Suojellaan Lapsia
Protect Children

Tech Platforms Used by Online Child Sexual Abuse Offenders

Research Report with Actionable Recommendations for the Tech Industry

Suojellaan Lapsia, Protect Children ry.

February 2024

AI-generated image

#ReDirection

Safe Online

TECH COALITION

Protect Children

Protect Children is a non-governmental, non-profit organisation based in Helsinki, Finland, working globally to end all forms of sexual violence against children. We adopt a holistic, research-based approach to address the issue from multiple angles, advocating for victims, survivors, and families; equipping children and young people with essential skills and knowledge to stay safe online and offline; developing offender-focused prevention measures; and conducting innovative research.

Learn more about Protect Children: www.suojellaanlapsia.fi/en

Suojellaan Lapsia
Protect Children

Authors

This report is written by Tegan Insoll, Head of Research; Valeriia Soloveva, Specialist; Eva Díaz Bethencourt, Specialist; Anna Ovaska, Deputy Director; and Nina Vaaranen-Valkonen, Executive Director.

Funding

The research presented in this report was conducted within Protect Children's Primary Prevention to Protect Children research project which is funded by the Tech Coalition Safe Online Research Fund.

Safe Online is the only global investment vehicle dedicated to keeping children safe in the digital world. Through investing in innovation and bringing key actors together, Safe Online helps shape a digital world that is safe and empowering for all children and young people, everywhere. The Tech Coalition Safe Online Research Fund is a groundbreaking collaboration fuelling actionable research and uniting the tech industry with academia in a bold alliance to end online child sexual exploitation and abuse.

Learn more: https://safeonline.global/tc-safe-online-research-fund/

Safe Online

TECH COALITION

Acknowledgements

Thank you to our project partners, Red PaPaz, Helsinki University Hospital, Dr. Juha Nurmi, Ahmia.fi; and Professor of Criminology, Mikko Aaltonen, University of Eastern Finland; to the UK Online CSEA Covert Intelligence Team for providing crucial information for this report; and to Simon Bailey, CBE, QPM, DL, MSt (Cantab), for your guidance and feedback on this report in your role as Expert Advisor to Protect Children. We would also like to extend a warm thank you to all our global colleagues who have provided their expertise and translated the research surveys mentioned in this report, and to Webropol Oy for continuing to support our work by hosting our research surveys.

Suggested citation: Suojellaan Lapsia, Protect Children ry. "Tech Platforms Used by Online Child Sexual Abuse Offenders: Research Report with Actionable Recommendations for the Tech Industry" (2024).

This publication has been produced with financial support from the Tech Coalition Safe Online Research Fund. However, the opinions, findings, conclusions, and recommendations expressed herein are those of the author Protect Children and do not necessarily reflect those of Safe Online or the Tech Coalition.

Table of Contents

Introduction

We are facing a global epidemic of online child sexual abuse and exploitation. With the advancement of technology, the spread and availability of child sexual abuse material (CSAM) has grown explosively and exponentially worldwide, and children are increasingly exposed to online sexual violence.

In this report, we uncover new insights from anonymous surveys of CSAM offenders on the technology and platforms actively employed by online child sexual abuse perpetrators to view and share CSAM and engage with children online.

The rapid development of technology has facilitated an alarming surge in the accessibility of child sexual abuse material on online platforms, both across the surface web and the dark web. Findings from the UK National Crime Agency indicate that CSAM can be located on the open web with as few as three clicks through commonly used search engines.[1] In 2023, there were a staggering 36.2 million global reports documenting suspected instances of child sexual abuse material online.[2] Moreover, a comprehensive global study conducted by Economist Impact on behalf of WeProtect Global Alliance revealed that 54% of respondents, aged 18–20, had encountered online sexual harms during childhood.[3]

Child sexual abuse material (CSAM) includes images, videos, live-streaming, and any other material that depicts real or simulated sexual violence against a child. Every image and video causes harm to children.

Acts of sexual violence against children of which there is recorded footage are particularly traumatic for the victim. For victims of CSAM, the awareness that there is tangible evidence of their sexual abuse, coupled with the fear of its possible spread and circulation online, can have long-lasting devastating impacts.[4] Each time the material is viewed, the victim faces re-victimisation. Furthermore, the use of CSAM has been found to have a concerning correlation with continued offending,[5] underscoring the urgent need to reduce the availability of CSAM online.

Emerging technologies, including generative artificial intelligence (AI), are introducing new dimensions to the landscape of online harms. The rise of AI-generated CSAM, which can range from altered images of real children to entirely synthetic yet realistic looking content, exacerbates the already pervasive challenges in identifying and combating CSAM.[6] Regardless of their format, all depictions of child sexual abuse are abhorrent, as they contribute to the normalisation of sexual violence against children and rationalise offending behaviour, leading to further victimisation.

This report presents findings from Protect Children's innovative ReDirection study, which collects self-report survey data from anonymous individuals searching for CSAM on dark web search engines. We examine new data on the technology pathways of CSAM offenders, providing valuable insights into how perpetrators access, distribute, and view illicit content online, as well as the technology and platforms they use to contact children. The findings provide valuable insights for the development of effective strategies to prevent online sexual violence against children. The report includes findings highly relevant for the tech industry, policy makers, law enforcement, and civil society.

Methodology

Within the ReDirection project, we collect unprecedented information about online child sexual abuse and exploitation through surveys of individuals searching for child sexual abuse material on dark web search engines.

The research surveys are suggested to people who have attempted to search for CSAM using a keyword or term that is known to be associated with CSAM. Searchers are met with the option to answer the "Help us to help you" or "No need for help" surveys, alongside suggested links to support services to stop using CSAM.

Launched in December 2020, the surveys have received over 30,000 responses in 21 languages, with English, Spanish, and Russian comprising around 80% of the total. The sample of respondents represents a population of anonymous CSAM offenders who have an interest in viewing material depicting sexual violence against children. Research into this population is limited, as previous studies have predominantly examined convicted or known samples of CSAM offenders.[7] As such, this research provides unprecedented insight into the behavioural patterns and habits of current, undetected offenders.

Help us to help you. Take few minutes to answer this survey.

This survey aims to gather information to support the development of a self-help program intended for people who are worried about their sexual interest, thoughts, feelings, or actions concerning children.

From the survey results, we have gained knowledge about the thoughts, feelings, and behaviours of CSAM offenders, including how they were first exposed to CSAM, and their help-seeking behaviour and attitudes. Read more about our ReDirection research: www.protectchildren.fi/en/redirection/

Involuntary exposure to CSAM in childhood is prevalent

70% were first exposed to CSAM when they were under the age of 18

50% were first exposed to CSAM accidentally

CSAM offenders predominantly search for CSAM depicting girls aged 4-13

45% search for CSAM depicting girls aged 4-13

18% search for CSAM depicting boys aged 4-13

Use of CSAM is strongly correlated with seeking contact with children

40% have sought contact with a child after viewing CSAM

Many CSAM offenders want to stop viewing CSAM, however very few have sought help

50% want to stop using CSAM, however only 28% have sought help to stop

Recognising a need to understand more about the tech pathways of CSAM offenders, we developed a set of new survey questions to directly inquire about the platforms the respondents have used to search for CSAM and to contact children. This research was made possible through the support of the Tech Coalition Safe Online Research Fund. This report analyses responses to these nine new survey questions, collected over eight and a half months from 27 April 2023 to 11 January 2024. The number of respondents varies between questions, from 75 to 1,528 respondents per question. For the full results, see the Survey Data section.

Key Findings

1. CSAM is easily accessible on the surface web, particularly on pornography sites and social media
   - Most respondents have encountered CSAM on the surface web
   - The surface web provides information on how to access CSAM on the dark web
2. Offenders view and share CSAM on popular social media and encrypted messaging apps
   - Social media platforms are used to search for, view & share CSAM
   - End-to-end encrypted messaging apps are used to search for, view & share CSAM
3. Perpetrators seek contact with children on social media, encrypted messaging apps, and online games
   - Many respondents have sought contact with children on social media
   - Offenders use online gaming platforms to seek contact with children
   - Encrypted messaging apps are used by perpetrators to contact children

KEY FINDING 1

CSAM is easily accessible on the surface web, particularly on pornography sites and social media

The proliferation of child sexual abuse material online has been increasingly recognised over recent years. Nonetheless, the dissemination of CSAM continues to occur on nearly all digital platforms, including websites visited every day by people around the world. Our research reveals that CSAM is shockingly accessible and available on the surface web and is often encountered on pornography websites and social media platforms.

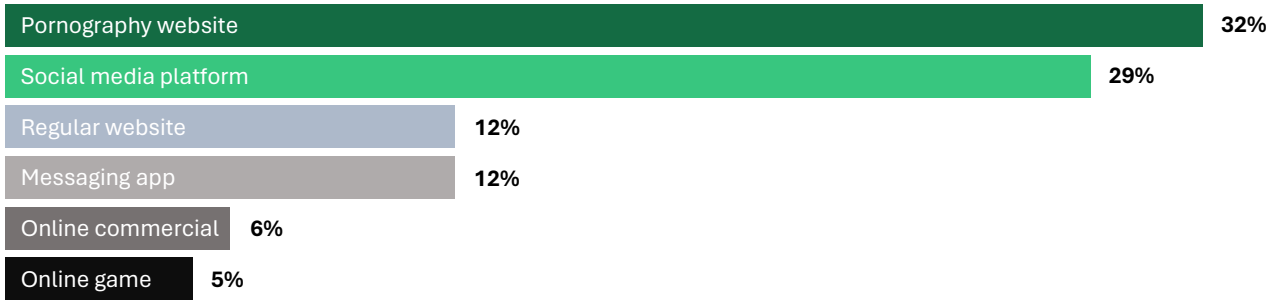
Most respondents have encountered CSAM on the surface web

77% of respondents have encountered CSAM or links to CSAM on the surface web

In response to the survey of individuals searching for CSAM on dark web search engines, 77% of respondents report that they have encountered CSAM or links to CSAM somewhere on the surface web. The majority say that they have encountered the material on a pornography website or on a social media platform. Regular websites and messaging apps are each cited by more than one in ten respondents as platforms where they have encountered CSAM.

Top locations where CSAM was encountered on the surface web

Question 1 'If you have encountered CSAM or links to CSAM on the surface web, where was it?' n=1,427



Accessibility of CSAM on pornography websites

32% of respondents have encountered CSAM or links to CSAM on a pornography website

32% of respondents report that they have encountered CSAM on a pornography website. When asked on which platform they have encountered CSAM, Pornhub (n=5) was the most cited platform. Although the majority of adult content websites have policies in place prohibiting any material depicting individuals under the age of 18 on their platforms,[8] our research is not the first to highlight the availability of CSAM on such platforms. A recent study found that almost a third of US online adult content consumers have unintentionally come across CSAM.[9] A number of pornography websites have been the centre of controversy for their role in hosting, distributing, and profiting from child sexual abuse, rape, trafficking in human beings, and other abusive and harmful material.[10]

Open-ended responses to option "Pornography website, which?"

The open-ended option was added to the survey on 1 November 2023.

"pornhub"	*"pornhub.com"*	*"pornhub"*	*"Pornhub"*
"Pornhub"	*"dark web"*	*"nice"*	*"BongaCams"*
"onestar.pw, allcams.cs, snapcamz.cc, and more sites like those"	*"Taboo"*	*"brasiltudoliberado"*	*"Не помню"*
	"xhamsters"	*"doeda"*	*[translation: I don't remember]*
	"ChatAvenue"	*"111"*	

The effectiveness of child safeguarding policies of adult content platforms is often criticised. For example, a recent case uncovered that a video uploaded to Pornhub had to be flagged 15 times before it would be reviewed, leading to a backlog of over 700,000 videos that were never reviewed as they did not receive enough reports.[11] In response to these cases, Pornhub has been taking significant steps to strengthen their Trust and Safety Policies and Procedures, including more robust verification of the age and consent of all individuals depicted in videos uploaded to the platform.[12] Nonetheless, there is an urgent need for further action to address the use of pornography platforms to disseminate abusive and illegal content.

