM, Seneviratne W, De Silva M, Cooray J. Online violence against children in urban and semi-urban settlements in Sri Lanka: a research on incidence, nature and scope. Save the Children (Sri Lanka) and World Vision Lanka. 2021.
- 33. Madigan S, Villani V, Azzopardi C, Laut D, Smith T, Temple JR et al. The prevalence of unwanted online sexual exposure and solicitation among youth: a meta-analysis. Journal of Adolescent Health. 2018;63(2):133–141.
- 34. Finkelhor D, Turner H, Colburn D. Online sexual offenses against children: types and national prevalence. JAMA Open Network. 2022.
- 2021 CyberTipline Reports by Electronic Service Providers (ESP). Alexandria, VA: National Center for Missing and Exploited Children; 2022 (https:// www.missingkids.org/content/dam/missingkids/ pdfs/2021-reports-by-esp.pdf, accessed 4 October 2022).
- Madigan S, Ly A, Rash CL, Van Ouytsel J, Temple JR. Prevalence of multiple forms of sexting behavior among youth: a systematic review and metaanalysis. JAMA Pediatrics. 2018;172(4):327–335.
- 37. Patchin JW, Hinduja S. Sextortion Among adolescents: results from a national survey of U.S. youth. Sexual Abuse. 2020;32(1):30–54.
- 38. Modecki KL, Minchin J, Harbaugh AG, Guerra NG, Runions KC. Bullying prevalence across contexts: a meta-analysis measuring cyber and traditional bullying. Journal of Adolescent Health. 2014;55(5):602–611.
- 39. Smith SG, Basile KC, Kresnow M-J. The national intimate partner and sexual violence survey: 2016/2017 report on stalking update release. Atlanta, GA: Centers for Disease Control and Prevention; 2022.
- Smahel D, Machackova H, Mascheroni G, Dedkova L, Staksrud E, Ólafsson K et al. EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. 2020.
- 41. Greijer S, Doek J. Interagency Working Group on Sexual Exploitation of Children. Terminology guidelines for the protection of children from sexual exploitation and abuse. Luxembourg City, Luxembourg: ECPAT International; 2016.

- 42. May-Chahal C, Palmer A, Doods S, Milan S. Rapid evidence assessment: characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation. Lancaster University: Independent Inquiry into Child Sexual Abuse; 2018.
- 43. ECPAT, INTERPOL, UNICEF. Disrupting Harm in Ethiopia: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence against Children; 2022.
- 44. ECPAT, INTERPOL, UNICEF. Disrupting harm in Thailand: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence against Children; 2022.
- 45. ECPAT, INTERPOL, UNICEF. Disrupting Harm in Tanzania: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence against Children; 2022.
- 46. ECPAT, INTERPOL, UNICEF. Disrupting Harm in Uganda: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence against Children; 2021.
- 47. ECPAT, INTERPOL, UNICEF. Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence against Children; 2021.
- 48. Wolak J, Finkelhor D, Mitchell KJ, Ybarra M. Online 'predators' and their victims: myths, realities, and implications for prevention and treatment. American Psychologist. 2008;63(2):111–128.
- 49. Mitchell KJ, Finkelhor D, Wolak J. The Internet and family and acquaintance sexual abuse. Child Maltreatment. 2005;10(1):49–60.
- 50. Ibrahim D. Online child sexual exploitation and abuse in Canada: a statistical profile of police-reported incidents and court charges, 2014 to 2020. Juristat: Canadian Centre for Justice Statistics; 2022:1–36.
- 51. Wolak J, Finkelhor D. Are crimes by online predators different from crimes by sex offenders who know youth in-person? Journal of Adolescent Health. 2013;53(6):736–741.
- 52. Bergen E, Davidson J, Schulz A, Schuhmann P, Johansson A, Santtila P et al. The effects of using identity deception and suggesting secrecy on the outcomes of adult-adult and adult-child or adult-adolescent online sexual interactions. Victims & Offenders. 2014;9(3):276–298.
- 53. De Santisteban P, Gámez-Guadix M. Prevalence and risk factors among minors for online sexual solicitations and interactions with adults. The Journal of Sex Research. 2018;55(7):939–950.
- 54. Ringenberg TR, Seigfried-Spellar KC, Rayz JM, Rogers MK. A scoping review of child grooming strategies: pre-and post-internet. Child Abuse & Neglect. 2022;123:105392.

- 55. Wolak J, Finkelhor D, Mitchell KJ. Trends in law enforcement responses to technology-facilitated child sexual exploitation crimes: The Third National Juvenile Online Victimization Study (NJOV-3). Durham, NH: Crimes against Children Research Center; 2012.
- 56. Seto MC. Internet sex offenders. Washington, DC: American Psychological Association; 2013.
- 57. Mitchell KJ, Jones L, Finkelhor D, Wolak J. Trends in unwanted online experiences and sexting [Final report]. Washington, DC: OJJDP Juvenile Justice Bulletin; 2014.
- Sklenarova H, Schulz A, Schuhmann P, Osterheider M, Neutze J. Online sexual solicitation by adults and peers – results from a population based German sample. Child Abuse & Neglect. 2018;76:225–236.
- 59. Broadhurst R. Child sex abuse images and exploitation materials. In: Leukfeldt R, Holt TJ, eds. Cybercrime: the human factor. London: Routledge; 2019.
- 60. Varrella A. Live streaming of child sexual abuse: background, legislative frameworks and the experience of the Philippines. ECPAT International Journal. 2017;12:47.
- 61. De La Salle University Social Development and Research Center, Department of Social Welfre and Development, Inter-Agency Council Against Child Pornography. National study on online sexual abuse and exploitation of children in the Philippines: a qualitative study with key findings and recommendations on how to protect children and address OSAEC in the Philippines. Mandaluyong City, Phillippines; UNICEF Philippines: 2021.
- 62. What is live-streamed abuse? Educational Articles [website]. Amsterdam: INHOPE Association (https://inhope.org/EN/articles/what-is-live-streamed-abuse?locale=en, accessed 18 October 2022).
- 63. The NETCLEAN Report. Live-streamed child sexual abuse, storage of child sexual abuse material, and emerging technologies challenges and opportunities. Law Enforcement Survey. Göteborg, Sweden: NETCLEAN; 2019.
- 64. Ojeda M, Del Rey R. Lines of action for sexting prevention and intervention: a systematic review. Archives of Sexual Behavior. 2022;51:1659–1687.
- 65. Doyle C, Douglas E, O'Reilly G. The outcomes of sexting for children and adolescents: a systematic review of the literature. Journal of Adolescence. 2021;92:86–113.
- 66. Wolak J, Finkelhor D. Sexting: a typology. Durham, NH: Crimes against Children Research Center University of New Hampshire; 2011.
- 67. Wolak J, Finkelhor D, Walsh W, Treitman L. Sextortion of minors: Characteristics and dynamics. Journal of Adolescent Health. 2018;62(1):72–79.

