hotline.ie

Your Voice Matters

Help us stop repeat victimisation by reporting

Annual Report 2023

CONTENT WARNING: Please be aware, the content enclosed in this publication relates to illegal content online, such as child sexual abuse and exploitation. Thus, some readers may find parts of this Annual Report uncomfortable or upsetting to read. The publication aims to raise awareness and inform. Whether you've been following these topical issues for years, or you are just beginning to learn more, this is an active conversation that requires consistent and ongoing attention and collaboration, together with long term strategic commitment from national Governments and the European Union.

The views expressed in this publication are those of the author and do not necessarily reflect those of our members, supporters, partners or the European Union.

©2024, Internet Service Providers Association of Ireland(ISPAI). All rights reserved. Hotline.ie is a registered business name of ISPAI (registered company no. 285632, not-for-profit). All third-party logos and trademarks are property of their respective owners and are used with permission. This publication may be saved and print copies may be made as needed for personal, research and other non-commercial use. The publication may also be quoted and cited as follows: Hotline.ie. (2024). Hotline.ie 2023 Annual Report. Dublin, Ireland

Co-funded by
the European Union

hotline.ie

Your Voice Matters

Help us stop repeat victimisation by reporting

Report now

Visit our secure and confidential web-reporting portal

hotline.ie/report

Learn more

Follow us on

x.com/Hotline_ie

Resource

webwise.ie

For further online safety advice, tips, and resources checkout the Webwise Parents Hub or Webwise Teachers Hub

Listen
DOCUMENTARY

Listen to:

Age, Sex, Location

RTÉ Radio 1 Documentary

44 MINS

Available on Spotify, Apple Podcasts, or play.acast.com

If you would like to learn more about Hotline.ie's work in an international context, the importance of cross-disciplinary and cross-border collaboration, we invite you to listen to a 44-minute radio documentary. In this sensitively made documentary you will hear accounts from a survivor of child sexual abuse, Hotline.ie and IWF Analysts, and a Detective in the Online Child Exploitation Unit of An Garda Síochána.

Whilst we are acutely aware that child sexual abuse and exploitation is an extremely sensitive and difficult topic, it can no longer be deemed as too sensitive or taboo to discuss in polite society. The cost of not knowing might be immense.

A list of other Irish support services to help you in your search for information is available at www.hotline.ie

