CyberTipline 2022 Report

The National Center for Missing & Exploited Children's CyberTipline offers the public and online electronic service providers an easy way to quickly report suspected incidents of sexual exploitation of children online.

Since the CyberTipline's inception in 1998, we have received millions of reports and reviewed hundreds of millions of images and videos of suspected child sexual abuse material **(CSAM)** in an effort to locate exploited children and help law enforcement rescue them from abusive situations. We work to disrupt the trading of child sexual abuse images and videos online and help survivors begin to rebuild their lives.

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

Published April 2023

Contents

In 2022, NCMEC's CyberTipline received **32 million** reports of suspected child sexual exploitation.

CyberTipline Reports

The CyberTipline receives reports about multiple forms of online child sexual exploitation. Reports regarding CSAM, legally referred to as child pornography, make up the largest reporting category. **Over 99.5% of the reports received by the CyberTipline in 2022 regarded incidents of suspected CSAM**

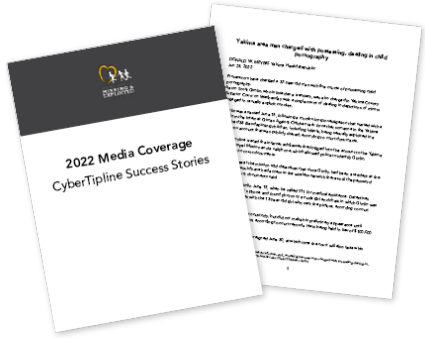
Over 99.5%
of the reports received by the CyberTipline in 2022 regarded incidents of suspected CSAM.

Categorization as selected by reporting party

Categorization of CyberTipline Reports	2020 Reports	2021 Reports	2022 Reports
Child Pornography (possession, manufacture, distribution)	21,669,264	29,309,106	31,901,234
Misleading Words or Digital Images on the Internet	8,689	5,825	7,517
Online Enticement of Children for Sexual Acts	37,872	44,155	80,524
Child Sex Trafficking	15,879	16,032	18,336
Unsolicited Obscene Material Sent to a Child	3,547	5,177	35,624
Misleading Domain Name	3,109	3,304	1,948
Child Sexual Molestation	11,770	12,458	12,906
Child Sex Tourism	955	1,624	940
Grand Total	**21,751,085**	**29,397,681**	**32,059,029**

In 2022, the category of Online enticement saw an increase of 82% from 2021 to 2022. One of the contributing factors in that growth was an alarming spike in reports of financial **sextortion**, a crime in which kids are targeted to share explicit photos and then threatened by offenders that they will share the images with the child's friends, family, or others if they don't give the blackmailer money. Several of these cases have had tragic outcomes with panicked children taking their own lives.

In previous years, sextortion offenders were more likely to target young girls with a goal of obtaining additional explicit images. In 2022, we saw a large increase in boys being blackmailed for money instead of images. NCMEC analysts have analyzed reports of financial sextortion to provide insights about the victims and offenders that can be used to create prevention resources and support law enforcement efforts to respond to these crimes.



2022 Media Coverage
CyberTipline Success Stories

Download PDF

Electronic Service Provider Reports

The CyberTipline receives reports from the public and online electronic service providers (ESPs). To date more than 1,500 ESPs are registered to make reports, and 17% of these are non U.S. based companies who voluntarily choose to report to the CyberTipline. In 2022, only 236 companies actually submitted CyberTipline reports and just 5 ESPs (Facebook, Instagram, Google, WhatsApp, and Omegle) accounted for more than 90% of the reports.

2022 CyberTipline Reports by
Electronic Service Providers (ESP)

Download PDF

In 2022, **99%** of CyberTipline reports were submitted by ESPs.

Number of reports by source

PUBLIC	ESP	TOTAL
256,504	31,802,525	32,059,029

U.S. based ESPs are **legally required** to report instances of child sexual abuse material (CSAM) or "apparent child pornography" to the CyberTipline when they become aware of them, but there are no legal requirements regarding proactive efforts to detect CSAM or what information an ESP must include in a CyberTipline report. As a result, there are significant disparities in the volume, content, and actionability of reports that ESPs submit.

For example, one company's reporting numbers may be higher because they apply robust efforts to identify and remove abusive content from their platforms.

Millions of CyberTipline reports every year, mostly submitted by a handful of companies, is evidence that what we know about the extent of child sexual exploitation online is just the tip of the iceberg. Most tech companies around the world choose not to proactively detect and report child sexual exploitation on their networks. What the CyberTipline data proves is the problem continues to grow with limited intervention by the global tech community.