- 68. Mori C, Park J, Temple JR, Madigan S. Are youth sexting rates still on the rise? A meta-analytic update. Journal of Adolescent Health. 2022;70(4):531–539.
- 69. Barroso R, Ramião E, Figueiredo P, Araújo AM. Abusive sexting in adolescence: prevalence and characteristics of abusers and victims. Frontiers in Psychology. 2021;12:1–9.
- 70. Patchin JW, Hinduja S. Sextortion among adolescents: results from a national survey of US youth. Sexual Abuse. 2018;32(1):1–25.
- 71. Woodward VH, Evans M, Brooks M. Social and psychological factors of rural youth sexting: an examination of gender-specific models. Deviant Behavior. 2017;38(4):461–476.
- Drouin M, Ross J, Tobin E. Sexting: a new, digital vehicle for intimate partner aggression? Computers in Human Behavior. 2015;50:197–204.
- 73. Kwan I, Dickson K, Richardson M, MacDowall W, Burchett H, Stansfield C et al. Cyberbullying and children and young people's mental health: a systematic map of systematic reviews. Cyberpsychology, Behaviour and Social Networking. 2020;23(2):72–82.
- 74. Pyżalski J. From cyberbullying to electronic aggression: typology of the phenomenon. emotional and Behavioural Difficulties. 2012;17 (3–4):305–317.
- 75. Calvete E, Orue I, Estévez A, Villardón L, Padilla P. Cyberbullying in adolescents: modalities and aggressors' profile. Computers in Human Behavior. 2010;26(5):1128–1135.
- Rivers I, Noret N. Findings from a five-year study of text and email bullying. British Educational Research Journal. 2010;36(4):643–671.
- 77. Ehman AC, Gross AM. Sexual cyberbullying: review, critique and future directions. Aggression and Violent Behavior. 2018;44:80–87.
- 78. Henry J. Bias-based cyberbullying: the next hate crime frontier? Criminal Law Bulletin. 2013;49(3):481–503.
- Ending school bullying: focus on the Arab States: UNESCO's contribution to the policy dialogue on bullying and learning organized by the Regional Center for Educational Planning United Arab Emirates. Paris: UNESCO; 2019 (https://unesdoc. unesco.org/ark:/48223/pf0000369497?locale=en, accessed 4 October 2022).
- Behind the numbers: ending school violence and bullying. Paris: UNESCO; 2019 (https://unesdoc. unesco.org/ark:/48223/pf0000366483, accessed 4 October 2022).
- 81. Stonard KE, Bowen E, Lawrence TR, Price SA. The relevance of technology to the nature, prevalence and impact of adolescent dating violence and abuse: a research synthesis. Aggression and Violent Behavior. 2014;19(4):390–417.

- Sorrentino A, Baldry AC, Farrington DP, Blaya C. Epidemiology of cyberbullying across Europe: differences between countries and genders. Educational Sciences: Theory and Practice. 2019;19(2):74–91.
- 83. Mitchell KJ, Jones LM, Turner HA, Shattuck A, Wolak J. The role of technology in peer harassment: does it amplify harm for youth? Psychology of Violence. 2016;6(2):193–204.
- 84. Tokunaga RS. Following you home from school: a critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior. 2010;26(3):277–287.
- 85. Sabella RA, Patchin JW, Hinduja S. Cyberbullying myths and realities. Computers in Human behavior. 2013;29(6):2703–2711.
- 86. Waasdorp TE, Bradshaw CP. The overlap between cyberbullying and traditional bullying. Journal of Adolescent Health. 2015;56(5):483–488.
- 87. Zweig JM, Dank M, Lachman P, Yahner J. Technology, teen dating violence and abuse, and bullying. Final Report. Washington, DC: Urban Institue, Justice Policy Center; 2013.
- 88. Mitchell KJ, Jones LM, Turner H, Blachman-Demner D, Kracke K. The Role of technology in youth harassment victimization. Justice Research, Journal of the National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention. 2016:1–12.
- 89. Machimbarrena JM, Calvete E, Fernández-González L, Álvarez-Bardón A, Álvarez-Fernández L, González-Cabrera J. Internet risks: an overview of victimization in cyberbullying, cyber dating abuse, sexting, online grooming and problematic internet use. International Journal of Environmental Research and Public Health. 2018;15(11):2471.
- 90. Marciano L, Schulz PJ, Camerini A-L. Cyberbullying perpetration and victimization in youth: a meta-analysis of longitudinal studies. Journal of Computer-Mediated Communication. 2020;25(2):163–181.
- 91. Espelage DL, Low SK, Anderson C, De La Rue L. Bullying, sexual, and dating violence from early to late adolescence. Methodology. 2014;9:1–73.
- 92. Zych I, Viejo C, Vila E, Farrington DP. School bullying and dating violence in adolescents: a systematic review and meta-analysis. Trauma, Violence and Abuse. 2021;22(2):397–412.
- 93. Davidson J, Livingstone S, Jenkins S, Gekoski A, Choak C, Ike T et al. Adult online hate, harassment and abuse: a rapid evidence assessment. London: UK Council for Internet Safety; 2019.
- 94. Sheridan LP, Grant T. Is cyberstalking different? Psychology, Crime and Law. 2007;13(6):627–640.
- 95. Walsh W, Finkelhor D, Turner H. Characteristics and dynamics of cyberstalking among adolescents and young adults. 2022 [forthcoming].