A thank you from all the Hotline.ie team

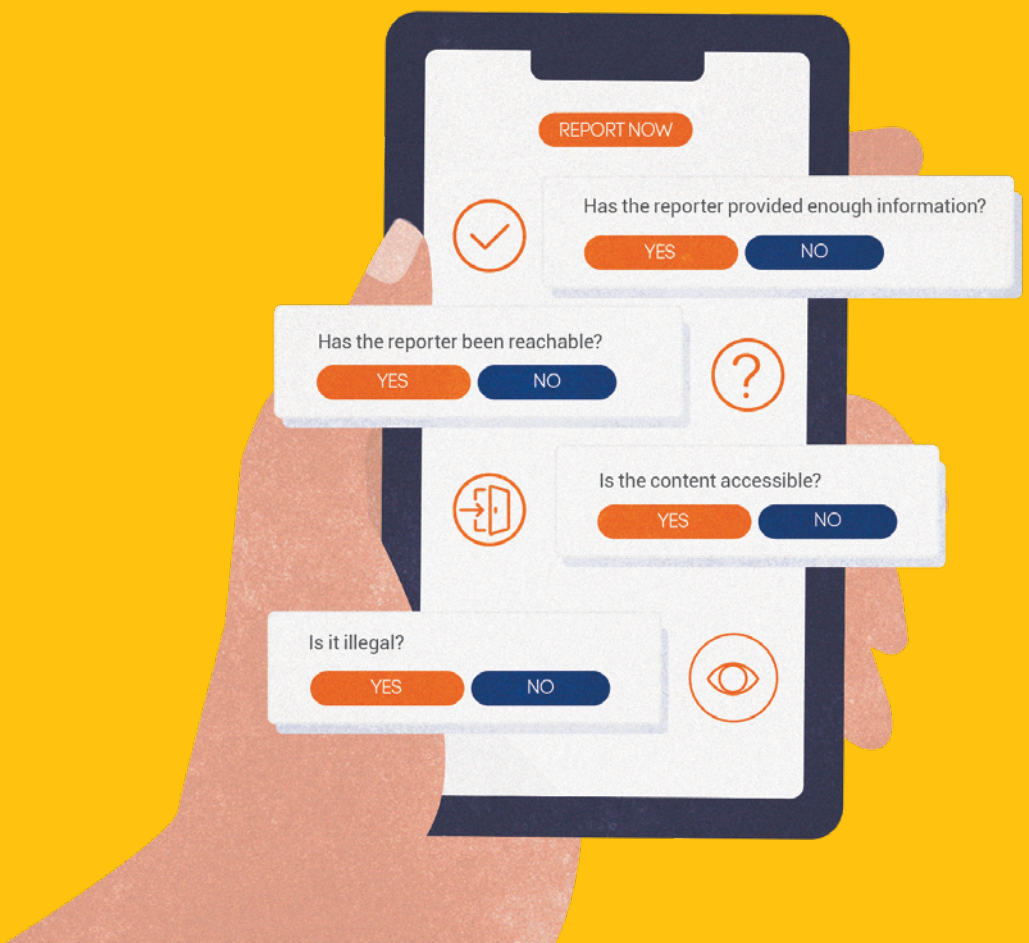
The team at Hotline.ie would like to express our appreciation to those who have taken the proactive step of reporting suspected illegal content online. Thanks to your actions we are actively able to safeguard those who are vulnerable or have been harmed, particularly children and young people.

We also want to thank our collaborators in this field, including our national partners, sister hotlines worldwide, An Garda Síochána, and the broader global child protection community.

Furthermore, we are immensely thankful to our members and the European Commission, whose co-funding facilitates and enables Hotline.ie to operate, and undertake our vital work.

Your continued and unwavering support and faith in our efforts is truly invaluable.

Sincerely, the team at Hotline.ie



Foreword Minister for Justice

Hotline.ie completed another year of its important, worthy and difficult work in 2023. It continues to provide a vital pathway for members of the public to report suspected illegal content online - particularly child sexual abuse material (CSAM) - securely, confidentially and anonymously.

Helen McEntee T.D., Minister for Justice

Hotline.ie has been carrying out its crucial work to combat the scourge of online child sexual abuse and other forms of abuse for almost a quarter of a century, operating to the highest professional standards in partnership with An Garda Síochána.

This Government continues to focus on building stronger and safer communities, including by making online safety a priority. Advancing technologies mean we have new and, often sophisticated, ways to commit crime. Working with partners like Hotline.ie, we continue to adapt how we respond to and support vulnerable victims.

The data in the 2023 Annual Report makes for often stark reading and it is, of course, vital to acknowledge that behind each case is a vulnerable victim, often a child, who has suffered.

Hotline.ie received some 40,543 public reports last year, the highest number ever and a 30% increase on 2022. While it is truly shocking to see year-on-year increases, the fact that public engagement with the service continues to grow must be welcomed.

Of the suspected illegal material, analysts determined 29,906 reports to be illegal across Hotline.ie's remit (child sexual abuse material, intimate image abuse, racism and xenophobia, and financial scams). Of the 29,906 URLs flagged, only 362 remain active - a hugely impressive removal rate.

The vast majority of reports overall – more than 38,000 – relate to suspected child sex abuse material, with some 29,044 assessed by the analysts at Hotline.ie as relating to child sexual abuse. This is a significant increase on 2022.

> Each report can involve anything from a single image to thousands of images and videos. Each image is a crime. These are abhorrent acts, and we must never become hardened to these figures.