Accessibility of CSAM on social media platforms

29% of respondents have encountered CSAM or links to CSAM on social media platforms

Among the survey respondents, the second most frequently mentioned place where they have come across CSAM on the surface web, after pornography sites, is social media platforms. When asked which platform, respondents frequently mentioned X (Twitter) (n=10), Instagram (n=7), Telegram (n=7), Facebook (n=6), and TikTok (n=4). Other platforms mentioned at least twice include Reddit, Discord, 4chan, and YouTube. Most social media platforms also offer direct messaging functions, which are increasingly end-to-end encrypted.

Open-ended responses to option "Social media platform, which?"

"youtube"	*"discord"*	*"Pixiv"*	*"twitter"*
"facebook"	*"telegram"*	*"searching"*	*"watts"*
"tiktok, instagram have softcore stuff that is a gateway to hardcore"	*"facebook"*	*"insta"*	*"facebook"*
	"whatsap"	*"telegram"*	*"Twitter is full of it"*
	"s"	*"twitter"*	*"Facebook"*
"twitter"	*"twitter.com"*	*"Facebook"*	*"Instagram"*
"twitter"	*"telegram"*	*"telegram"*	*"youtube"*
"Instagram"	*"Twitter/X"*	*"Telegram"*	*"twitter i f*****g hate that place for ruining my life over the past years"*
"snapchat,Instagram"	*"VKontakte"*	*"Tumblr, Facebook"*	
"tiktok"	*"tik tok"*	*"telegram"*	
"telegrsm"	*"Discord; reddit.com; tiktok"*	*"4chan /b/"*	*"twitter"*
"instagram"		*"4chan"*	*"Twitter"*
"reddit"	*"Instagram"*		

Each year, social media platforms identify and report tens of millions of instances of content depicting child sexual abuse and exploitation to the National Center for Missing & Exploited Children (NCMEC).[13] In 2022, Facebook alone submitted over 21 million reports, while Instagram submitted an additional 5 million reports.[14] These numbers continue to surge annually. Notably, TikTok had an 86% increase in reports compared to the previous year.[15] Additionally, investigations conducted by the UK Online CSEA Covert Intelligence Team have noted the alarming prevalence of CSAM across various widely used social media platforms.

High numbers of reports can be indicative of proactive efforts to address the spread of abusive and harmful content on social media platforms. Nonetheless, these figures highlight the massive proliferation of CSAM on social media platforms and emphasise the urgent need for strengthened online safety regulation, as well as the implementation of preventative measures by social media companies. Internet service providers, including social media platforms, currently have no legal obligation to actively search for and detect child sexual abuse material on their platforms. As such, there may be a significant underreporting of the actual prevalence of CSAM online.

There is a lack of a clear and harmonised legal framework to combat online CSEA, which is necessary to effectively tackle this phenomenon. According to the Internet Watch Foundation, Europe is the world's largest host of CSAM,[16] and the European Commission has stated that the EU is failing to protect children from falling victim to online child sexual exploitation and abuse.[17] In addition, voluntary actions from States against child sexual exploitation and abuse have been proven insufficient to prevent, detect, and combat child sexual abuse material.[18]

Other platforms mentioned by respondents where they have encountered CSAM

Open-ended responses to option "Regular website, which?"

"many pop online i don't know atm"
"Yandex, Google, Brave, Duckduckgo"
"bing"
"4chan"
"twitter"
"4chan"
"Комментарии в ютуб, реклама на телеграм канал" [translation: Comments on YouTube, advertising on Telegram channel]
"flickr"
"bazoocam"

Open-ended responses to option "Messaging app, which?"

"telegram and discord"
"sms"
"whatsapp"
"telegram"
"Telegram"
"telegram"
"kik"
"telegram"
"telegram"
"kik"
"Telegram"
"telegram"
"telegram"
"a"
"Telegramm"
"telegram"
"WhatsApp"
"Telegram"
"telegram"
"kik"
"telegram"
"Whatsapp"
"telegram"
"discord"
"Telegram"
"Viber"

Open-ended responses to option "Online game, which?"

"Mobile legends"
"gta"
", dv,ld"
"Free fire"
"roblox"

Open-ended responses to option "Other, what?"

"real life"
"Dark web"
"instagram and telegram same person"
"telegram app and mega app and twitter"
"deepweb"
"atravez de una app"
"Deep shearc"
"Discord"
"Twitter "
"Tiktok18+, iwanu"
"deep web"
"deep web"
"mr"
"google images"
"tiktok 18+"
"другие онион поисковики"
"image search"
"4chan"
"If you type key words but disoriented it pops up easily on the filtered web"
"imgsrc.ru"
"searching for somthing unrelated on duckduckgo"
"хз"
"4chan"
"pixiv.net"
"Yandex"
"no"
"nenhum"
"覚えていない" [translation: I don't remember]
"自分の経験" [translation: own experience]
"onion"
"TOR"
"Discord server"
"prefer not to say"
"Yandex"
"Some "nonude modeling" sites link to other sites which link to other sites which link to other sites, it takes a lot of jumping through hoops but you might eventually find it"
"deepweb"
"I have seen on reels"
"darknet search engine"
"I'd rather not say. Unwise."

The impact of the ease of access to CSAM on the surface web

The widespread availability and accessibility of CSAM on the surface web reflects significant harms. The staggering numbers of reports highlight the vast number of victims subjected to online sexual abuse and survivors, who face ongoing victimisation as their images continue to circulate online.

70% were first exposed to CSAM when they were under the age of 18

40% were first exposed when they were under 13 years old

Additionally, the widespread availability of CSAM online may lead to instances of involuntary exposure, which can be incredibly harmful to children and young people. Research within the ReDirection project has revealed that involuntary exposure to CSAM in childhood is common among those who search for CSAM, as a majority (70%) of survey respondents were first exposed to CSAM when they were under the age of 18, and around half say that they first encountered the content accidentally.[19] Such exposure to violent or abusive sexual content can be shocking and even traumatising for children, and may have a number of adverse effects, including on the development of risky and harmful sexual behaviours in the future.[20] Consequently, there is an urgent need for action to combat the availability of CSAM online, to end the cycle of abuse of survivors and prevent further offending against children.

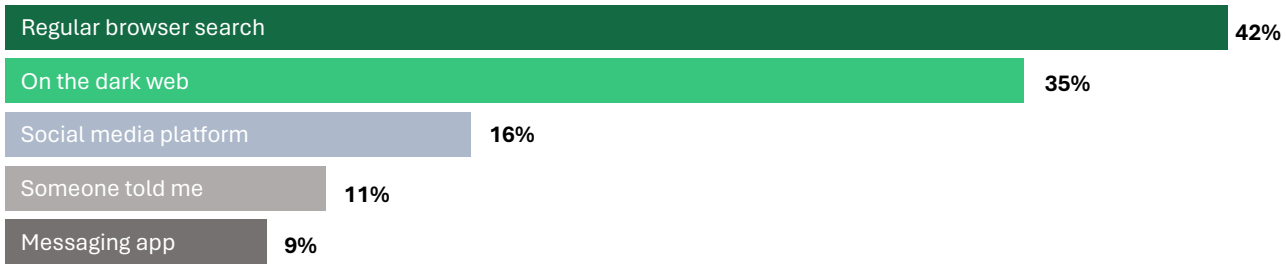
The surface web provides information on how to access CSAM on the dark web

42% of respondents learnt how to access CSAM on the dark web via a regular browser search

Information on how to evade detection and access CSAM via anonymous and secure platforms is available on the surface web through regular search engines. 42% of respondents report that they found information from a regular search engine on how to access CSAM on the dark web, while 16% of respondents report that they found this information on social media, and 9% via a messaging app.

Where respondents learnt how to access CSAM in the dark web

Question 6 'Where did you learn how to access CSAM in the dark web?' n=1,338



This finding is supported by data provided by the UK Online CSEA Covert Intelligence Team which highlights that offenders often use communication methods available on the surface web to establish and maintain contact between each other and share methods to access CSAM and groom children. Telegram, X (Twitter), Session, Teleguard, and Discord are widely used for offender-to-offender communication due to the lack or absence of content moderation, robust privacy settings, and communication features.[21]

KEY FINDING 2

Offenders view and share CSAM on popular social media and encrypted messaging apps

In response to the survey, 32% of respondents say that they have used social media platforms to search for, view, or disseminate CSAM. 29% of respondents say that they have used messaging apps for the same purpose. The platforms used most frequently by offenders are the same platforms that are frequented by children and young people.

Social media platforms are used to search for, view & share CSAM

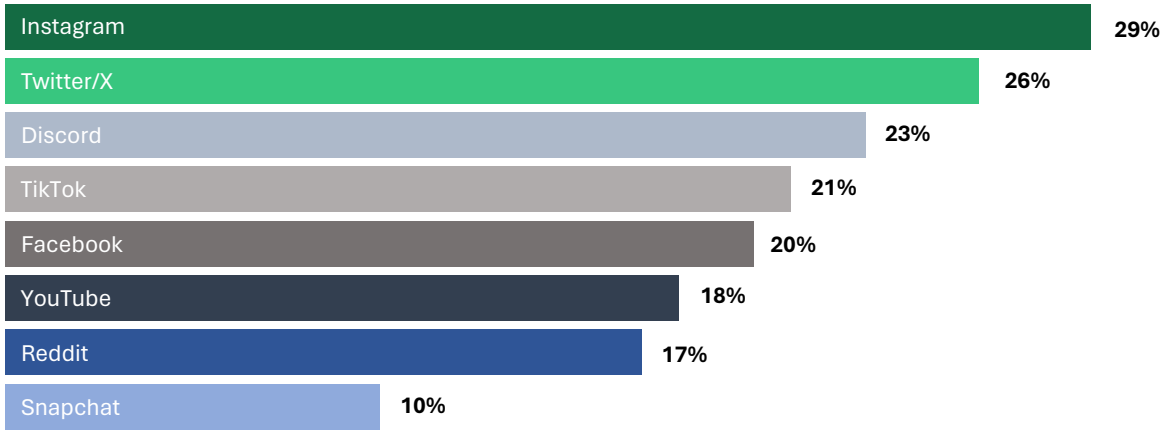
32% of respondents have used social media platforms to search for, view, or share CSAM

Social media platforms are commonly used to search for and view sexually abusive images and videos of children. One in three respondents to our survey of individuals searching for CSAM on dark web search engines report that, alongside using the dark web to find CSAM, they have also actively used popular social media platforms to view and share the imagery.

Of the social media platforms presented in the survey, the top platforms used by respondents to search for, view, or share CSAM are Instagram (29%), which is used by nearly a third of respondents, X (Twitter) (26%), and Discord (23%). Additionally, Discord, TikTok, and Facebook, and are each used by at least one in five respondents to view CSAM. Other social media platforms mentioned by survey respondents in response to the option "Other, what?" include Telegram and WhatsApp, which, although primarily messaging apps, also offer social networking features. The majority of the social media platforms mentioned also offer private and group messaging functions. There is an unmistakable overlap between the social media platforms most used for viewing and sharing CSAM and the platforms most popular among children and young people.[22]

Most frequently mentioned social media platforms used to search, view, and share CSAM

Question 3 'What social media platform on the surface web have you used to search, view, or share CSAM?' n=435



Viewing and disseminating CSAM may involve a range of illegal and harmful activities. Offenders use social media platforms to find images and videos of children, which may include CSAM shared by other offenders,

images of children posted by regular users, or "self-generated CSAM", i.e., images captured by a child.* Additionally, offenders often use features promoting connectivity between platform users to connect with likeminded people and join thematic communities that post or trade violent material. Finally, child sexual abuse material offenders misuse social media platforms to search for vulnerable children to groom or sexually extort (see Key Finding 3). Establishing contact with a child may result in further offences, involving, among other things, contact sexual abuse or the production of new child sexual abuse material.