- Collier K. Hackers are leaking children's data and there's little parents can do. NBC News. 21 September 2021.
- 97. Holt TJ, Navarro JN, Clevenger S. Exploring the moderating role of gender in juvenile hacking behaviors. Crime & Delinquency. 2020;66(11):1533–1555.
- 98. Quayyum F, Cruzes DS, Jaccheri L. Cybersecurity awareness for children: a systematic literature review. International Journal of Child-Computer Interaction. 2021;30:100343.
- 99. Zhang-Kennedy L, Chiasson S. A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys (CSUR). 2021;54(1):1–39.
- 100. Lenhart A, Ybarra M, Zickuhr K, Price-Feeney M. Online harassment, digital abuse, and cyberstalking in America. New York: Data and Society Research Institute; 2016.
- 101. Pascual A, Marchini K. 2018 Child identity fraud study. Javelin Strategy & Research. 2018.
- 102. Kardefelt-Winther D, Maternowska C. Addressing violence against children online and offline. Nature Human Behaviour. 2020;4(3):227–230.
- 103. Jessor R, Jessor S. Problem behavior theory and adolescent health (Vol 2). New York: Springer; 2017.
- 104. Baumgartner SE, Sumter SR, Peter J, Valkenburg PM. Identifying teens at risk: developmental pathways of online and offline sexual risk behavior. Pediatrics (English Edition). 2012;130(6):e1489.
- 105. Finkelhor D, Ormrod RK, Turner HA. Polyvictimization: a neglected component in child victimization. Child Abuse & Neglect. 2007;31(1):7–26.
- 106. Zych I, Farrington DP, Llorent VJ, Ribeaud D, Eisner MP. Childhood risk and protective factors as predictors of adolescent bullying roles. International Journal of Bullying Prevention. 2021;3(2):138–146.
- 107. Farrington DP, Gaffney H, Lösel F, Ttofi MM.
 Systematic reviews of the effectiveness of
 developmental prevention programs in reducing
 delinquency, aggression, and bullying. Aggression
 and Violent Behavior. 2017;33:91–106.
- 108. Joseph HL, Kuperminc GP. Bridging the siloed fields to address shared risk for violence: building an integrated intervention model to prevent bullying and teen dating violence. Aggression and Violent Behavior. 2020;55:1–12.
- 109. (44) INSPIRE: seven strategies for ending violence against children. Geneva: World Health Organization; 2016.
- 110. Implementing the global strategic response to eliminate child sexual exploitation and abuse. WeProtect Global Alliance; 2021 (https://www. weprotect.org/library/guidance-for-implementing-the-global-strategic-response/, accessed 18 October 2022).

- 111. Fighting child sexual abuse: Commission proposes new rules to protect children. Brussels: European Commission; 2022 (https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2976, accessed 4 October 2022).
- 112. Letourneau EJ, Harris AJ, Shields RT, Walfield SM, Ruzicka AE, Buckman C et al. Effects of juvenile sex offender registration on adolescent well-being: an empirical examination. Psychology, Public Policy, and Law. 2018;24(1):105.
- 113. Harris AJ, Walfield SM, Shields RT, Letourneau EJ. Collateral consequences of juvenile sex offender registration and notification: Results from a survey of treatment providers. Sexual Abuse. 2016;28(8):770–790.
- 114. Bayliss B. The kids are alright: Teen sexting, child pornography charges, and the criminalization of adolescent sexuality. University of Colorado Law Review. 2020;91:251.
- 115. Bulger M, Burton P, O'Neill B, Staksrud E. Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online. New Media & Society. 2017;19(5):750–764.
- 116. Global threat assessment 2021. In: Working togehter to end the sexual abuse of children online. WeProtect Global Alliance; 2022 (https://www.weprotect.org/global-threat-assessment-21/#report, accessed 18 October 2022).
- 117. Braga AA, Weisburd D, Turchan B. Focused deterrence strategies effects on crime: a systematic review. Campbell Systematic Reviews. 2019;15(3).
- 118. Braga AA, Weisburd D, Turchan B. Focused deterrence strategies and crime control: an updated systematic review and meta-analysis of the empirical evidence. Criminology & Public Policy. 2018;17(1):205–250.
- 119. Trang S, Brendel B. A meta-analysis of deterrence theory in information security policy compliance research. Information Systems Frontiers. 2019;21(6):1265–1284.
- 120. Roeder OK, Eisen L-B, Bowling J, Stiglitz JE, Chettiar IM. What caused the crime decline? Columbia Business School Research Paper. 2015;15–28.
- 121. Piza EL, Welsh BC, Farrington DP, Thomas AL. CCTV surveillance for crime prevention. Criminology & Public Policy. 2019;18(1):135–159.
- 122. Guerette RT, Bowers KJ. Assessing the extent of crime displacement and diffusion of benefits: a review of situational crime prevention evaluations. Criminology. 2009;47(4):1331–1368.
- 123. Sherman LW. Policing domestic violence 1967–2017. Criminology & Public Policy. 2018;17(2):453–465.

- 124. Gottfredson DC, Crosse S, Tang Z, et al. Effects of school resource officers on school crime and responses to school crime. Criminology & Public Policy. 2020;19(3):905–940.
- 125. Ojanen T. Terrorist profiling: human rights concerns. Critical Studies on Terrorism. 2010;3(2):295–312.
- 126. Blair G, Weinstein JM, Christia F, Arias E, Badran E, Blair RA et al. Community policing does not build citizen trust in police or reduce crime in the Global South. Science. 2021;374(6571).
- 127. Bennett T, Holloway K, Farrington DP. Does neighborhood watch reduce crime? A systematic review and meta-analysis. Journal of Experimental Criminology. 2006;2(4):437–458.
- 128. Allara E, Ferri M, Bo A, Gasparrini A, Faggiano F. Are mass-media campaigns effective in preventing drug use? A Cochrane systematic review and meta-analysis. BMJ Open. 2015;5(9):e007449.
- 129. Find your local child helpline [website].
 Amsterdam: Child Helpline International (https://childhelplineinternational.org/helplines/, accessed 18 October 2022).
- 130. Fighting CSAM: a safe childhood. Amsterdam: INHOPE Association (https://www.inhope.org/EN?locale=en, accessed 18 October 2022).
- 131. Hoffberg AS, Stearns-Yoder KA, Brenner LA. The effectiveness of crisis line services: a systematic review. Frontiers in Public Health. 2020;7:1–14.
- 132. Lester D. Evidence-based suicide prevention by helplines: a meta-analysis. In: Pompili M, Tatarelli R, eds. Evidence-based practice in suicidology: a source book. Göttingen, Germany: Hogrefe Publishing; 2011:139–151.
- 133. Mathieu SL, Uddin R, Brady M, Batchelor S, Ross V, Spence SH et al. Systematic review: The state of research into youth helplines. Journal of the American Academy of Child & Adolescent Psychiatry. 2021;60(10):1190–1233.
- 134. Fighting child sexual abuse online [online toolkit]. California: Google; 2022 (https://protectingchildren.google/intl/en/#introduction, accessed 18 October 2022).
- 135. Lorenzo-Dus N, Kinzel A, Di Cristofaro M.
 The communicative modus operandi of online child sexual groomers: recurring patterns in their language use. Journal of Pragmatics. 2020;155:15–27.
- 136. Report on trends in online crime and their potential implications in the fight against commercial child pornography. Financial Coalition Against Child Pornography; 2011. (https://www.icmec.org/wpcontent/uploads/2015/10/Trends-in-Online-Crime-Feb.-2011.pdf, accessed 18 October 2022).