My Department and I remain steadfastly committed to tackling these horrific crimes. Sexual exploitation of children is an extremely serious offence and there is comprehensive legislation in place to deal with it. Ireland is also fully committed to playing an active role in negotiations on new EU laws that will require online service providers to deal with child sexual abuse material, and attempts to groom children, on their platforms.

The 2023 Hotline.ie Annual Report also includes statistics on intimate image abuse (IIA), or the non-consensual sharing of intimate images and videos. It is coming up on three years since - on the back of 'Coco's Law' - my Department partnered with Hotline.ie to make reporting IIA easy and accessible. Once illegal content is reported to Hotline.ie, their experts assess and decide on next steps, including getting the content removed.

In 2023, Hotline.ie identified 470 intimate image reports related to publicly shared images or videos. Some 95% were successfully taken down, with the remaining 5% in the process of being removed. This removal rate is encouraging, particularly as all the content was hosted outside of Ireland.

Up to the end of 2023, there had been 349 prosecutions (charges/summons) in relation to 254 incidents under Coco's Law (The Harassment, Harmful Communications and Related Offences Act 2020).

Hotline.ie also continues to play a key role in combatting scams and xenophobia. Some 89 fraudulent websites were removed last year, while almost 130 reports of suspected racism or xenophobia were made - with 37% relating to hate speech. These figures show that, in our digitised world, the threats are varied, and constant vigilance is required.

Finally, I would like to thank the team at Hotline.ie for their unwavering support and dedication to our shared mission.

Reporting to Hotline.ie is a choice to use your voice to protect victims

Hotline.ie/report

Welcome from the Chair of the Board of Hotline.ie

Welcome to the Hotline.ie 2023 Annual Report. 2023 has been a significant year for the company in many ways, but throughout the many events and changes, the dedicated staff continued their critical work.

Brian Nisbet Chair of the Board of Hotline.ie

As the number of reports received by Hotline.ie continues to rise, a 30% increase on 2022 to over 40,000 reports, the vital nature of the service remains clear. Whether the report is in relation to child sexual abuse and exploitation, non-consensual intimate images, racism and xenophobia, or financial scams, each one of those reports represents a victim in need of support. Thinking about the reality of the victims and perpetrators is frequently uncomfortable, but as a society we must confront our discomfort and collectively work to protect and support the victims, remove the criminal content from the Internet and reduce the opportunity for the crimes to be committed.

As the Internet continues to evolve, we need to continue to evolve as a society and change our way of thinking. For instance, we believe that the national conversation around intimate image abuse has changed for the better and that those whose images are shared online are victims, but there is still substantial work needed with each new generation and technology to continue that positive evolution.

In 2023 99% of the material reported to Hotline.ie was removed and none of what remained was hosted in Ireland. However, even that 1% is too much and shows that there is more work that needs to be done on the borderless Internet to help those most in need of protection.

Hotline.ie would like to thank our members, and the other ISPs and hosting providers with whom we work, for their cooperation and rapid reaction to reports. The work we do has to be reflected in these actions and there is no such thing as an "acceptable" amount of time for the images, URLs or other material to stay online.

It is only through collaboration that both this work and progress can be made. Hotline.ie is part of the international INHOPE network of hotlines and global cooperation with them, with law enforcement and with other relevant groups is vital. In Ireland we continue to work closely with An Garda Síochána and the Department of Justice, along with the other members of the Irish Safer Internet Centre.

On a more administrative, but important, level 2023 saw Hotline.ie adopt a new company constitution and governance improvements. This is ongoing work, and we hope to engage more with our members to continue to ensure the company can perform its crucial work. As part of the AGM which brought in these changes, I was honoured to be reappointed as Chairperson of the Board.

Sadly, I must also note the departure of two longstanding and core members of Hotline.ie staff.

Siobhan Coyle worked tirelessly on so many parts of the day-to-day operations of the company and her calm and highly organised approach to finance, HR and so many other matters will be greatly missed.