Actionable & Informational Reports

NCMEC makes CyberTipline reports, including our additional analysis, available to law enforcement around the world. These efforts help law enforcement prioritize the most urgent cases allowing them to take fast action when a child is most at risk. **In 2022, NCMEC staff escalated over 49,000 reports to law enforcement as the reported incident was urgent in nature or there was information that a child was in imminent danger.**

In 2022, NCMEC escalated more than

49,000

urgent reports to law enforcement that involved a child in imminent danger.

To further assist law enforcement with prioritization, NCMEC also categorizes reports it receives from the tech industry as "actionable" or "informational." An actionable report is one where the tech company provides sufficient information for law enforcement. This typically includes user details, imagery, and a possible location. An informational report is one when the tech company provides insufficient information or where the imagery is considered viral and has been reported many times.

NCMEC designated **49%** of the reports from the tech industry as **"actionable"** when referring them to law enforcement in 2022, while **51%** of the reports made to the CyberTipline were designated as **"informational".**

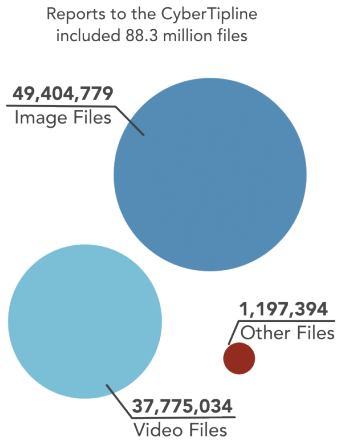
NCMEC notifies companies when their reports consistently lack substantive information. In 2022, 4% of CyberTipline reports submitted by the tech industry contained such little information that it was not possible for NCMEC to determine where the offense occurred or the appropriate law enforcement agency to receive the report. For the companies listed below, more than 90% of their reports lacked adequate, actionable information.

In 2022, ESPs submitted **49.4 million** images to the CyberTipline of which **18.8 million** (38%) were unique. Of the **37.7 million** videos reported by ESPs, **8.3 million** (22%) were unique.

CyberTipline Files

Reports made to the CyberTipline by ESPs can include images, videos and other files related to the child sexual exploitation incident being reported.

Unfortunately, child sexual abuse images and videos are often circulated and shared online repeatedly. CSAM of a single child victim can be circulated for years after the initial abuse occurred. One of the CyberTipline's critical functions is to identify unique images through the work of analysts and the use of technology.



File Review & Triage

NCMEC analysts review suspected CSAM submitted by companies and label images and videos with information about the type of content, the estimated age range of the people seen and other details that help law enforcement prioritze the reports for review. For example, tags can indicate if the imagery contains elements like violence or beastiality or if there are infants or toddlers.

After labeling these files, NCMEC's systems are able to use robust hash matching technology to automatically recognize future versions of those images and videos reported to the CyberTipline. The automated hash matching process reduces the amount of duplicative child sexual abuse imagery that NCMEC staff view and focuses analyst attention on newer imagery. This process helps ensure the most urgent CyberTipline reports where a child may be suffering ongoing abuse, get immediate attention.

NCMEC tagged more than **13.4 million** files in 2022.

Hash Sharing

Hash values are unique digital fingerprints assigned to pieces of data like images and videos. They are an important tool in the effort to stop the spread of CSAM. When a triple vetted image or video is identified as containing CSAM, NCMEC adds the hash value to a list that is shared with technology companies.

On a voluntary basis, companies can elect to use NCMEC's hash list to detect CSAM on their systems so the abusive content can be reported and removed. In 2022, fewer than 50 companies elected to access the hash lists.

In 2022, NCMEC added **1.1 million** hash values to our growing list of more than **6.3 million** hash values of known child sexual abuse material.

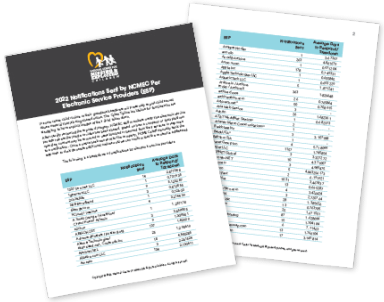
In 2022, with support from Meta, NCMEC launched a new service called Take It Down, that uses hash values to help stop the online spread of nude, partially nude, or sexually explicit images and videos taken before people were 18 years old. A user can anonymously submit these hash values to NCMEC to be shared with ESPs who voluntarily participate in the Take It Down initiative. To learn more about this service and see the participating platforms, visit **Takeitdown.NCMEC.org**.