- 137. Prichard J, Scanlan J, Watters P, Wortley R, Hunn C, Garrett E. Online messages to reduce users' engagement with child sexual abuse material: a review of relevant literature for the reThink chatbot. Tasmania: The Lucy Faithfull Foundation, University of Tasmania; 2022.
- 138. Prichard J, Wortley R, Watters PA, Spiranovic C, Hunn C, Krone T. Effects of automated messages on internet users attempting to access "barely legal" pornography. Sexual Abuse. 2022;34(1):106–124.
- 139. Prichard J, Scanlan J, Krone T, Spiranovic C, Watters P, Wortley R. Warning messages to prevent illegal sharing of sexual images: results of a randomised controlled experiment. Trends & Issues In Crime and Criminal Justice. 2022;647:1–15.
- 140. Martijn C, Smeets E, Jansen A, Hoeymans N, Schoemaker C. Don't get the message: the effect of a warning text before visiting a proanorexia website. International Journal of Eating Disorders. 2009;42(2):139–145.
- 141. Caillon J, Grall-Bronnec M, Saillard A, Leboucher J, Péré M, Challet-Bouju G. Impact of warning popup messages on the gambling behavior, craving, and cognitions of online gamblers: a randomized controlled trial. Frontiers in Psychiatry. 2021;12:1–11.
- 142. Testa A, Maimon D, Sobesto B, Cukier M.
 Illegal roaming and file manipulation on target
 computers: assessing the effect of sanction
 threats on system trespassers' online behaviors.
 Criminology & Public Policy. 2017;16(3):689–726.
- 143. (36) Harvey L, Cassidy S, Brennan M. A systematic review of strategies to prevent online child sexual exploitation and abuse perpetration. London:

 National Institute for Health Research; 2022

 (https://www.crd.york.ac.uk/prospero/display_record.php?ID=CRD42022303545, accessed 18

 October 2022).
- 144. Beier KM. Preventing child sexual abuse the prevention project Dunkelfeld. Journal of Sexual Medicine. 2018;15(8):1065–1066.
- 145. Silovsky JF, Hunter MD, Taylor EK. Impact of early intervention for youth with problematic sexual behaviors and their caregivers. Journal of Sexual Aggression. 2019;25(1):4–15.
- 146. Tanner-Smith EE, Durlak JA, Marx RA. Empirically based mean effect size distributions for universal prevention programs targeting school-aged youth: a review of meta-analyses. Prevention Science. 2018;19(8):1091–1101.
- 147. Vaivada T, Sharma N, Das JK, Salam RA, Lassi ZS, Bhutta ZA. Interventions for health and well-being in school-aged children and adolescents: a way forward. Pediatrics. 2022;149(6).

- 148. Juras R, Kelsey M, Lipsey M, Steinka-Fry K, Layzer J, Farb A et al. Meta-analysis of federally funded teen pregnancy prevention programs. The Assistant Secretary for Planning and Evaluation, Administration for Children and Families. Office of Population Affairs, Office of US Department of Health and Human Services; 2019.
- 149. Johnson BT, Scott-Sheldon LA, Huedo-Medina TB, Carey MP. Interventions to reduce sexual risk for human immunodeficiency virus in adolescents: a meta-analysis of trials, 1985–2008. Archives of Pediatrics & Adolescent Medicine. 2011;165(1):77–84.
- 150. Mavedzenge SN, Luecke E, Ross DA. Effective approaches for programming to reduce adolescent vulnerability to HIV infection, HIV risk, and HIV-related morbidity and mortality: a systematic review of systematic reviews. Journal of Acquired Immune Deficiency Syndromes. 2014;66:S154–S169.
- 151. Tobler NS, Roona MR, Ochshorn P, Marshall DG, Streke AV, Stackpole KM. School-based adolescent drug prevention programs: 1998 meta-analysis. Journal of Primary Prevention. 2000;20(4):275–336.
- 152. Gaffney H, Farrington DP, Ttofi MM. Examining the effectiveness of school-bullying intervention programs globally: a meta-analysis. International Journal of Bullying Prevention. 2019;14–31.
- 153. De La Rue L, Polanin JR, Espelage DL, Pigott TD. A meta-analysis of school-based interventions aimed to prevent or reduce violence in teen dating relationships. Review of Educational Research. 2017;87(1):7–34.
- 154. Ligiero D, Hart C, Fulu E, Thomas AL, Radford L. What works to prevent sexual violence against children: Executive Summary. Washington, DC: Together for Girls; 2019.
- 155. Fraguas D, Díaz-Caneja CM, Ayora M, Durán-Cutilla M, Abregú-Crespo R, Ezquiaga-Bravo I et al. Assessment of school anti-bullying interventions: a meta-analysis of randomized clinical trials. JAMA Pediatrics. 2021;175(1):44–55.
- 156. Mikton C, Butchart A. Child maltreatment prevention: a systematic review of reviews. Bulletin of the World Health Organization. 2009;87(5):353–361.
- 157. Bo A, Hai AH, Jaccard J. Parent-based interventions on adolescent alcohol use outcomes: a systematic review and meta-analysis. Drug and Alcohol Dependence. 2018;191:98–109.
- 158. Widman L, Evans R, Javidi H, Choukas-Bradley S. Assessment of parent-based interventions for adolescent sexual health: a systematic review and meta-analysis. JAMA Pediatrics. 2019;173(9):866–877.
- 159. Spencer CM, Topham GL, King EL. Do online parenting programs create change?: A meta-analysis. Journal of Family Psychology. 2020;34(3):364–374.