Ana Niculescu, who was Hotline.ie's CEO, was the driving force at the heart of the company during her tenure. She worked with the staff and the Board to continuously improve what Hotline.ie could do for those in need and her leadership has put the hotline in the strong position it is in today.

On behalf of the Board, I would like to express my deep gratitude to Ana and Siobhan and wish them well.

With more legislative changes on the horizon and a new CEO in 2024, there will certainly be challenges to face in the near future. My confidence in the staff, my fellow Board members, and our partners and stakeholders, is strong and I have no doubt Hotline.ie will continue to evolve and to be there to help those who need it.

In 2023 99% of the material reported to Hotline.ie was removed and none of what remained was hosted in Ireland

Contents

INTRODUCTION 1-4

1 About Hotline.ie
2 Call it for what it is
3 Journey of a report
4 What to report

STATISTICS & FINDINGS 5-8

6 Context and the dataset
7 Statistics & findings

ONLINE CHILD SEXUAL ABUSE & EXPLOITATION 9-23

10 Know the law
11 Statistics & findings
13 The children in the imagery
14 CSAM findings and insights
15 Hotline.ie Analyst insight
16 Services misused for CSAM distribution
18 Comparative analysis
19 Hotline.ie Analyst insight
20 Snapshot of CSAM hosting patterns
22 Hosting insights
23 Hotline.ie Analyst insight

INTIMATE IMAGE ABUSE 24-33

25 Know the Law
26 What is intimate image abuse?
27 How can Hotline.ie help?
28 Statement of purpose
30 Those impacted by IIA
31 IIA site types
31 Outcome sought by the reporter
32 Sexual extortion scams
33 Signposting

FINANCIAL SCAMS AND RACISM & XENOPHOBIA 34-38

35 Findings & insights
36 Identifying and avoiding financial online scams

PARTNERSHIPS 39-43

40 Building partnerships for tangible impact
41 Working in partnership for good
43 Our members

44 Glossary of terms

hotline.ie

Your Voice Matters

Help us stop repeat victimisation by reporting at Hotline.ie/report

About Hotline.ie

Hotline.ie is the Irish centre of expertise combatting illegal material online. We are a not-for-profit organisation working in close collaboration with law enforcement, the Irish Government, tech companies, NGOs and others, to make the internet a safer and more inclusive place for children, young people, and adults alike.

We have been providing people residing in Ireland with a secure and confidential web-reporting portal since 1999 and the victim centred vision we began with is still at the heart of all we do. The team at Hotline.ie never loses sight of the fact that behind every report there's a real person, real harm and real suffering.

Our web-reporting portal remains distinct and independent from any specific law enforcement agency or online service provider's reporting channels. This allows us to handle reports across a wide variety of online services and platforms, recognising the diverse ways in which illegal material is shared, accessed, and spread.

Our commitment is driven by the understanding that the impact of this material can haunt abuse victims for a lifetime. We strive to combat the misuse of digital mediums and ensure a safer online environment for all.

At the heart of Hotline.ie's work is a dedicated team of compassionate and resilient staff members, who possess extensive expertise, having received police training and international certification, ensuring every report received is meticulously assessed against rigorous standards and in accordance with Irish law.

Partnership approach

Global problems such as child sexual abuse and exploitation require global solutions and, that is why Hotline.ie has been an integral part of a multifaceted European and international ecosystem, working collaboratively with a diverse mix of stakeholders, since inception.

Hotline.ie's operational procedures are approved and overseen by the Department of Justice, and we work closely with An Garda Síochána and our members. Hotline.ie are members of InHope and the Irish Safer Internet Centre.

How we are funded

We are a not-for-profit and our work is co-financed by the European Union through grant aid and by our members, who are tech companies, search providers, mobile operators, hosting, and internet service providers. Our resources are finite, and we encourage others to play their part whether by reporting suspected illegal content online to hotline.ie/report, funding us, or collaborating on the development of best practices, tech, and research.