Offenders misuse features of social media platforms to view and disseminate CSAM

Some features offered by social media platforms unintentionally create spaces where illegal behaviour can proliferate, as offenders actively identify ways to surpass child safeguarding mechanisms or abuse available features to search for and disseminate violent content. For example, a recent investigation by the Stanford Internet Observatory found that it is possible to use indicative search terms and hashtags to search for CSAM on Instagram.[23] Instagram's recommendation algorithms have been reported to disseminate "self-generated" CSAM and facilitate CSAM trading.[24] The investigation found that the Instagram CSAM-seller network includes between 500 and 1,000 accounts, making it one of the most used platforms for CSAM trading.[25]

29% of respondents who have used a social media platform to view or share CSAM have used Instagram

According to the UK Online CSEA Covert Intelligence Team, X (Twitter) is commonly used by offenders to connect with like-minded individuals, disseminate indicative content, and share websites where CSAM can be accessed.[26] It is being increasingly used to share AI-generated, cartoon, or drawn CSAM.

Investigations by the UK Online CSEA Covert Intelligence Team have found Discord to be the most mentioned communication platform for offender-offender communication outside of the dark web.[27] Its in-built features and lack of text moderation allow offenders to stay connected and create communities, where they share grooming strategies, links to websites that host CSAM, and information about accounts of children on various social media platforms.[28]

TikTok's strong recommendation algorithms allow offenders to advertise CSAM trading, connect with other offenders, search for children to groom, and view sexualised content depicting children. The app users utilise indicative wording, images, emojis, and black screens to surpass AI moderation.[29] One respondent to our survey reported that they had learnt how to use the dark web to access CSAM via TikTok by using code words often used to mean "child pornography", from the shared initialism "CP". In 2022, Forbes published an extensive article researching "in-private" CSAM posting – a form of violation when individuals post illegal material on TikTok in private accounts and subsequently share account's log-in information with other offenders.[30]

20% of respondents who have used a social media platform to view or share CSAM have used Facebook

In our study, 20% of respondents reported having used Facebook to search for, view, or disseminate CSAM. Recent cases support this finding, including a suit brought against Meta in December 2023 which, on the basis of an undercover investigation, alleged that certain content depicting child exploitation is ten times

* The term 'self-generated CSAM' does not sufficiently emphasize the unintended and non-consensual nature of this material, which often originates from grooming or sexual extortion. While searching for a more appropriate term, we continue using the term 'self-generated CSAM' providing additional remarks and acknowledging its drawbacks.

more prevalent on Facebook and Instagram than on Pornhub and OnlyFans.[31] A journalist investigation from 2022 found that Facebook fails to moderate groups openly hosting CSAM and accessible via explicit term search.[32]

New Forms of CSAM Distributed on Social Media Platforms: AI-Generated CSAM

New forms of CSAM are posing complex and evolving threats to children, including the production of AI-generated CSAM. Perpetrators are increasingly using AI to manipulate existing CSAM or images of children as well as to create completely AI-generated sexually abusive content depicting children.[33] In a period of five weeks, the Internet Watch Foundation (IWF) reported seven URLs confirmed as containing AI-generated CSAM.[34] Additionally, an IWF snapshot study of a dark web CSAM forum found over 20,000 AI-generated images posted in a one-month period.[35]

AI-generated CSAM The use of AI to create simulated or fictional images, videos, audios, or texts depicting child sexual abuse and exploitation.

AI-generated CSAM is created in different ways, such as through deepfake or 'nudification' processes, or by prompting instructions in an auto-regressive language model. It is often generated via open-access surface web platforms and even online games: for example, in 2021, the game AI Dungeon was misused to generate text depicting sexual exploitation of children.[36] Some generative AI tools are specifically designed to create sexual content, and a 2019 study by DeepTrace Labs found that 96% of all online deepfake video content was non-consenting pornographic material.[37] Other AI tools designed to 'nudify' images, i.e., alter images to make people appear naked, are gaining popularity.[38] This 'nudification' technology is also being used against children. In 2023, a group of male adolescents in Spain allegedly 'nudified' images of over 20 girls and adolescents and shared them via WhatsApp and Telegram.[39] In an attempt to tackle this, TikTok and Meta have blocked popular search terms associated with nudification tools.[40]

> "The abuse against me was recorded on video, pictures were taken and distributed to other people. Some of the pictures had been edited in a way so that it looked like intercourse."
> **Survivor of childhood sexual violence responding to the global #OurVoice survivor survey**

The creation, distribution, and use of simulated or fictional images or videos depicting child sexual abuse and exploitation violate the rights of the child and are incompatible with the inalienable value of human dignity. Not only does such material contribute to the normalisation of harmful behaviours constituting sexual violence against children, but also to the objectification and sexualisation of children. All this ultimately contributes to the dehumanisation and exploitation of the image of children and perpetuates a culture of violence, consequently violating children's inherent dignity.

End-to-end encrypted messaging apps are used to search for, view & share CSAM

29% of respondents have used a messaging app to search for, view, or share CSAM

In addition to social media platforms, we found that many respondents use messaging apps to view and share CSAM. Telegram was by far the most popular messaging app mentioned (46%), followed by WhatsApp (37%). Session, Wickr Me, and Signal were each mentioned by 13% of respondents who had used a

messaging app to search for or share CSAM. These messaging apps are often favoured by offenders due to the security and privacy offered by end-to-end encryption, which allows them to commit crimes without fear of detection or law enforcement presence. Other apps mentioned by multiple respondents in response to the option "Other, what?" include Discord, Kik Messenger, Instagram, X (Twitter), and Google Messages. In addition, the following were mentioned each by one respondent: Facebook Messenger, Enigma, ICQ, OK.RU, MEGA, OmeTV, and Minichat.

Messaging apps used to search for, view, and share CSAM

Question 5 'What messaging app have you used to search, view, or share CSAM?' n=358

46% of respondents who have used a messaging app to view or share CSAM have used Telegram

Nearly half of respondents who had used a messaging app to view and disseminate child sexual abuse material reported that they used Telegram. According to its Terms of Service, the platform explicitly forbids the posting of "illegal pornographic content on publicly viewable Telegram channels, bots, etc." , however it does not explicitly forbid this in private channels.[41] The UK Online CSEA Covert Intelligence Team reports Telegram to be one of the most trusted platforms for the sharing of illegal imagery, as well as for offender-offender communication.[42] It is commonly used by first-generation producers and for live-streaming of abuse. The messenger does not disclose any data to third parties, including governments, and has many privacy features that appeal to offenders such as end-to-end encryption, secret chats, self-destruct messages, editing and deleting any message from all devices after sending or receiving it, and private groups and channels.[43]

37% of respondents who have used a messaging app to view or share CSAM have used WhatsApp

37% of respondents who have used a messaging app to view or share CSAM report that they have used WhatsApp for this purpose. Whilst WhatsApp uses PhotoDNA to identify illegal material, only unencrypted content or reported is scanned,[44] leaving volumes of data without moderation.[45]

Signal and Session have been reported to attract child sexual abuse offenders with their strong privacy-by-design approach.[46] The messengers do not have access to any content exchanged between their users and collect minimal data and metadata from their users. Additional features such as group chats provide a secure space for exchanging CSAM and information that can facilitate crimes of sexual violence against children.[47]

Fighting the dissemination of CSAM: Wickr and Omegle

> One way for these people to reveal themselves was also any online streaming service, such as Omegle.
> **Survivor of childhood sexual violence responding to the global #OurVoice survivor survey**

Failure to adopt a child rights-by-design approach leads to the proliferation of illegal activity that can be difficult to stop retrospectively. In 2023, two platforms notorious for child rights violations, Wickr Me and Omegle, were discontinued.[48] Omegle, an online platform connecting strangers via video chat, faced numerous claims, and was eventually shut down after settling a large case initiated by a woman who was sexually abused on the platform at the age of 11.[49] Wickr Me, an end-to-end encrypted instant messenger owned by Amazon Web Services, was mentioned in 72 child sexual abuse cases in the United States, the United Kingdom, and Australia between 2018 and 2022.[50] In total, Wickr reported 15 instances of child sexual abuse material to NCMEC, while third partied filed around 3,500 reports involving the messenger.[51] In the online community, Wickr Me acquired a strong association with the dissemination of CSAM.[52] In our research, 13% of CSAM offenders who have used a messaging app to view and share CSAM reported having used Wickr Me.

Dissemination of CSAM on End-to-End Encrypted Messaging Apps

An increasing number of service providers are introducing end-to-end encryption, a secure communication method that allows only the recipient and the sender to see the contents messages, on their platforms.[53] Although designed as a safety feature, end-to-end encryption brings new risks to children online. End-to-end encryption, when introduced without additional child protection measures, makes it virtually impossible to detect child sexual abuse imagery on online platforms. Additionally, end-to-end encryption severely hinders law enforcement efforts to identify and rescue victims of sexual abuse and exploitation.

The detection and reporting of CSAM is essential for helping law enforcement prioritise the most urgent cases, for preventing the further victimisation of children, and for discovering trends that can assist in preventing these crimes. Without CSAM being detected and reported, ultimately the material cannot be removed, allowing for the cycle of revictimisation to continue.[54]

End-to-end encryption can also significantly contribute to the online disinhibition effect, as offenders become confident that their illegal activity cannot be detected, resulting in the emergence of large-scale CSAM communities.[55] Strong connectivity features such as groups, channels, or search options have turned some instant messengers into hubs of offending. Such messengers often become a part of grooming schemes when offenders coerce children to switch communication platforms to make sure the crime leaves minimal digital footprint.

KEY FINDING 3

Perpetrators seek contact with children on social media, encrypted messaging apps, and online games

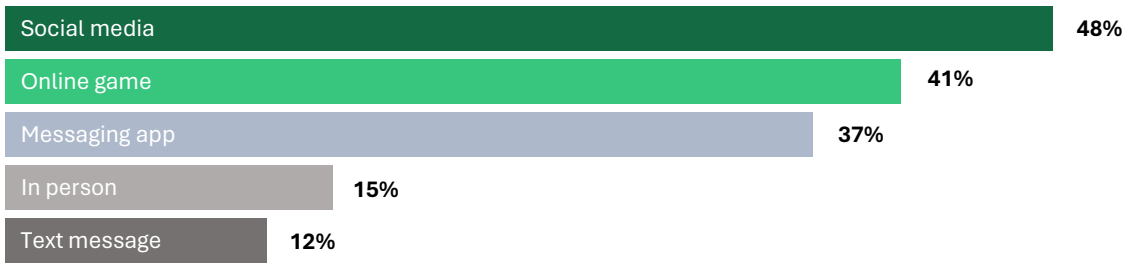
Our ReDirection research demonstrates that searching for, viewing, and sharing CSAM is strongly correlated with seeking direct contact with children, as around 40% of respondents say that they have sought contact with a child after viewing CSAM.[56] Additionally, nearly 60% of respondents say that they are afraid that their use of CSAM will lead to further sexual acts.[57]

70% of respondents who have sought contact with a child did so online

The present study reveals that 70% of respondents who have sought contact with a child tried to establish contact with a child online, the majority using social media platforms, online games, or messaging apps. Some respondents mentioned other methods they have used to contact children, including anonymous online video chat.

How CSAM offenders have established first contact with children

Question 7 'How have you attempted to establish the first contact with a child?' n=203



In the digital age, grooming methods used by perpetrators have multiplied and diversified. Today, one offender can reach hundreds of children in a matter of minutes, and the crime can occur fully online. The WeProtect Global Alliance reports that the prevalence of online grooming ranges between 9-19%.[58] Moreover, the NSPCC reports that online grooming crimes have risen by 82% in the past five years,[59] and similar exponential increases have been reported in France.[60] In-built features of online platforms, strengthened by rapidly developing AI, can facilitate and accelerate grooming. Combined with end-to-end encryption that hinders police investigations, grooming has evolved into a colossal threat. Over the internet, offenders can subject children to financial, sexual, or other forms of extortion. They can force the child to commit sexual violence on themselves or a peer, record or livestream the abuse, or coerce a child to meet in-person. In some cases, the violence can last for years.