- 160. Rudolph J, Zimmer-Gembeck MJ, Shanley DC, Hawkins R. Child sexual abuse prevention opportunities: parenting, programs, and the reduction of risk. Child Maltreatment. 2018;23(1):96–106.
- 161. Shipe SL, Guastaferro K, Noll JG, Connell CM, Morgan PL, Crowley DM. Taking a school-based child sexual abuse prevention program to scale: a cost analysis. Prevention Science. 2022.
- 162. To prevent and to protect: report of the task force of the Catholic Medical Association on the sexual abuse of children and prevention. Wynewood, PA: Catholic Medical Association Task Force; 2006.
- 163. Ricardo C, Eads M, Barker G. Engaging boys and young men in the prevention of sexual violence: a systematic and global review of evaluated interventions. In: Sexual violence research initiative. Washington, DC; 2011.
- 164. Xue J, Hu R, Zhang W, Zhao Y, Zhang B, Liu N et al. Virtual reality or augmented reality as a tool for studying bystander behaviors in interpersonal violence: Scoping review. Journal of Medical Internet Research. 2021;23(2):e25322.
- 165. DeSmet A, Shegog R, Van Ryckeghem D, Crombez G, De Bourdeaudhuij I. A systematic review and meta-analysis of interventions for sexual health promotion involving serious digital games. Games for Health Journal. 2015;4(2):78–90.
- 166. Williford A, Elledge LC, Boulton AJ, DePaolis KJ, Little TD, Salmivalli C. Effects of the KiVa antibullying program on cyberbullying and cybervictimization frequency among Finnish youth. Journal of Clinical Child & Adolescent Psychology. 2013;42(6):820–833.
- 167. DeGue S, Valle LA, Holt MK, Massetti GM, Matjasko JL, Tharp AT. A systematic review of primary prevention strategies for sexual violence perpetration. Aggression and Violent Behavior. 2014;19(4):346–362.
- 168. Ng ED, Chua JYX, Shorey S. The effectiveness of educational interventions on traditional bullying and cyberbullying among adolescents: a systematic review and meta-analysis. Trauma, Violence, & Abuse. 2022;23(1):132–151.
- 169. Beelmann A, Lösel F. A comprehensive metaanalysis of randomized evaluations of the effect of child social skills training on antisocial development. Journal of Developmental and Life-Course Criminology. 2021;7(1):41–65.
- 170. Teding van Berkhout E, Malouff JM. The efficacy of empathy training: a meta-analysis of randomized controlled trials. Journal of Counseling Psychology. 2016;63(1):32.
- 171. Salmivalli C, Laninga-Wijnen L, Malamut ST, Garandeau CF. Bullying prevention in adolescence: solutions and new challenges from the past decade. Journal of Research on Adolescence. 2021;31(4):1023–1046.

- 172. Torgal C, Espelage DL, Polanin JR, Ingram KM, Robinson LE, El Sheikh AJ et al. A meta-analysis of school-based cyberbullying prevention programs' impact on cyber-bystander behavior. School Psychology Review. 2021:1–15.
- 173. Ojeda M, Del Rey R. Lines of action for sexting prevention and intervention: a systematic review. Archives of Sexual Behavior. 2021;51:1659–1687.
- 174. Chen Q, Chan KL, Guo S, Chen M, Lo CK-M, Ip P. Effectiveness of digital health interventions in reducing bullying and cyberbullying: a meta-analysis. Trauma, Violence, & Abuse. 2022;0(0):1–7.
- 175. Peters G-JY, Ruiter RA, Kok G. Threatening communication: a critical re-analysis and a revised meta-analytic test of fear appeal theory. Health Psychology Review. 2013;7(sup1):S8–S31.
- 176. Tannenbaum MB, Hepler J, Zimmerman RS, Saul L, Jacobs S, Wilson K et al. Appealing to fear: a meta-analysis of fear appeal effectiveness and theories. Psychological Bulletin. 2015;141(6):1178–1204.
- 177. Sun WH, Miu HYH, Wong CKH, Tucker JD, Wong WCW. Assessing participation and effectiveness of the peer-led approach in youth sexual health education: systematic review and meta-analysis in more developed countries. The Journal of Sex Research. 2018;55(1):31–44.
- 178. Nocentini A, Zambuto V, Menesini E. Anti-bullying programs and information and communication technologies (ICTs): a systematic review.

 Aggression and Violent Behavior. 2015;23:52-60.
- 179. Olweus D, Limber SP, Breivik K. Addressing specific forms of bullying: a large-scale evaluation of the olweus bullying prevention program. International Journal of Bullying Prevention. 2019;1(1):70–84.
- 180. Espelage DL, Low S, Van Ryzin MJ, Polanin JR. Clinical trial of second step middle school program: impact on bullying, cyberbullying, homophobic teasing, and sexual harassment perpetration. School Psychology Review. 2015;44(4):464–479.
- 181. Garaigordobil M, Martínez-Valderrey V.
 Technological resources to prevent cyberbullying during adolescence: the Cyberprogram 2.0
 Program and the Cooperative Cybereduca 2.0
 Videogame. Frontiers in Psychology. 2018;9:745.
- 182. Garaigordobil M, Martínez-Valderrey V. The effectiveness of Cyberprogram 2.0 on conflict resolution strategies and self-esteem. Journal of Adolescent Health. 2015;57(2):229–234.
- 183. Menesini E, Nocentini A, Palladino BE, Frisen A, Berne S, Ortega-Ruiz R et al. Cyberbullying definition among adolescents: a comparison across six European countries. Cyberpsychology, Behavior, and Social Networking. 2012;15(9):455–463.
- 184. Lee M-S, Zi-Pei W, Svanström L, Dalal K. Cyber bullying prevention: intervention in Taiwan. PLOS ONE. 2013;8(5):e64031.

- 185. Foshee VA, McNaughton Reyes HL, Vivolo-Kantor AM, Basile KC, Chang L-Y, Faris R et al. Bullying as a longitudinal predictor of adolescent dating violence. Journal of Adolescent Health. 2014;55(3):439–444.
- 186. Foshee VA, McNaughton Reyes HL, Chen MS, Ennett ST, Basil KC, DeGue S et al. Shared risk factors for the perpetration of physical dating violence, bullying, and sexual harassment among adolescents exposed to domestic violence. Journal of Youth Adolescence. 2016;45(4):672–686.
- 187. Leemis RW, Espelage DL, Basile KC, Mercer Kollar LM, Davis JP. Traditional and cyber bullying and sexual harassment: a longitudinal assessment of risk and protective factors. Aggressive Behavior. 2019;45(2):181–192.
- 188. AlShabibi A, Al-Suqri M. Cybersecurity awareness and its impact on protecting children in cyberspace. Paper presented at the 22nd International Arab Conference on Information Technology (ACIT), 21–23 December 2021.
- 189. Ali S, Abou Haykal H, Youssef EYM. Child Sexual abuse and the internet—a systematic review. Human Arenas. 2021:1–18.
- 190. Patterson A, Ryckman L, Guerra C. A systematic review of the education and awareness interventions to prevent online child sexual abuse. Journal of Child & Adolescent Trauma. 2022:1–11.
- 191. Walsh K, Zwi K, Woolfenden S, Shlonsky A. Schoolbased education programs for the prevention of child sexual abuse: a Cochrane systematic review and meta-analysis. Research on Social Work Practice. 2018;28(1):33–55.
- 192. Schneider M, Hirsch JS. Comprehensive sexuality education as a primary prevention strategy for sexual violence perpetration. Trauma, Violence, & Abuse. 2020;21(3):439–455.
- 193. International technical guidance on sexuality education: an evidence-informed approach. Paris: UNESCO Publishing; 2018.
- 194. National sex eduation standards: Core content and skills, K-12. Second edition. Washington, DC: Future of Sex Education Initiative; 2020.
- 195. Kirby D, Obasi A, Laris B. The effectiveness of sex education and HIV education interventions in schools in developing countries. In: Preventing HIV/AIDS in young people. Geneva: World Health Organization; 2006 (WHO Technical Report Series, No. 938 (http://apps.who.int/iris/bitstream/handle/10665/43453/WHO_TRS_938_eng.pdf; jsessionid=104EEB844C9624CED58FF075338A0413?sequence=1, accessed 13 October 2022).
- 196. Schenker I. New challenges for school AIDS education within an evolving HIV pandemic. Prospects. 2001;31(3):415–434.
- 197. Lee C, Wong JS. Examining the effects of teen dating violence prevention programs: a systematic review and meta-analysis. Journal of Experimental Criminology. 2022;18(1):1–40.