The team at Hotline.ie works relentlessly to:

Reduce the prevalence of illegal material

Break the cycle of abuse

Prevent repeat-victimisation

Call it for what it is

We use the terms “child sexual abuse material” (CSAM) and “child sexual abuse imagery” (CSAI) to accurately convey the severity and nature of the images and videos we assess daily. These terms challenge any notion that crimes against children can be committed with the consent of a child (under the age of 18).

Under Irish law (The Child Trafficking and Pornography Act, 1998), the term “child pornography” is used to describe such materials. However, we refrain from using this term as it can imply a level of legitimacy or consent that is completely inappropriate in the context of child sexual abuse. Instead, we use the terms CSAM or CSAI to ensure that the language reflects the gravity of the crime and the reality of the abuse suffered by these children.

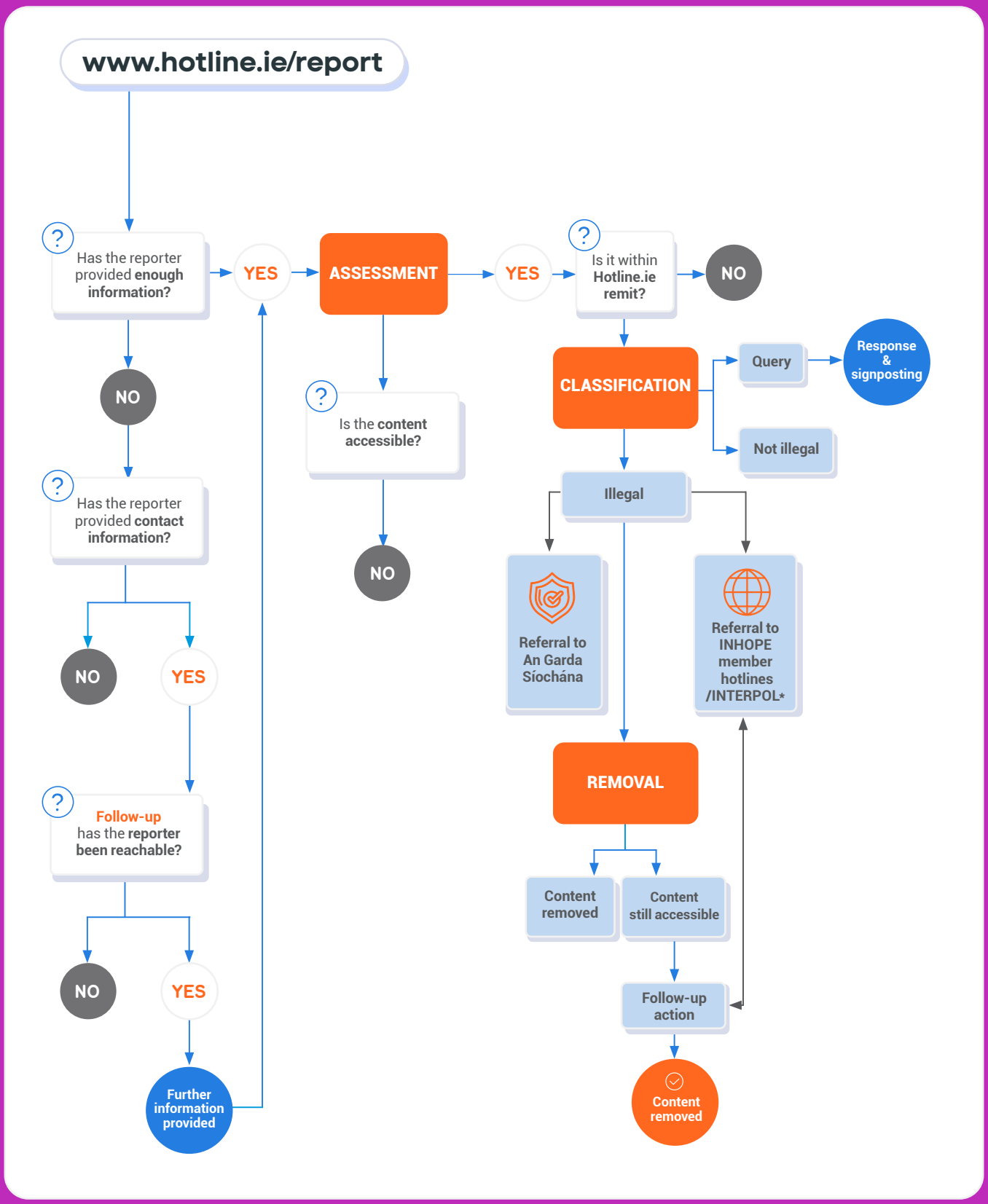
The use of these terms is also outlined in the Luxembourg Terminology Guidelines, which provide guidance to individuals and agencies working to prevent and eliminate all forms of sexual exploitation and abuse of children. These guidelines help ensure a better understanding and use of the various terms and concepts encountered in their work.