In 2022, the average take-down time following a NCMEC notification for image or videos was **less than 2 days.**

Removal Notices & Tracking

In some cases, the reports about imagery of child sexual exploitation online are made by the child victims, their guardians/caregivers, or INHOPE member hotlines from around the world. For those reports, the CyberTipline can be a lifeline for families by notifying the platforms to review and remove the explicit images of the child.

NCMEC staff review the reported imagery and if it falls in one of the three categories below, a notification is made to the ESP where the image or video is located:



2022 Notifications Sent by NCMEC Per ESP

Download PDF

CSAM

Child sexual abuse material which may violate federal and/or state law or a company's Terms of Service, or Member Services Agreement or Community Guidelines or Standards.

Exploitative

Exploitative content which depicts identified child victims, but the images themselves may not reach the legal threshold of child sexual abuse material. Examples of this are images or videos that may contain nudity, non-pornographic content originating from child sexual abuse material or otherwise sexually suggestive content of identified child victims.

Predatory Text

These notices may contain text that is related to sexually predatory comments or personal information about an identified child victim or CSAM survivor. Personal information identifying the child in the image/video may pose safety concerns for the child or survivor.

Based on a company's Terms of Service, imagery may be removed or users blocked in response to a notification.
Once a notice has been sent, NCMEC staff manually track the status and will generate additional notices until the content is addressed.

Of the **32 million** reports that the CyberTipline received in 2022, **89.9%** resolved to locations outside the U.S.

Global Response

The federal statute 18 USC 2258A requires U.S. companies to report to the CyberTipline if they become aware of suspected CSAM on their platforms and servers. Because these companies have users worldwide and those incidents are reported to NCMEC, by extension the CyberTipline serves as a **global clearinghouse.** In fact, most CyberTipline reports, 89.9% in 2022, involve the upload of child sexual abuse material by users outside of the U.S.

Most CyberTipline reports of CSAM include indicators of where the files were uploaded. It is important to note that country-specific numbers may be impacted by the use of proxies and anonymizers. In addition, each country applies its own national laws when assessing the reported content. These numbers are not indicative of the level of child sexual abuse in a particular country.

2022 CyberTipline Reports by Country

Download PDF

Because of the global nature of these crimes, NCMEC has forged partnerships with law enforcement in 150 countries and territories that receive CyberTipline reports, including Interpol and Europol. Interpol also assists in the dissemination of CyberTipline report information to certain countries where NCMEC doesn't have a direct connection to law enforcement.

NCMEC staff also provide CyberTipline trainings in other countries, mentor NGOs seeking to expand technical and operational capacities within their own hotlines, educate on best practices, and share child safety and prevention material around the world. We collaborate with dozens of global NGOs, including WeProtect, ECPAT, International Justice Mission (IJM), Internet Watch Foundation, the Canadian Centre for Child Protection, UNICEF and many others. NCMEC is also a founding member of INHOPE, a global network of 50 member hotlines across six continents.

Case Management Tool

With 90% of CyberTipline reports resolving internationally, it's imperative that there is a referral system in place enabling a global response to CyberTipline reports. The NCMEC Case Management Tool (CMT), developed with financial support from OJJDP and Meta, enables NCMEC to securely and quickly share reports with law enforcement around the world.

The CMT allows law enforcement in the U.S. and abroad to receive, triage, prioritize, organize and manage CyberTipline reports. Through robust and customizable data display, dashboards and metrics, law enforcement users can tailor their report queue for more immediate triage and better response. It also helps police agencies refer reports to other law enforcement agencies for a more targeted response. The system helps NCMEC notify law enforcement of high priority reports.

In support of easier adoption and use by international users, the Case Management Tool fields and interface are available in eight languages (English, Spanish, French, German, Portuguese, Arabic, Hindi, Thai) with additional translations planned. Domestically all Internet Crimes Against Children task forces, the Federal Bureau of Investigation and Homeland Security Investigations also have access.

OJJDP CyberTipline Report

In consultation with the Office of Juvenile Justice and Delinquency Prevention (OJJDP) NCMEC prepared this additional transparency report regarding CyberTipline activity in 2022. It is a complimentary resource to the report on this page and contains some additional detail about the reports made to the CyberTipline in 2022.

2022 NCMEC/OJJDP Transparency Report

Download PDF

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

Every child deserves a safe childhood.

If you suspect child sexual exploitation, please make a report at CyberTipline.org or call NCMEC at 1-800-THE-LOST (1-800-843-5678).

NCMEC.org/cybertiplinedata