Many respondents have sought contact with children on social media

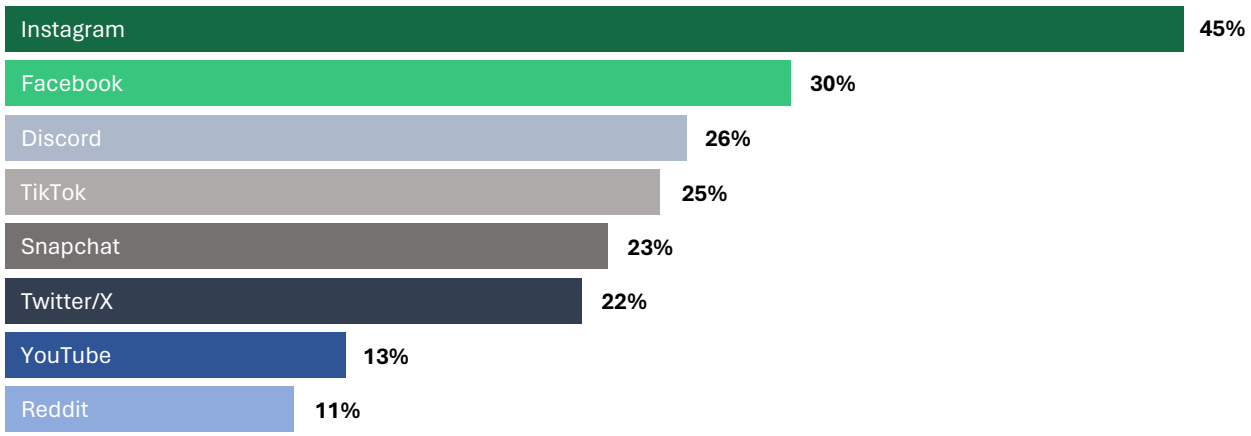
48% of respondents have attempted to establish first contact with a child on social media

The most common method reported by respondents to contact children is through social media. 48% of respondents who have contacted a child said that they used social media to establish the first contact.

Instagram was by far the most mentioned platform, selected by 45% of respondents as a social media platform they have used to contact children. Next is Facebook (30%), Discord (26%), and TikTok (25%), followed by Snapchat (23%), X (Twitter) (22%), YouTube (13%), and Reddit (11%). Other platforms mentioned by respondents in response to the option "Other, what?" include VK, Likee, and Telegram.

Most frequently mentioned social media platforms used to contact children

Question 9 'On which social media platform have you attempted to contact a child?' n=96



Altogether, Meta platforms Facebook, Instagram, and WhatsApp were mentioned in 51% of cases involving grooming that happened in England and Wales in the first quarter of 2020.[61] Instagram was mentioned in 37% of all cases.

Upon registration, Instagram does not verify the age of the new user. As Instagram actively promotes user connectivity, one child's account can be encouraged to connect with accounts displaying similar behaviour or interests. This may lead offenders who misreported their age to profiles owned by children. Even if the child's account is private, an adult user can still videocall or message them. Young people under 16, or 18 in some countries, have their Instagram account set to private by default, however this can be switched off at any time, including during signup.[62] Regardless of these issues, in December 2023, Meta announced their plan to rollout end-to-end encryption on Instagram and Messenger chat.[63]

Discord also serves as a place where offenders attempt to establish contact with children. They often use Disboard, a public list of Discord servers, to detect communities especially popular with underage users. As Discord strictly moderates visual content, offenders try to move children to more secure, encrypted platforms where their activity cannot be detected.

Due to TikTok's safety features, offenders may not be able to reach out to children directly, however they exploit other features available on the app. Forbes investigative article revealed that offenders can join livestreams of children and urge them to perform sexual actions.[64] To avoid moderation, they use indicative terms in communication where e.g., "outfit check" means that they would like to see the child's full body. Offenders entice children by sending them TikTok gifts that can be withdrawn in the form of money.

Offenders use online gaming platforms to seek contact with children

41% of respondents have attempted to contact a child on an online gaming platform

41% of respondents who have sought contact with a child shared that they tried to establish contact through an online game. For a long time, online games have been overlooked in the research of online crimes of

sexual violence against children and have only recently drawn the attention of professionals. Online games constitute an especially dangerous environment for children, as young users do not expect to be exposed to a real-life danger in a virtual world. Respondents to the #MyVoiceMySafety survey aged 7-10 shared that, when online, they felt the safest on gaming platforms and in private messaging apps.[65] Indeed, in many online games, communication with strangers is normalised, being a core part of the gaming process. In these circumstances, users may grow less suspicious of strangers, letting their guard down. At the same time, for offenders, it is easier to hide their real identity in gaming where many users do not reveal personal information. Recent research has shown that it takes 19 seconds for the child to be exposed to grooming during gaming and, on average, 45 minutes to be groomed.[66]

> In online games, many adults wanted nude photos and tried to pressure me into taking them. Many bets on sexual role-plays, for which I received goods in the games as a reward.
> **Survivor of childhood sexual violence responding to the global #OurVoice survivor survey**

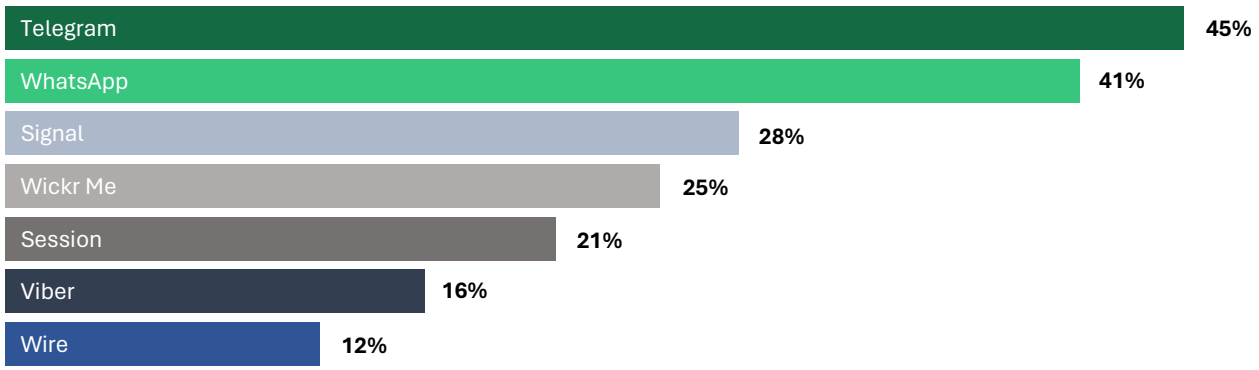
Encrypted messaging apps are used by perpetrators to contact children

37% of respondents have attempted to establish first contact with a child on a messaging app

37% of respondents shared that they established the first contact with a child via a messenger, mostly via end-to-end encrypted messengers Telegram (45%) and WhatsApp (41%). The next most mentioned apps include Signal (28%), WickrMe (25%), Session (21%), Viber (16%), and Wire (12%). Other platforms mentioned by respondents in response to the option "Other, what?" include Discord, Omegle, Snapchat, and Likee.

Most frequently mentioned messaging apps used to contact children

Question 8 'On which messaging app have you attempted to contact a child?' n=75



When perpetrating online crimes of sexual violence against children, offenders use a variety of platforms due to differences in security levels, audiences, and overall functionality. The phenomenon of making the child switch platforms is known as 'off-platforming'.[67]

Offenders use instant messengers with end-to-end encryption, such as Discord or X (Twitter), to maintain communication with each other. The lack of text moderation allows offenders to share grooming strategies, discuss offending and even share identified social media accounts of vulnerable children. Then, offenders proceed to online platforms popular among underage users such as Instagram, Discord, Snapchat, or online

games to contact children. Finally, the "destination" of the grooming process is usually a secure, end-to-end encrypted messenger, where evidence of the crime cannot be identified or accessed. Altogether, due to the lack of child safety-by-design approach, online platforms create an extremely dangerous and interconnected environment that facilitates offending and puts children at risk.[68]

> Adult men contacted me in online applications such as Kik messenger. The messages were harassing, enticing and sexual. I also received a lot of messages from adult men through other applications. They sent very sexually tinged messages, revealing pictures and videos.
> **Survivor of childhood sexual violence responding to the global #OurVoice survivor survey**

Research has shown that, despite the commonly spread stereotype of online child sexual abuse offenders as tech savvy individuals, many of them use in-built privacy features such as E2EE rather than securing their privacy by additional means. 54% of individuals arrested for possession of CSAM in Australia did not disguise owned material in any way.[69]

Quotes from survivors of online sexual violence against children

"The abuse against me was recorded on video, pictures were taken and distributed to other people. Some of the pictures had been edited in a way so that it looked like intercourse."

"In online games, many adults wanted nude photos and tried to pressure me into taking them. Many bets on sexual role-plays, for which I received goods in the games as a reward."

"Adult men contacted me in online applications such as Kik messenger. The messages were harassing, enticing and sexual. I also received a lot of messages from adult men through other applications. They sent very sexually tinged messages, revealing pictures and videos. One way for these people to reveal themselves was also any online streaming service, such as Omegle."

"In my case, sexual violence has mostly happened online. I used to have free access to the internet because my parents are not very familiar with technology. It started with kid-oriented platforms, where grown men pretended to be kids and got me to give them my phone number and send them pictures of myself."

"I believe that the violence that happened on the internet normalised sexual encounters between an adult and a child for me, which made me think that it was normal in later life."

"I was a child exploitation survivor, in organized abuse. As soon as technology became available, it was used to share CSAMs and communicate with me."

#OurVoice global survivor survey

Suojellaan Lapsia
Protect Children

Findings from the Global #OurVoice Survey for Survivors of Sexual Violence in Childhood

Protect Children's global #OurVoice survivor survey provides vital information on the experiences of victims and survivors of childhood sexual violence around the world. Our goal is to raise the long-silenced voices and wisdom of survivors, to impact legislative change, and to ultimately prevent all crimes of sexual violence against children.

The survey is available in 18 languages, and data collection has been ongoing since 4 November 2023. As of 1 February 2024, 6,872 survivors around the world have responded to the survey. The responses have provided invaluable insight into the experiences of survivors who have been subjected to technology-facilitated crimes of sexual violence in childhood.

In response to the survey, 404 survivors report that their abuse happened online or was in some way facilitated by technology. A majority, namely 84%, shared that they were subjected to abuse on more than one occasion. In total, 83% of those who experienced online abuse say that it has led to long-term consequences, namely depression, difficulties in forming and maintaining close relationships, anxiety disorder/panic attacks, and PTSD/PTS symptoms.

83% of survivors of online child sexual abuse say that their abuse has led to long-term consequences

84% of survivors of online child sexual abuse were subjected to sexual violence as a child on more than one occasion

The scale and impact of online crimes of sexual violence against children is being increasingly recognised around the globe. We have included throughout this report quotes from respondents to the global #OurVoice survivor survey to demonstrate the harmful nature of technology-facilitated crimes of sexual violence against children.

It is vital that the voices of all victims and survivors of childhood sexual violence are heard and that we do our utmost to facilitate healing and recovery and ensure the safety of all children. We provide support resources for respondents to the #OurVoice survivor survey and ask participants to share information that can help to strengthen victim's rights and protect children.

We appreciate and thank each and every survivor who shared their experiences through this survey. We will use the knowledge we gain to support survivors all over the world and continue fighting to end all forms of sexual violence against children.

Take part in the survey
https://ourvoicesurvey.com/

Actionable Recommendations

The findings presented in this report highlight key issues that require urgent action by the tech industry, among other actors. On the basis of the findings of this research, alongside insights from our work, we have developed five actionable recommendations for the tech industry.

The recommendations should be considered holistically, as one approach alone is not adequate to tackle the enormous scale of the problem of online child sexual exploitation and abuse. All actors have a responsibility to address sexual violence against children and keep children safe in all environments.

1. Build and develop platforms with a children's rights-by-design approach
2. Ensure availability and accessibility of online safety resources and information for children
3. Effectively detect, report, and remove CSAM and combat OCSEA
4. Implement deterrence and perpetration prevention measures
5. Ensure robust and proportionate age assurance measures

RECOMMENDATION 1

Build and develop platforms with a children's rights-by-design approach

We urge service providers to place children's safety and rights at the forefront of technological development and ensure that digital environments are designed to prioritise children's rights.

We recommend tech companies to design platforms with a children's rights-by-design approach.[70] Child safety must be prioritised in the development of services that are available to children and can influence their safety or well-being. Technology companies should enrich safety-by-design by incorporating children's voices and providing accessible, child-friendly, and effective reporting tools with a meaningful response system.