The need for the Terminology Guidelines arose from a growing concern that changes to existing terms, particularly established legal terms, could lead to confusion or misunderstanding and even hinder the effective prevention and elimination of child sexual exploitation (Luxembourg Terminology Guidelines). Hereinafter, we will use the term “child pornography” when specifically referring to the legal definition. Otherwise, we will use the terms CSAM or CSAI.

> The imagery I assess every day is a record of the horrific abuse suffered by a child. In most cases, these children are younger than 12 and subjected to a level of physical and psychological abuse that is sometimes beyond comprehension. I urge you to consider this message while you read our report or when raising awareness of these crimes against the most vulnerable in society. Avoid and reject the use of terms that would trivialise the abuse suffered by child sexual abuse victims and survivors. Call it for what it is – child sexual abuse – and in doing so challenge the normalisation of such crimes against children.

Eoin, Hotline.ie Analyst

The journey of a report



* This step only applies to reports classified by Hotline.ie Analysts as CSAM, and especially important when the material is hosted outside Irish jurisdiction

What to report

Hotline.ie only handles reports referring to suspected illegal content encountered online. Urgent situations where persons may be in immediate danger should always be directed to An Garda Síochána.

You can securely, anonymously, and confidentially report to Hotline.ie incidents involving the following:

- **Child sexual abuse material (images, video, text, computer generated material)**
- **Activities related to the sexual exploitation of children, such as child grooming**
- **Intimate image abuse (non-consensual sharing of intimate images and videos)**
- **Racism or xenophobia**
- **Financial scams purporting to be Irish services or have Irish contact details, appearing to have originated from Ireland**

Why report?

Reporting to Hotline.ie is a choice to use your voice to protect victims, and any potential future victims, from the direct and secondary harm caused by illegal material shared online. It's the right thing to do, and it only takes a minute.

Your report will be confidentially handled by a team of professionals who have the necessary expertise, technology and procedures in place so that illegal material is removed at source and law enforcement are notified through the most efficient channels.

If you have any doubt of whether the content you saw is illegal we still urge you to report it to us, our analysts are trained to identify illegal content and can direct you to any support service you may need

Statistics & Findings

40,543

total reports

submitted to Hotline.ie in 2023.
A 30% increase in the number of reports from the previous year.

Context and the dataset

The Hotline.ie annual report aims to highlight the challenges and achievements in tackling illegal content, primarily the online distribution, availability, and proliferation of child sexual abuse and exploitation, intimate image abuse, racism and xenophobia, and financial scams that target Irish residents.

It provides an overview of the important work we carry out for the benefit of all society, outlines key statistical findings from the year gone by and contextualises our work and contribution to European and international efforts to combat illegal material online.

While the figures and findings included in this report make for uncomfortable reading, we hope it sheds light on some difficult topics which should no longer be deemed too sensitive or taboo to discuss in, particularly when the cost of not knowing might be immense.