- 198. Rothman EF, Daley N, Alder J. A pornography literacy program for adolescents. American Journal of Public Health. 2020;110(2):154–156.
- 199. Knack N, Holmes D, Fedoroff JP. Motivational pathways underlying the onset and maintenance of viewing child pornography on the Internet.

 Behavioral Sciences & the Law. 2020;38(2):100–116.
- 200. Horvath MA, Alys L, Massey K, Pina A, Scally M, Adler JR. Basically... porn is everywhere: a rapid evidence assessment on the effects that access and exposure to pornography has on children and young people [project report]. London: Office of the Children's Commissioner for England; 2013.
- 201. Rothman EF, Adhia A, Christensen TT, Paruk J, Alder J, Daley N. A pornography literacy class for youth: results of a feasibility and efficacy pilot study. American Journal of Sexuality Education. 2018;13(1):1–17.
- 202. Livingstone S, Kardefelt Winther D, Saeed M. Global Kids Online Comparative Report. Innocenti Research Report. Florence: UNICEF Office of Research; 2019.
- 203. Wolak J, Finkelhor D, Mitchell KJ. Trends in arrests of "online predators". Durham, NH: Crimes against Children Research Center, University of New Hampshire; 2009.
- 204. Milon-Flores DF, Cordeiro RLF. How to take advantage of behavioral features for the early detection of grooming in online conversations. Knowledge-Based Systems. 2022;240:108017.
- 205. Lorenzo-Dus N, Kinzel A. 'so is your mom as cute as you?': Examining patterns of language use by online sexual groomers. Journal of corpora and discourse studies. 2019;2:14–39.
- 206. FAQ: Common questions from teens [website]. Nevada, USA: Nevada Public Health Foundation; 2022 (https://www.nevadapublichealthfoundation. org/programs/statutory-rape-preventionprogram/faq/, accessed 13 October 2022).
- 207. Statutory rape prevention: what would you do? [website]. Virginia, USA: Virginia Department of Health; 2022 (https://www.vdh.virginia.gov/statutory-rape-prevention/what-can-you-do/, accessed 13 October 2022).
- 208. Döring N. Consensual sexting among adolescents: risk prevention through abstinence education or safer sexting? Cyberpsychology: Journal of Psychosocial Research on Cyberspace. 2014;8(1).
- 209. Patchin JW, Hinduja S. It is time to teach safe sexting. The Journal of Adolescent Health. 2020;66(2):140–143.
- 210. Sabbah-Mani J. Sexting education: an educational approach to solving the media fueled sexting dilemma. Southern California Interdisciplinary Law Journal. 2014;24:529.

- 211. Garis MG. The 7 golden rules for how to sext safely (and oh-so effectively), according to a sexologist. Sex Advice [website]. Well & Good: New York, NY: 2020 (https://www.wellandgood.com/how-to-sext-safely/, accessed 13 October 2022).
- 212. Ouytsel JV. Teenagers are going to sext, let's teach them to do it safely. Psyche. (https://psyche.co/ideas/teenagers-are-going-to-sext-lets-teach-them-to-do-it-safely, accessed 13 October 2022).
- 213. Foshee VA, Linder GF. The safe dates project: theoretical basis, evaluation design, and selected baseline findings. Youth Violence Prevention. 1996;12(5):39–47.
- 214. Simpson DM, Leonhardt ND, Hawkins AJ. Learning about love: a meta-analytic study of individually-oriented relationship education programs for adolescents and emerging adults. Journal of Youth and Adolescence. 2018;47(3):477–489.
- 215. Wolfe DA, Crooks C, Jaffe P, Chiodo D, Hughes R, Ellis W et al. A school-based program to prevent adolescent dating violence: a cluster randomized trial. Archives of Pediatrics and Adolescent Medicine. 2009;163(8):692–699.
- 216. Roberto AJ, Eden J, Savage MW, Ramos-Salazar L, Deiss DM. Outcome evaluation results of school-based cybersafety promotion and cyberbullying prevention intervention for middle school students. Health Communication. 2014;29(10):1029–1042.
- 217. ECPAT International, UNICEF Office of Research Innocenti. Children's disclosures of online sexual exploitation and abuse. disrupting harm data insight 2. Global Partnership to End Violence Against Children; 2022 (https://www.end-violence.org/sites/default/files/2022-05/DH-data-insight-2_FinalB%282%29.pdf, accessed 13 October 2022).
- 218. Reyns BW. A situational crime prevention approach to cyberstalking victimization: preventive tactics for Internet users and online place managers. Crime Prevention and Community Safety. 2010;12(2):99–118.
- 219. Smith SG, Chen J, Basile KC, Gilbert LK, Merrick MT, Patel N et al. The National Intimate Partner and Sexual Violence Survey (NISVS): 2010–2012 State Report. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention; 2017.
- 220. Ortega-Barón J, González-Cabrera J, Machimbarrena JM, Montiel I. Safety.Net: a pilot study on a multi-risk internet prevention program. International Journal of Environmental Research and Public Health. 2021;18(8):4249.
- 221. Know It, Name It, Stop It [website]. Stalking Prevention Awareness and Resource Center; 2017.