End-to-end encryption should not be implemented without appropriate safeguards. Encrypted platforms are quickly becoming a safe haven for child sexual abuse offenders. The rollout of end-to-end encryption on tech platforms, without appropriate safeguards, directly undermines a children's rights-by-design approach, as it hinders law enforcement efforts to identify and rescue victims, prevents identification of grooming, and prevents tech companies' ability to detect child sexual abuse material. This puts children at increased risk of abuse and exploitation and continues the cycle of revictimisation of survivors. As such, we urge tech companies not to implement end-to-end encryption on their services unless they put in place further safeguards to ensure access to evidence by law enforcement and maintain the ability to detect and report child sexual abuse material.

Avoid misuse of functionality provided by the platform. Technology companies must subject all updates to thorough trials to engineer out the possibility to abuse its tools to harm children, always with guidance from children's perspectives. One of the ways to address misuse of the platform's functions is to limit opportunities for contact and interaction between adult and child users, i.e., by making accounts of child users invisible for adult users.

Monitor and address emerging threats. Technology companies must take a proactive approach in maintaining child safety by design by continuously monitoring and eliminating emerging risks. This includes constant improvement of existing filtering algorithms, age verification systems, and any other safeguarding mechanisms in place.

Follow good practices when using AI technologies. Online service providers must invest in good practices when using AI technologies and elaborate clear guidelines for privacy, personal data protection and information, and user safety. In addition, service providers must implement robust measures to reduce or eliminate the risk of AI being misused or abused, for example to generate CSAM. At the same time, we encourage tech companies to invest resources in AI technologies that contribute to preventing harm, and to train AI algorithms with a focus on child protection and a human rights-based and intersectional perspective, to avoid discrimination and bias.

Any platform that can be accessed by children or influence their safety and well-being must be built with a children's rights-by-design approach. Children must be provided with an opportunity to meaningfully participate in the product development and share their experiences through an effective reporting system. Children's inherent vulnerabilities must not be exploited for profit.

RECOMMENDATION 2

Ensure availability and accessibility of online safety resources and information for children

We call on online platforms to ensure that online safety resources and information are provided in a comprehensive and accessible manner for all children, families, victims, and survivors.

As evidenced by the research report, social media, instant messengers, and online games are all being used to commit crimes of sexual violence against children. As such, internet service providers have the responsibility to ensure that the rights of the child are respected on their platforms. Moreover, internet service providers must ensure sure that children understand the rights they are entitled to online, understand how their rights are protected, and be well-informed about the safeguarding mechanisms at their disposal.

Inform children about their rights online. Tech companies must take effective measures to guarantee children's right to information on their platforms. All information and resources must be comprehensive, available, and accessible to all children and young people. The right to information expands to children and young people's families, as well as to victims and survivors. Internet service providers should offer age-appropriate information in all languages and the information should be culturally adapted to ensure equal access.

Offer comprehensive information about safeguarding mechanisms. Over three quarters of respondents to our survey reported that they have encountered CSAM on the surface web, highlighting that CSAM is widely accessible and available on common online platforms and websites. As a result, involuntary exposure to harmful material among children and young people is prevalent. Internet service providers must provide clear and age-appropriate information about what constitutes illegal behaviour or content with relevant examples. Internet service providers must ensure that support and safeguarding mechanisms are easily accessible and well explained, so if a child or young person is concerned about their safety, they know how to access appropriate support. This contributes to prevent discrimination and re-victimisation in case of child victims.

We encourage internet service providers to offer relevant, country-specific, and accessible information for children on where to seek support in cases when a child feels that the platform negatively influences their well-being, when exposed to harmful or illegal content, or when subject to online sexual violence. Internet service providers should inform children what cases must be reported to the police and explain the procedure of reporting. We encourage internet service providers to offer information about available support after a child user blocks another user or flags inappropriate content.

Adopt an intersectional approach. Children belonging or identifying themselves with minority groups are at greater risk of being exposed to online child sexual abuse and exploitation, according to WeProtect Global Alliance.[71] As such, internet service providers must take measures to effectively combat sexual violence against children from all angles. Adopting an intersectional approach means recognising the differences between children and understanding the co-existence of multiple forms of discrimination among them, based on gender, race, ethnicity, gender identity, sexual orientation, disability, class, and other grounds of discrimination. Through an intersectional approach, internet service providers can ensure that their platforms are adapted and accessible for all children. Ultimately, this would help to ensure that children can stay safe in the digital environment.

RECOMMENDATION 3

Effectively detect, report, and remove CSAM and combat sexual violence against children online

We urge all internet service providers to take active steps to detect, report, and remove CSAM from their platforms, and to eliminate all forms of sexual violence against children including grooming.

Our research results find that child sexual abuse material is widely available online, especially on pornography sites and social media platforms. The circulation of CSAM online leads to the continuous revictimisation of survivors of sexual violence. In addition, the accessibility of the material increases the risk of exposure to harmful material to children and young people, which has been found to be associated with an increased risk of harmful sexual behaviour.[72] Our previous research has shown that people who view CSAM are likely to contact children.[73] By effectively removing CSAM from the internet, further victimisation can be prevented. The less CSAM that circulates the internet, the less likely it is for an individual to come across the material.

Proactively detect child sexual abuse material. Reactive detection of child sexual abuse material based on user reports is an important measure to ensure the removal of abusive material from online platforms. However, this alone is inadequate to address the proliferation of CSAM online, and efficient proactive detection measures must be adopted. In 2022, electronic service providers sent more than 31.8 million reports of suspected child sexual exploitation to NCMEC's CyberTipline.[74] These reports are essential for helping law enforcement prioritise the most urgent cases, for identifying and rescuing victims,[75] for preventing the further victimisation of children, for empowering survivors, and for discovering trends that can assist in preventing these crimes.[76] We recognise the significant efforts of companies who currently proactively detect and report CSAM and encourage them to continue their efforts to combat child sexual abuse and exploitation. However, only 236 electronic service providers submitted CyberTipline reports in 2022 and just five companies (Facebook, Instagram, Google, WhatsApp, and Omegle) accounted for more than 90% of the reports.[77] Most tech companies around the world still choose not to proactively detect and report child sexual abuse and exploitation on their platforms.[78] Thus, we urge all companies that host user-generated content, particularly social media platforms, messaging platforms, and file-sharing platforms, to begin proactive detection and reporting of CSAM with urgency. By both proactively and reactively detecting child sexual abuse material, tech companies have an important role in contributing to the removal of the material, thus ending the cycle of revictimisation for victims and survivors.

Cooperate with law enforcement and report information. Internet service providers must forge efficient collaboration with national and international law enforcement agencies and report any form of sexual violence against children including grooming or attempts thereto. Law enforcement agencies must be allowed to conduct searches on the platform to ensure removal of reported, detected, or suspected child sexual abuse material. Furthermore, to facilitate ongoing investigation, it is advisable to provide relevant law enforcement agencies with access to visual and written content exchanged between the perpetrator and the victim that facilitated or constituted sexual violence against children, as well as to any other content or data collected and processed by the service provider about the victim and the perpetrator. Additionally, reporting is key to ensure the effective protection of children from abuse or exploitation and to avoid revictimisation. We urge internet service providers to report to national law enforcement agencies and national reporting hotlines any form of sexual violence against children immediately when brought to their attention.

RECOMMENDATION 4

Implement deterrence and perpetration prevention measures

We urge all internet service providers to implement effective deterrence and prevention measures for persons who are at risk of committing crimes of sexual violence against children on their platforms.

It is vital to implement effective deterrence and prevention measures for potential and actual perpetrators of crimes of sexual violence against children, to prevent offending before it occurs. As demonstrated by our research results, child sexual abuse material is widely accessible and available on the surface web, where it is not only viewed, disseminated, and procured by persons actively seeking to engage with the material, but children themselves are also being exposed to the material involuntarily. A majority of current CSAM offenders were first exposed to the material as children themselves. Finally, 40% of CSAM offenders report having sought contact with a child after viewing the material. A clear escalation within the offending pathway is visible, which underlines the importance of effective deterrence and prevention measures for people who search for and view child sexual abuse and exploitation material.

We encourage online service providers and tech companies to make available resources for individuals who are worried about their thoughts and who fear they might commit or recommit harmful acts against children. All tech companies should promote a space of respect for the rights of the child, and of safety and good practices focused on child protection. In addition, online service providers and tech companies should encourage users to report any suspicious, abusive, or harmful content involving children. The reporting processes should be simple and accessible.

All platforms that allow for image or video sharing, in particular pornography websites, must prohibit all search terms that refer to any form of child sexual abuse and exploitation and include deterrence messages to appear when searches are conducted using such terms. Deterrence messages should educate individuals about the repercussions of searching for CSAM, by clearly informing about the real-life consequences on the child victim, as well as the legal consequences of searching for and viewing CSAM or committing any other form of sexual violence against children. Deterrence messages should additionally refer individuals to relevant perpetration prevention resources for individuals at risk of committing or recommitting offences against children. These deterrence messages should appear on all platforms whenever a user searches for CSAM, attempts to contact a child, or carries out any other harmful activity online.

To keep all children safe from sexual violence comprehensively and effectively, prevention efforts must include potential offender-focused prevention and intervention measures at a low threshold.

RECOMMENDATION 5

Ensure robust and proportionate age assurance measures

We call on service providers to assure the age of all users meaningfully and consistently, using robust and proportionate measures to create a safer online experience for children and young people.

The adoption of robust age assurance measures is essential to limit opportunities for grooming, and prevent children from accessing harmful content, by regulating access of users to specific content, services, and communication with other users. Service providers should introduce robust and mandatory age assurance mechanisms for all users.

Age assurance must constitute a recurring process rather than a one-time verification to limit opportunities to circumvent the system. Based on the results of age assurance, the users should receive access to age-appropriate content and services offered by the service provider. The users should be clearly informed how and why their age influences access to particular services provided by the platform. If the platform hosts adult content, age assurance must additionally concern every person depicted in the content.

> “In my case, sexual violence has mostly happened online. I used to have free access to the internet because my parents are not very familiar with technology. It started with kid-oriented platforms, where grown men pretended to be kids and got me to give them my phone number and send them pictures of myself.”
>
> **Survivor of childhood sexual violence responding to the global #OurVoice survivor survey**

Technology companies must regularly monitor and eliminate opportunities to abuse the age assurance systems. They should clearly inform the users about the consequences of circumventing the age assurance system and the risks that it can cause to their safety. We also advise platforms to develop effective sanctions for circumventing age assurance system that can affect the user’s access to the platform. Users who violate the age assurance system should be identified and removed from the platform.

The age assurance measures must respect the right to personal data and privacy of communications. As implementing an effective international age assurance system that does not compromise users’ personal information constitutes a challenge, we strongly recommend supporting the research and development of new-age verification systems.

Survey Data

This report presents data from nine questions of the "Help us to help you" survey of individuals searching for child sexual abuse material on dark web search engines, collected over eight and a half months from 27 April 2023 to 11 January 2024. The complete quantitative data from these questions is laid out in this section.

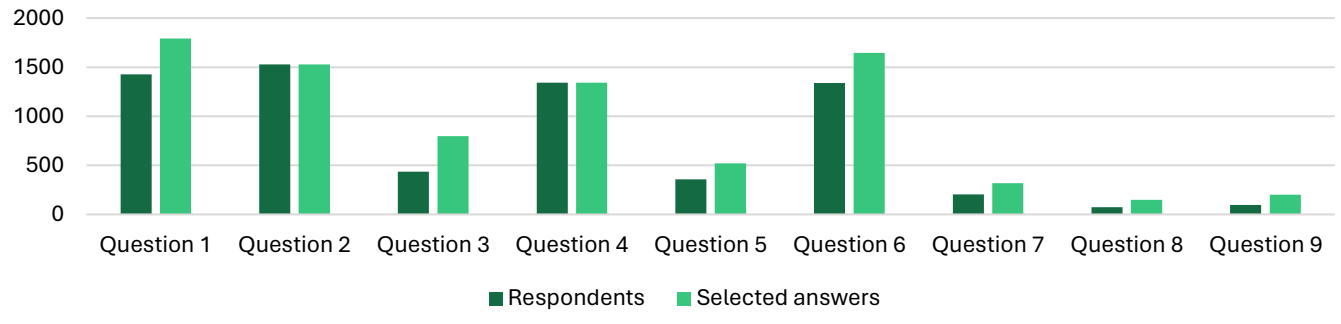
Question Rules & Visibility

Seven questions allow for the respondents to select multiple answers, and two questions are single selection. Four questions are visible to all respondents, whilst five questions are only visible to select respondents, based on their responses to previous questions. The number of respondents varies between questions, from 75 to 1,528 respondents per question.

Overview of Questions

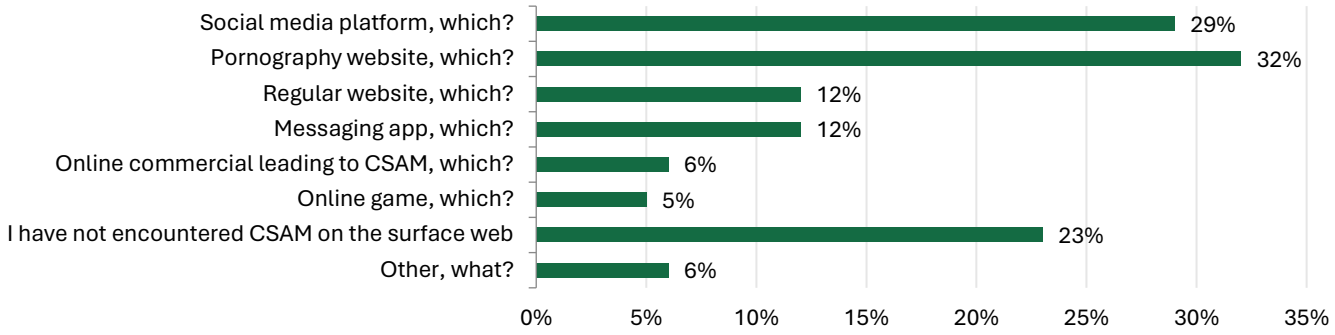
	Question	Rules	Visibility	Respondents	Selected answers
1	If you have encountered CSAM or links to CSAM on the surface web, where was it?	Multiple selection	All	1,427	1,793
2	Have you used any social media platforms on the surface web to search, view or share CSAM?	Single selection	All	1,528	1,528
3	What social media platform on the surface web have you used to search, view, or share CSAM?	Multiple selection	Conditional	435	798
4	Have you used any messaging apps to search, view or share CSAM?	Single selection	All	1,341	1,341
5	What messaging app have you used to search, view, or share CSAM?	Multiple selection	Conditional	358	519
6	Where did you learn how to access CSAM in the dark web?	Multiple selection	All	1,338	1,645
7	How have you attempted to establish the first contact with a child?	Multiple selection	Conditional	203	317
8	On which messaging app have you attempted to contact a child?	Multiple selection	Conditional	75	149
9	On which social media platform have you attempted to contact a child?	Multiple selection	Conditional	96	200

Respondents and Selected Answers per Question



1. If you have encountered CSAM or links to CSAM on the surface web, where was it?

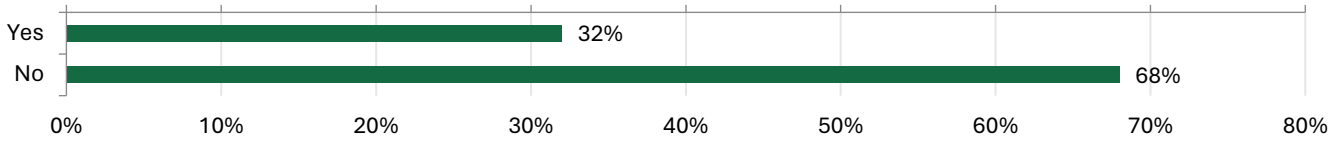
Survey rules: Multiple selection possible.
Respondents: 1,427
Selected answers: 1,793



	N	%
Social media platform, which?	411	28.8%
Pornography website, which?	452	31.7%
Regular website, which?	176	12.3%
Messaging app, which?	174	12.2%
Online commercial leading to CSAM, which?	81	5.7%
Online game, which?	78	5.5%
I have not encountered CSAM on the surface web	330	23.1%
Other, what?	91	6.4%
	1,793	

2. Have you used any social media platforms on the surface web to search, view or share CSAM?

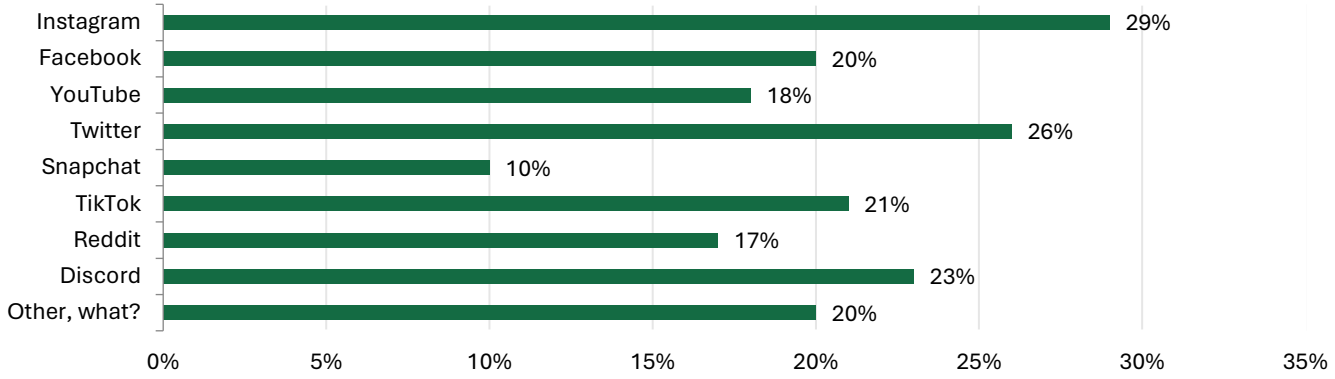
Survey rules: Single selection.
Respondents: 1,528



	N	%
Yes	487	31.9%
No	1041	68.1%
	1528	

3. What social media platform on the surface web have you used to search, view, or share CSAM?

Survey rules: This question is visible only to respondents who answered "Yes" to the question "Have you used any social media platforms on the surface web to search, view or share CSAM?". Multiple selection possible.
Respondents: 435
Selected answers: 798

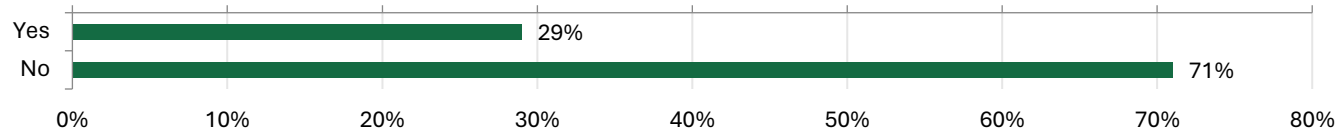


	N	%
Instagram	127	29.2%

Facebook	89	20.5%
YouTube	77	17.7%
Twitter	112	25.7%
Snapchat	43	9.9%
TikTok	92	21.1%
Reddit	72	16.6%
Discord	101	23.2%
Other, what?	85	19.5%
	798	

4. Have you used any messaging apps to search, view or share CSAM?

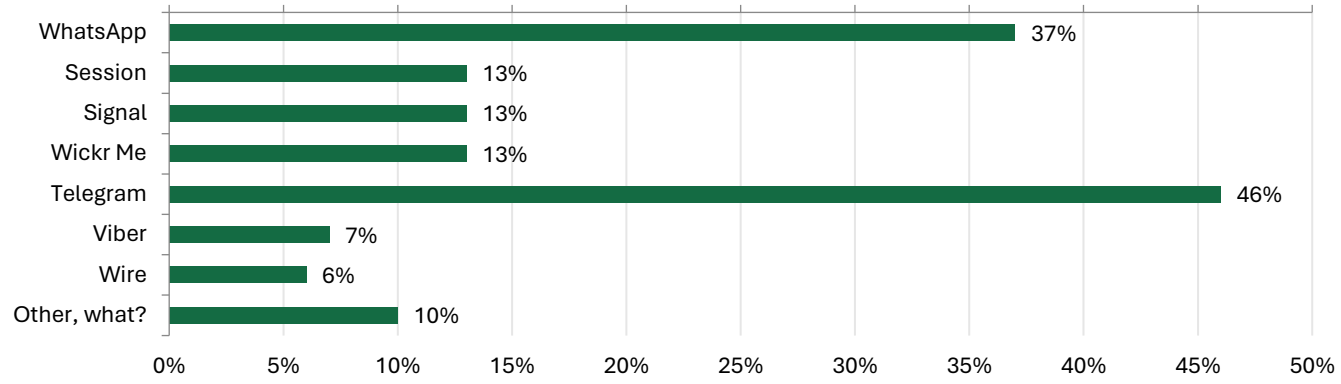
Survey rules: Single selection.
Respondents: 1,341



	N	%
Yes	385	28.7%
No	956	71.3%
	1341	

5. What messaging app have you used to search, view, or share CSAM?

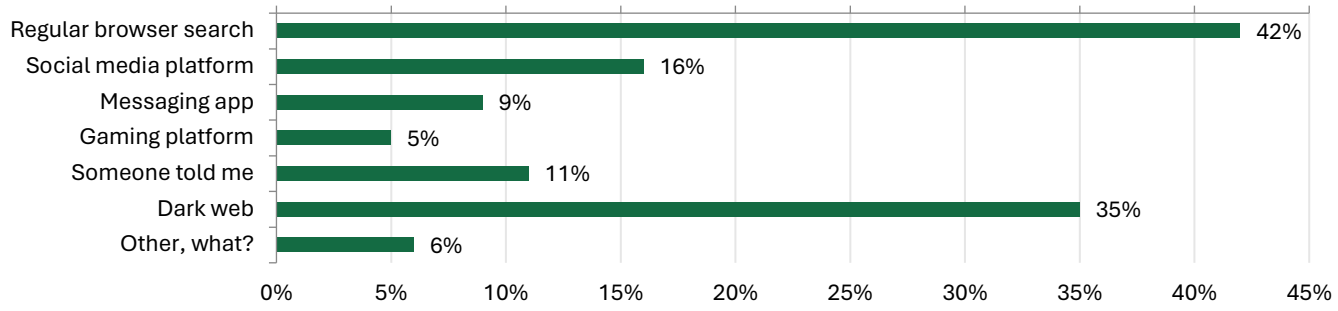
Survey rules: This question is visible only to respondents who answered "Yes" to the question "Have you used any messaging apps to search, view or share CSAM?"). Multiple selection possible.
Respondents: 358
Selected answers: 519



	N	%
WhatsApp	131	36.6%
Session	47	13.1%
Signal	46	12.8%
Wickr Me	47	13.1%
Telegram	163	45.5%
Viber	26	7.3%
Wire	22	6.1%
Other, what?	37	10.3%
	519	

6. Where did you learn how to access CSAM in the dark web?

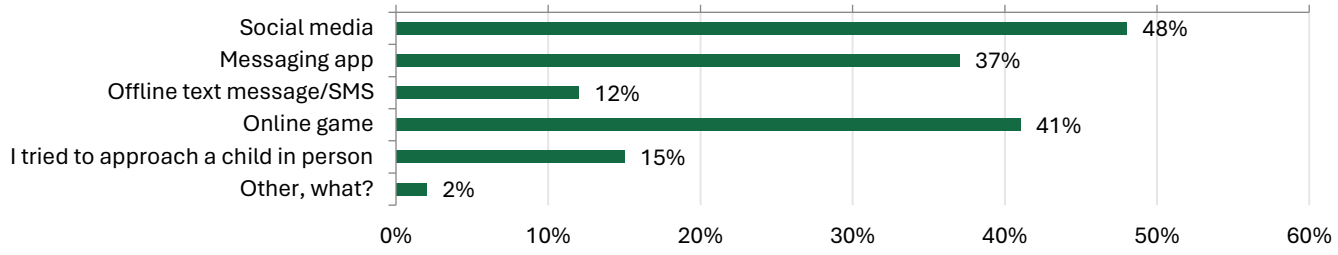
Survey rules: Multiple selection possible.
Respondents: 1,338
Selected answers: 1,645