Annex 1: Methodology

This project aims to provide a user-friendly review and summary of the state of research on interventions to prevent and respond to online VAC. The review report was prepared with several considerations in mind, including that it:

- be based on the most up-do-date evidence from research and practice;
- provide specific examples of messages and programme elements most likely to succeed;
- be easily understood and readily accessible to non-academic audiences including programme developers, practitioners, educators, and advocates;
- · be international in its scope.

We consulted with an expert panel before beginning formal searches for the review to find out whether other online VAC domains should be added and to make sure we incorporated the wide variety of terminology used in relation to the topic.

A key challenge in reviewing and summarizing the state of research on online VAC domains is that many terms can be used to mean the same thing. For example, nonconsensual sexting can be called "image-based abuse", "aggravated sexting", "revenge porn", and "abusive dissemination of sexually explicit images on the Internet". Another challenge is that different online VAC domains have different amounts of literature. For example, cyberbullying has a large volume of literature, including many high-quality experimental studies and several high-quality systematic reviews and meta-analyses that summarize the findings of large bodies of evidence. In contrast, livestreaming of child sexual abuse has a very limited number of papers, and no prevention programme evaluations have been published so far. To deal with this variation and complexity, we used three complementary approaches that we called "streams".

- A best-practice review of the youth-focused prevention literature in related topic areas.
 We used a rapid "review of reviews" approach.
 We reviewed gold standard systematic reviews and meta-analyses on related forms of prevention programming with larger and more wellestablished literatures than online VAC. We did this to identify high-level principles of successful programmes. Related topic areas included:
 - sex education and sexual risk-taking;
 - · dating violence and healthy relationships;
 - bullying prevention;
 - delinquency prevention;
 - child sexual abuse prevention;
 - substance abuse prevention;
 - bystander mobilization;
 - suicide prevention and mental health promotion;
 - general reviews on what works in youth-based prevention programmes.
- 2. A rapid review of evaluations of online safety programmes for children and adolescents. At first, we focused on searching and summarizing findings of comprehensive reviews of formal evaluation studies on programme interventions aimed at preventing online VAC generally (i.e., finding existing syntheses of broad areas such as online safety, cybersecurity, and digital citizenship). We then focused on reviews of specific online VAC domains that had amassed sizable literature (e.g., cyberbullying, and child sexual exploitation and abuse). After that, we focused on single evaluations of prevention programmes for new and emerging online VAC domains (i.e., looking for evaluations in areas for which reviews did not yet exist, such as for teen sexting, cyberstalking, and livestreaming). We did this to make sure we could identify areas in which there was stronger and weaker evidence of effectiveness (or no evidence at all), and to pinpoint the programming components that seemed to account for success.



A desk review of online VAC programmes for children and adolescents. We focused on finding programmes addressing online VAC domains in as many countries as possible. We reviewed these programmes against a set of pre-determined criteria developed from our reviews in order to identify messages and methods being used or recommended to prevent online VAC generally, and online VAC domains specifically. We aimed to identify strengths (how programme features align with general principles of success) and to identify weaknesses (how and where programmes fail to address important online VAC characteristics; make assumptions that are not supported by the research; or fail to incorporate widely supported and wellestablished principles for effective prevention).

The following sections provide more detail on the specific methods used in each of these three streams.

1. Best-practice review of the youth-focused prevention literature

Using a broad "review of reviews" approach, multiple literature searches were conducted in Google Scholar to retrieve gold standard systematic reviews and metaanalyses of the child and youth-focused prevention literature to identify high level principles of successful interventions in domains related to online VAC. One of the authors (DF) ran a series of keyword searches of the literature between 23 March 2022 to 5 June 2022. Search strategies combined "meta-analysis" or "review" along with keywords related to topic areas including, but not limited to: sex education, sexual risk-taking, dating violence, bullying prevention, resilience, mindfulness and empathy promotion, conflict management, child sexual abuse prevention, bystander mobilization, and mental health. Because the three work streams were conducted in parallel, emerging themes from Stream 2 (in relation to programme components) and Stream 3 (in relation to programme messaging) could be incorporated into searches for Stream 1.The full search list, dates, and details can be found in Open Science Framework: https://osf.io/zpc6k/. Titles and abstracts of records retrieved from the Google Scholar searches were independently screened, selected, and summarized by one author (DF).

2. Rapid review of evaluations of online safety programmes for children and adolescents

This rapid review adhered to the Preferred Reporting Items Systematic Reviews. A review protocol was developed before undertaking the review. It can be found in Open Science Framework: https://osf.io/zpc6k/.

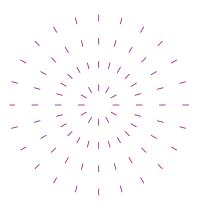
Eligibility criteria: The authors searched for reviews and evaluation studies that addressed four key questions:

- What studies have been conducted on interventions for specific online VAC topics?
- 2. Were the interventions effective?
- 3. What were the characteristics of the interventions?
- 4. Which programme characteristics (components, elements) and messages were associated with more successful prevention?

The authors included systematic reviews and metaanalyses, narrative reviews, randomized controlled trials, as well as quasi-experimental research. No date limiters were applied. Only publications in English, or in other languages that could be adequately translated into English using Google Translate, were included.

The target population consisted of children under the age of 18 years or parents of children under the age of 18. The settings included studies conducted in schools, youth-serving organizations, and online (within apps or online programmes, with specific Internet service providers or social media vendors).

Interventions were defined as educational or psycho-educational programmes designed to increase knowledge or skills, or change attitudes or behaviour, to prevent online VAC. These could be primary (universal) or secondary (targeted) prevention initiatives. Interventions were included only if the study measured online VAC outcomes such as awareness, knowledge, skills, self-efficacy, attitudes, behaviours, experiences, or harms in relation to online VAC domains such as cyberbullying, cyberharassment, sexual interactions in the online environment, sexting, receiving or creating sexual images, online interaction with adults, or security of private information.



Search strategy: Multiple databases were included in the search strategy including PubMed, PsycInfo, ERIC, CINAHL, Violence and Abuse Abstracts, and Engineering Village. Searches were conducted in three phases:

- Phase 1: Systematic reviews and meta-analyses of broader terms
- Phase 2: Systematic reviews and meta-analyses of more specific topics
- Phase 3: Randomized controlled trials and quasi-experimental research of more specific topics

Using a combination of keywords and relevant subject terms, the Health and Human Services Librarian (EO) conducted a three-pronged search of the literature between May 2022 and June 2022. When available, validated filters were applied to increase the accuracy of retrieving specific study methodologies. The authors did not search grey literature databases and search engines, but grey literature did appear in the database search results.