	N	%
Regular browser search	556	41.6%
Social media platform	208	15.5%
Messaging app	114	8.5%
Gaming platform	72	5.4%
Someone told me	142	10.6%
Dark web	468	35.0%
Other, what?	85	6.4%
	1645	

7. How have you attempted to establish the first contact with a child?

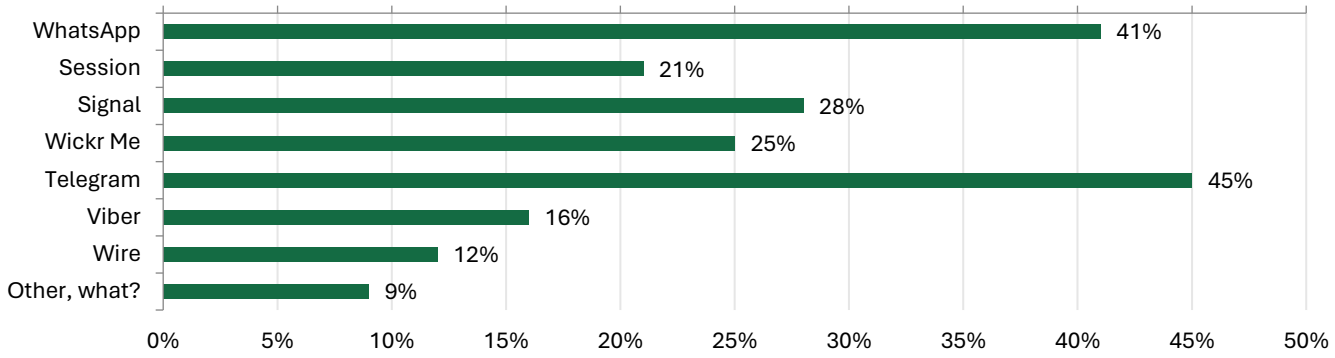
Survey rules: This question is visible only to respondents who answered "Rarely", "Monthly", "Weekly", or "Nearly every time" to the question "How often after viewing CSAM have you sought direct contact with children through online platforms?". Multiple selection possible.
Respondents: 203
Selected answers: 317



	N	%
Social media	98	48.3%
Messaging app	75	36.9%
Offline text message/SMS	25	12.3%
Online game	84	41.4%
I tried to approach a child in person	31	15.3%
Other, what?	4	2.0%
	317	

8. On which messaging app have you attempted to contact a child?

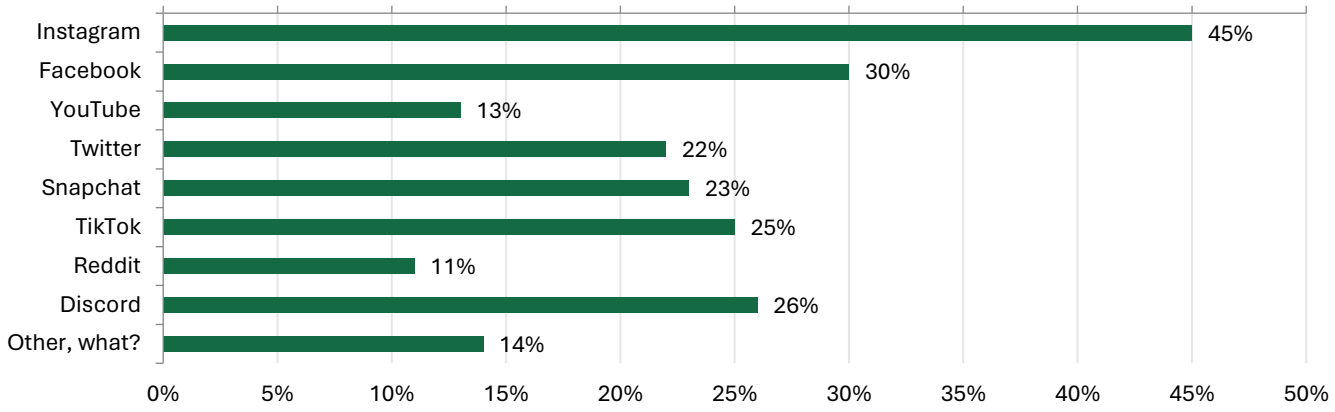
Survey rules: This question is visible only to respondents who answered "Messaging app" to the question "How have you attempted to establish the first contact with a child?". Multiple selection possible.
Respondents: 75
Selected answers: 149



	N	%
WhatsApp	31	41.3%
Session	16	21.3%
Signal	21	28.0%
Wickr Me	19	25.3%
Telegram	34	45.3%
Viber	12	16.0%
Wire	9	12.0%
Other, what?	7	9.3%
	149	

9. On which social media platform have you attempted to contact a child?

Survey rules: This question is visible only to respondents who answered "Social media" to the question "How have you attempted to establish the first contact with a child?". Multiple selection possible.
Respondents: 96
Selected answers: 200



	N	%
Instagram	43	44.8%
Facebook	29	30.2%
YouTube	12	12.5%
Twitter	21	21.9%
Snapchat	22	22.9%
TikTok	24	25.0%
Reddit	11	11.5%
Discord	25	26.0%
Other, what?	13	13.5%
	200	

References

[1] National Crime Agency. (2020). European police chiefs back NCA demands for tech companies to do more to prevent child sex abuse. https://www.nationalcrimeagency.gov.uk/news/european-police-chiefs-back-nca-demands-for-tech-companies-to-do-more-to-prevent-child-sex-abuse.

[2] National Center for Missing & Exploited Children. (2024). NCMEC Debuts New Sextortion Videos for Safer Internet Day. https://www.missingkids.org/blog/2024/new-sextortion-videos-safer-internet-day; National Center for Missing & Exploited Children. (2023). CyberTipline 2022 Report. https://www.missingkids.org/cybertiplinedata.

[3] WeProtect Global Alliance. (2022). Estimates of childhood exposure to online sexual harms and their risk factors. https://www.weprotect.org/economist-impact-global-survey/.

[4] Canadian Centre for Child Protection. (2017). Survivors' Survey. Full Report 2017. https://content.c3p.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf.

[5] Insoll, T., Ovaska, A. K., Nurmi, J., Aaltonen, M., & Vaaranen-Valkonen, N. (2022). Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. Journal of Online Trust and Safety, 1(2). https://doi.org/10.54501/jots.v1i2.29.

[6] Sullivan, E. Law Enforcement Braces for Flood of Child Sex Abuse Images Generated by A.I. (2024). The New York Times. https://www.nytimes.com/2024/01/30/us/politics/ai-child-sex-abuse.html.

[7] Rimer, J. R. (2019). "In the street they're real, in a picture they're not": Constructions of children and childhood among users of online child sexual exploitation material. Child Abuse & Neglect, 90. https://doi.org/10.1016/j.chiabu.2018.12.008; Merdian, H. L., Moghaddam, N., Boer, D. P., Wilson, N., Thakker, J., Curtis, C., & Dawson, D. (2018). Fantasy-driven versus contact-driven users of child sexual exploitation material: Offender classification and implications for their risk assessment. Sexual Abuse, 30 (3). https://doi.org/10.1177/1079063216641109; Bourke, M.L., Hernandez, A.E. (2009). The 'Butner Study' Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders. Journal of Family Violence, 24 (3). https://doi.org/10.1007/s10896-008-9219-y.

[8] Pornhub. (2023). Terms Of Service. https://www.pornhub.com/information/terms; xHamster. (2023). Terms & Conditions / User Agreement. https://xhamster.com/info/terms; XVideos. (2023). Terms of Service. https://info.xvideos.net/legal/tos.

[9] VerifyMy. (2024). Research reveals proliferation of child sexual abuse material on US adult websites. https://verifymy.io/blog/research-reveals-proliferation-of-child-sexual-abuse-material-on-us-adult-websites/.

[10] National Center on Sexual Exploitation. (2020). Judge Sides with Survivors of CSAM in Powerful Ruling Against Pornhub/MindGeek. https://endsexualexploitation.org/articles/judge-sides-with-survivors-mindgeek-ruling/

[11] Thies, B.F. (2023). Pornhub had roadblock for reviewing potential child sexual content, documents show. Washington Examiner. https://www.washingtonexaminer.com/news/2448580/pornhub-had-roadblock-for-reviewing-potential-child-sexual-content-documents-show/.

[12] Pornhub. (2024). Co-Performer Verification: Proof of Consent. https://www.pornhub.com/blog/co-performer-verification-proof-of-consent; Iovine, A. (2024). Pornhub will require proof of consent from all performers. Mashable. https://mashable.com/article/pornhub-will-require-proof-of-consent-from-all-performers.

[13] National Center for Missing & Exploited Children. (2023). 2022 CyberTipline Reports by Electronic Service Providers (ESP). https://www.missingkids.org/content/dam/missingkids/pdfs/2022-reports-by-esp.pdf.

[14] National Center for Missing & Exploited Children. (2023). 2022 CyberTipline Reports by Electronic Service Providers (ESP). https://www.missingkids.org/content/dam/missingkids/pdfs/2022-reports-by-esp.pdf.

[15] National Center for Missing & Exploited Children. (2023). 2022 CyberTipline Reports by Electronic Service Providers (ESP). https://www.missingkids.org/content/dam/missingkids/pdfs/2022-reports-by-esp.pdf.

[16] Internet Watch Foundation. (2022). Europe remains 'global hub' for hosting of online child sexual abuse material. https://www.iwf.org.uk/news-media/news/europe-remains-global-hub-for-hosting-of-online-child-sexual-abuse-material/.

[17] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' COM(2022) 209 final (CSA Proposal), 2.

[18] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' COM(2022) 209 final (CSA Proposal), 2.

[19] Insoll, T., Ovaska, A., Vaaranen-Valkonen, N. (2021). CSAM Users in the Dark Web: Protecting Children Through Prevention. https://www.suojellaanlapsia.fi/en/post/csam-users-in-the-dark-web-protecting-children-through-prevention.

[20] Mori, C., Park, J., Racine, N., Ganshorn, H., Hartwick, C., & Madigan, S. (2023). Exposure to sexual content and problematic sexual behaviors in children and adolescents: A systematic review and meta-analysis. Child Abuse & Neglect, 143. https://doi.org/10.1016/j.chiabu.2023.106255; Bergenfeld, I., Cheong, Y. F., Minh, T. H., Trang, Q. T., & Yount, K. M. (2022). Effects of exposure to sexually explicit material on sexually violent behavior among first-year university men in Vietnam. PLoS one, 17 (9). https://doi.org/10.1371%2Fjournal.pone.0275246; Grant, H. (2023). Pornography driving UK teens towards child abuse material, say experts. The Guardian. https://www.theguardian.com/society/2023/sep/26/pornography-driving-teens-child-abuse-material-charities-police.

[21] Material provided by the UK Online CSEA Covert Intelligence Team.

[22] Vogels, E.A., Gelles-Watnick, R. & Massarat, N. (2022). Teens, Social Media and Technology 2022. Pew Research Center. https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.

[23] Thiel, D., DiResta, R. & Stamos, A. (2023). Cross-Platform Dynamics of Self-Generated CSAM. Stanford Internet Observatory, 1.2.0. https://stacks.stanford.edu/file/druid:jd797tp7663/20230606-sio-sg-csam-report.pdf.

[24] Thiel, D., DiResta, R. & Stamos, A. (2023). Cross-Platform Dynamics of Self-Generated CSAM. Stanford Internet Observatory, 1.2.0. https://stacks.stanford.edu/file/druid:jd797tp7663/20230606-sio-sg-csam-report.pdf.

[25] Thiel, D., DiResta, R. & Stamos, A. (2023). Cross-Platform Dynamics of Self-Generated CSAM. Stanford Internet Observatory, 1.2.0. https://stacks.stanford.edu/file/druid:jd797tp7663/20230606-sio-sg-csam-report.pdf.

[26] Material provided by the UK Online CSEA Covert Intelligence Team.

[27] Material provided by the UK Online CSEA Covert Intelligence Team.

[28] Material provided by the UK Online CSEA Covert Intelligence Team.

[29] Levine, A.S. (2022). These TikTok Accounts Are Hiding Child Sexual Abuse Material In Plain Sight. Forbes. https://www.forbes.com/sites/alexandralevine/2022/11/11/tiktok-private-csam-child-sexual-abuse-material/?sh=2fe9bc0a3ad9.

[30] Levine, A.S. (2022). These TikTok Accounts Are Hiding Child Sexual Abuse Material In Plain Sight. Forbes. https://www.forbes.com/sites/alexandralevine/2022/11/11/tiktok-private-csam-child-sexual-abuse-material/?sh=2fe9bc0a3ad9.

[31] Goswami, R. (2023). Facebook and Instagram content enabled child sexual abuse, trafficking: New Mexico lawsuit. CNBC. https://www.cnbc.com/2023/12/06/facebook-content-enabled-child-sexual-abuse-new-mexico-lawsuit.html.

[32] Putnam, L. (2022). Facebook Has a Child Predation Problem. Wired. https://www.wired.com/story/facebook-has-a-child-predation-problem/.

[33] WeProtect Global Alliance. (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response. https://www.weprotect.org/global-threat-assessment-23/#full-report.

[34] Internet Watch Foundation. (2023). Prime Minister must act on threat of AI as IWF 'sounds alarm' on first confirmed AI-generated images of child sexual abuse. https://www.iwf.org.uk/news-media/news/prime-minister-must-act-on-threat-of-ai-as-iwf-sounds-alarm-on-first-confirmed-ai-generated-images-of-child-sexual-abuse/.

[35] Internet Watch Foundation. (2023). How AI is being abused to create child sexual abuse imagery. https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/.

[36] United States Department of Homeland Security. (2021). Increasing Threat of Deepfake Identities. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

[37] Ajder, H., Patrini, G., Cavalli, F. & Cullen, L. (2019). The State of Deepfakes: Landscape, Threats, and Impact. DeepTrace Labs. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

[38] Murphy, M. & Bloomberg. (2023). 'Nudify' apps that use AI to undress women in photos are soaring in popularity. Fortune. https://fortune.com/2023/12/08/nudify-apps-use-ai-popularity-deepfakes/;

Montgomery, B. (2024). Taylor Swift AI images prompt US bill to tackle nonconsensual, sexual deepfakes. The Guardian. https://www.theguardian.com/technology/2024/jan/30/taylor-swift-ai-deepfake-nonconsensual-sexual-images-bill.

[39] Viejo, M. (2023). Decenas de menores de Extremadura denuncian que circulan fotos de falsos desnudos suyos creadas por inteligencia artificial: "Me dio un vuelco el corazón". El País. https://elpais.com/espana/2023-09-18/la-policia-investiga-el-desnudo-integral-de-varias-menores-en-extremadura-con-inteligencia-artificial-me-dio-un-vuelco-el-corazon.html; Hedgecoe, G. (2023). El escándalo en un pequeño pueblo de España por las imágenes de decenas de niñas y jóvenes desnudas generadas por IA. BBC News Mundo. https://www.bbc.com/mundo/articles/cz9r6792k13o.

[40] Murphy, M. & Bloomberg. (2023). 'Nudify' apps that use AI to undress women in photos are soaring in popularity. Fortune. https://fortune.com/2023/12/08/nudify-apps-use-ai-popularity-deepfakes/.

[41] Terms of service. (n.d.). Telegram. https://telegram.org/tos.

[42] Material provided by the UK Online CSEA Covert Intelligence Team.

[43] Telegram FAQ. (n.d.). Telegram. https://telegram.org/faq?setln=en#q-there-39s-illegal-content-on-telegram-how-do-i-take-it-down.

[44] How WhatsApp Helps Fight Child Exploitation. (n.d.) WhatsApp Help Center. https://faq.whatsapp.com/5704021823023684.

[45] Burgess, M. (2021). Police caught one of the web's most dangerous paedophiles. Then everything went dark. Wired UK. https://www.wired.co.uk/article/whatsapp-encryption-child-abuse#:~:text=PhotoDNA%20is%20used%20on%20WhatsApp,child%20sexual%20abuse%20in%20photos.

[46] Material provided by the UK Online CSEA Covert Intelligence Team.

[47] Material provided by the UK Online CSEA Covert Intelligence Team.

[48] Chappell, B. (2023). Video chat site Omegle shuts down after 14 years — and an abuse victim's lawsuit. NPR. https://www.npr.org/2023/11/09/1211807851/omegle-shut-down-leif-k-brooks; Goggin, B. (2022). Amazon's chat app is flooded with child sexual abuse images. NBC News. https://www.nbcnews.com/tech/tech-news/wickr-amazon-aws-child-messaging-app-sex-abuse-problem-rcna20674.

[49] Chappell, B. (2023). Video chat site Omegle shuts down after 14 years — and an abuse victim's lawsuit. NPR. https://www.npr.org/2023/11/09/1211807851/omegle-shut-down-leif-k-brooks.

[50] Goggin, B. (2022). Amazon's chat app is flooded with child sexual abuse images. NBC News. https://www.nbcnews.com/tech/tech-news/wickr-amazon-aws-child-messaging-app-sex-abuse-problem-rcna20674.

[51] Goggin, B. (2022). Amazon's chat app is flooded with child sexual abuse images. NBC News. https://www.nbcnews.com/tech/tech-news/wickr-amazon-aws-child-messaging-app-sex-abuse-problem-rcna20674.

[52] Goggin, B. (2022). Amazon's chat app is flooded with child sexual abuse images. NBC News. https://www.nbcnews.com/tech/tech-news/wickr-amazon-aws-child-messaging-app-sex-abuse-problem-rcna20674.

[53] Crisan, L. (2023). Launching Default End-to-End Encryption on Messenger. Meta. https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/.

[54] Insoll, T., Ovaska, A. (2023). Encrypted Services and Messaging Apps Are Being Used to Contact Children and Disseminate Child Sexual Abuse Material. Protect Children. https://www.suojellaanlapsia.fi/en/post/encryption-online-child-sexual-abuse-statement.

[55] Teunissen, C. & Napier, S. (2022). Child sexual abuse material and end-to-end encryption on social media platforms: An overview. Trends & issues in crime and criminal justice, (653). https://www.aic.gov.au/sites/default/files/2022-07/ti653_csam_and_end-to-end_encryption_on_social_media_platforms.pdf.

[56] Insoll, T., Ovaska, A. K., Nurmi, J., Aaltonen, M., & Vaaranen-Valkonen, N. (2022). Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. Journal of Online Trust and Safety, 1(2). https://doi.org/10.54501/jots.v1i2.29.

[57] Insoll, T., Ovaska, A. K., Nurmi, J., Aaltonen, M., & Vaaranen-Valkonen, N. (2022). Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. Journal of Online Trust and Safety, 1(2). https://doi.org/10.54501/jots.v1i2.29.

[58] WeProtect Global Alliance. (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response. https://www.weprotect.org/global-threat-assessment-23/#full-report.

[59] National Society for the Prevention of Cruelty to Children. (2023). 82% rise in online grooming crimes against children in the last 5 years. https://www.nspcc.org.uk/about-us/news-opinion/2023/2023-08-14-82-rise-in-online-grooming-crimes-against-children-in-the-last-5-years/.

[60] Radio France. 2024. Sextorsion: "Si je ne répondais pas assez vite, il me rappelait que, de toute façon, il allait tout diffuser". https://www.radiofrance.fr/franceinter/podcasts/le-zoom-de-la-redaction/le-zoom-de-la-redaction-du-mercredi-07-fevrier-2024-4478028.

[61] National Society for the Prevention of Cruelty to Children. (2020). Instagram most used platform in child grooming crimes during lockdown. https://www.nspcc.org.uk/about-us/news-opinion/2020/instagram-grooming-crimes-children-lockdown/.

[62] Instagram. (2021). Giving Young People a Safer, More Private Experience. https://about.instagram.com/blog/announcements/giving-young-people-a-safer-more-private-experience.

[63] Crisan, L. (2023). Launching Default End-to-End Encryption on Messenger. Meta. https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/.

[64] Levine, A. S. (2022). How TikTok Live became 'A strip club filled with 15-Year-Olds.' Forbes. https://www.forbes.com/sites/alexandralevine/2022/04/27/how-tiktok-live-became-a-strip-club-filled-with-15-year-olds/?sh=1cf0fdc62d78.

[65] WeProtect Global Alliance. (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response. https://www.weprotect.org/global-threat-assessment-23/#full-report.

[66] WeProtect Global Alliance. (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response. https://www.weprotect.org/global-threat-assessment-23/#full-report.

[67] WeProtect Global Alliance. (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response. https://www.weprotect.org/global-threat-assessment-23/#full-report.

[68] Material provided by the UK Online CSEA Covert Intelligence Team.

[69] Guerra, E., & Westlake, B. G. (2021). Detecting child sexual abuse images: Traits of child sexual exploitation hosting and displaying websites. Child Abuse & Neglect, 122. https://doi.org/10.1016/j.chiabu.2021.105336.

[70] Child rights by design. Digital Futures Commission, 5RIGHTS Foundation. https://childrightsbydesign.digitalfuturescommission.org.uk/.

[71] WeProtect Global Alliance. (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response. https://www.weprotect.org/global-threat-assessment-23/#full-report.

[72] Mori, C., Park, J., Racine, N., Ganshorn, H., Hartwick, C., & Madigan, S. (2023). Exposure to sexual content and problematic sexual behaviors in children and adolescents: A systematic review and meta-analysis. Child Abuse & Neglect, 143. https://doi.org/10.1016/j.chiabu.2023.106255.

[73] Insoll, T., Ovaska, A. K., Nurmi, J., Aaltonen, M., & Vaaranen-Valkonen, N. (2022). Risk factors for child sexual abuse material users contacting children online: Results of an anonymous multilingual survey on the dark web. Journal of Online Trust and Safety, 1(2). https://doi.org/10.54501/jots.v1i2.29.

[74] National Center for Missing & Exploited Children. (2023). CyberTipline 2022 Report. https://www.missingkids.org/cybertiplinedata.

[75] "The Child Victim Identification Program began in 2002 after NCMEC analysts repeatedly saw images of the same child victims in their reviews and began tracking which victims had been previously identified by law enforcement. So far, more than 19,100 children have been identified." National Center for Missing & Exploited Children. (n.d.). Child Sexual Abuse Material (CSAM). https://www.missingkids.org/theissues/csam#:~:text=The%20Child%20Victim%20Identification%20Program,19%2C100%20children%20have%20been%20identified.

[76] National Center for Missing & Exploited Children. (n.d.). Child Sexual Abuse Material (CSAM). https://www.missingkids.org/theissues/csam#:~:text=The%20Child%20Victim%20Identification%20Program,19%2C100%20children%20have%20been%20identified.

[77] National Center for Missing & Exploited Children. (n.d.). Child Sexual Abuse Material (CSAM). https://www.missingkids.org/theissues/csam#:~:text=The%20Child%20Victim%20Identification%20Program,19%2C100%20children%20have%20been%20identified.

[78] National Center for Missing & Exploited Children. (n.d.). Child Sexual Abuse Material (CSAM). https://www.missingkids.org/theissues/csam#:~:text=The%20Child%20Victim%20Identification%20Program,19%2C100%20children%20have%20been%20identified.

Suojellaan Lapsia
Protect Children

Protect Children

Protect Children is a non-governmental, non-profit organisation based in Helsinki, Finland, working globally to end all forms of sexual violence against children.

We adopt a holistic, research-based approach to address the issue from multiple angles, advocating for victims, survivors, and families; equipping children and young people with essential skills and knowledge to stay safe online and offline; developing offender-focused prevention measures; and conducting innovative research.

Learn more about Protect Children: www.suojellaanlapsia.fi/en

Authors

This report is written by Tegan Insoll, Head of Research; Valeriia Soloveva, Specialist; Eva Díaz Bethencourt, Specialist; Anna Ovaska, Deputy Director; and Nina Vaaranen-Valkonen, Executive Director.

#ReDirection

Safe Online

TECH COALITION