The first search included broader topic terms in addition to validated filters for systematic reviews and meta-analyses. The second search included more focused topic keywords and validated filters for systematic reviews and meta-analyses. The third search used a combination of some terms in search one and some from search two and included validated filters to yield randomized controlled trials and quasi-experimental studies. This three-pronged approach was taken due to time restrictions and to better manage the number of results to review. The full search strategies for each database can be found Open Science Framework: https://osf.io/zpc6k/.

Study selection and data extraction: Titles and abstracts of all records retrieved from searches were independently screened by one author (KW). Data extraction was conducted independently by a single reviewer and verified by another reviewer. As this was a rapid review, full risk-of-bias assessment was not conducted. Three broad quality criteria were extracted to assess: (i) whether violence against children online outcomes were measured; (ii) whether experimental and quasi-experimental studies formed the basis for findings; and (iii) whether a review or study protocol was reported. The data extraction templates can be found in Open Science Framework: https://osf.io/zpc6k/.

A total of 1013 systematic review and meta-analyses records were saved in the Covidence systematic review management tool from the first and second search combined. After removing duplicates, the remaining 793 records underwent title and abstract screening by one of the authors. Of those, 703 records did not meet the inclusion criteria, leaving 90 records for full-text screening. The PRISMA Flow Diagram for Reviews and Meta-analyses (see Fig. A1) illustrates the number of citations selected for inclusion and lists the reasons for exclusion after full-text screening and data extraction. The remaining 18 records were included for synthesis.

For the final search of primary studies, a total of 645 records were retrieved. In total, 187 duplicates were removed, leaving 458 records for title and abstract screening. Of these, 429 records did not meet inclusion criteria and 29 records underwent full-text screening. The second PRISMA Flow Diagram for Primary Studies shown in Fig. A2 illustrates the selection process of primary studies. A total of eight articles were included for synthesis.

3. Desk review of online VAC programmes for children and adolescents

A systematic review of websites about online Internet safety was conducted from May-July 2022 by inputting the search terms "online safety programme" and "Internet safety education" into the Google search engine. The search screening was limited to the first and second pages of results. After the initial search using broad keywords, additional targeted queries were conducted. These queries aimed to reduce the location bias of the search results in an attempt to source an international sample of programmes. Examples of the targeted search terms include "online safety programme in Asia" and "Internet safety education in Latin America". Further targeted searches were conducted to identify programmes in specific countries that did not appear in the previous searches. Examples of search terms for these narrow searches included "online safety programme in South Africa" and "Internet safety education in the Philippines".

Eligibility criteria: Internet safety programmes were included for review if they met the definition of a "well-developed programme". This definition comprised three criteria:

- 1. A multi-page website describing the programme and its components.
- Educational modules for children and youth for independent direct engagement or indirect engagement via educators who would be delivering the modules or information to children and youth.
- 3. Coverage of at least two or more online VAC topics.

Websites available in English, or that could be adequately translated into English using Google Translate, were included. To be included, websites were not required to be exclusively dedicated to online VAC topics but could also contain information about other Internet-related topics. Exclusion criteria included websites focused solely on one, or no, online VAC-related topics.

A total of 56 websites that qualified were reviewed and analysed. Each website was assessed using criteria developed from our review of the effectiveness literature in Stream 1 and Stream 2. These criteria included structural and content elements, the online VAC topics covered, generic skills taught, and how the programmes addressed the topics of online grooming and sexting. Each element was coded either yes or no. Programme online access mode was coded only (only online), not possible (only offline), or possible (mixture of both online and offline). The data extraction templates can be found in Open Science Framework: https://osf.io/zpc6k/.

Figure A1. PRISMA flow diagram for Stream 2 reviews identified via academic databases

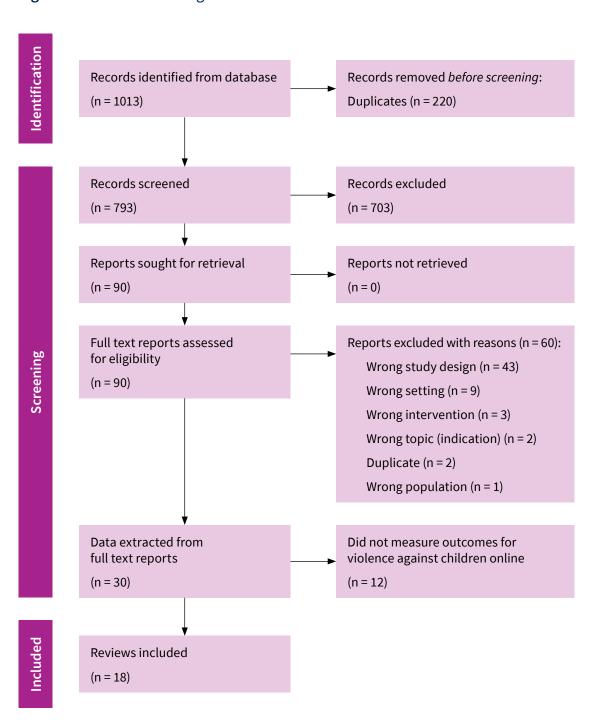
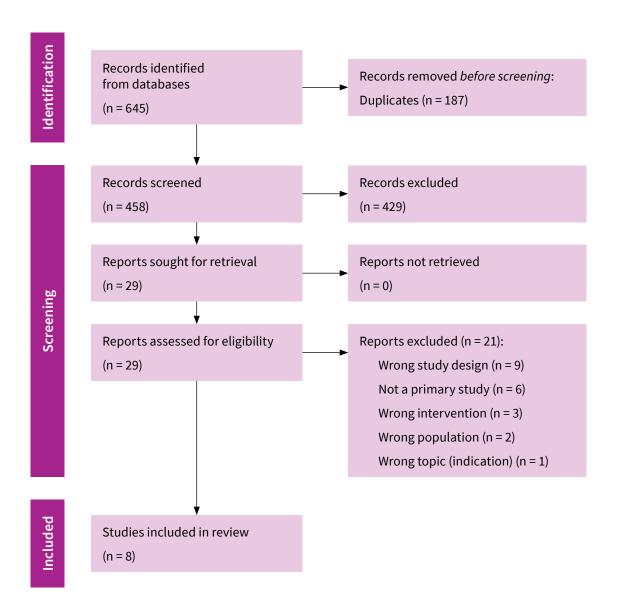


Figure A2. PRISMA flow diagram for Stream 2 evaluation studies identified via academic databases



20 Avenue Appia 1211 Geneva 27 Switzerland

Email: violenceprevention@who.int who.int/teams/social-determinants-of-health/violence-prevention