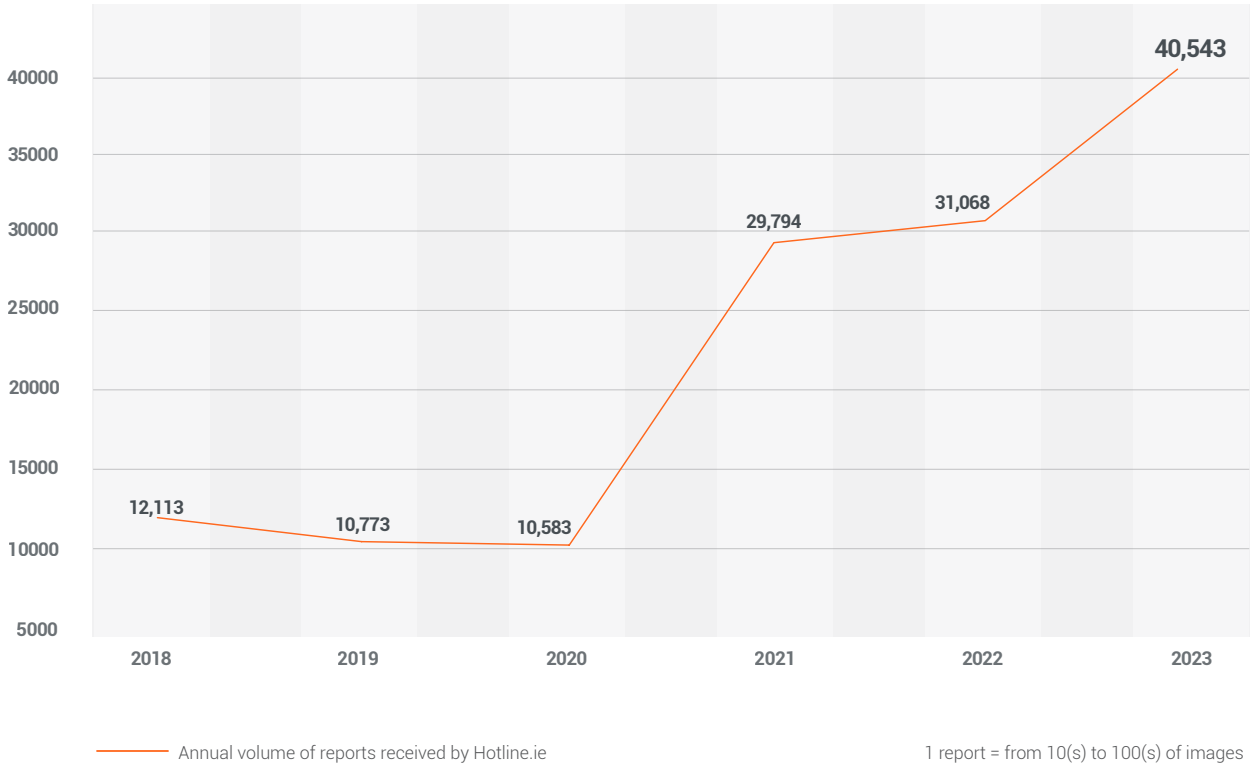
The dataset, unless otherwise specified, refers to the period from January 1st to December 31st, 2023.

The figures and findings included in this publication are predicated on reports received from the public by Hotline.ie. Under current operational procedures, approved by the Department of Justice and An Garda Síochána, Hotline.ie is not mandated to proactively search for child sexual abuse material (CSAM) on the internet. However, when we receive a public report and there is evidence suggesting further illegal content is being linked to on other websites, we will investigate. If further illegal content is accessible or displayed on those other websites, we will derive a report and action it.

The percentages are rounded to the nearest whole number.

Statistics & findings

Annual volume of reports received by Hotline.ie



Total reports received and actioned by Hotline.ie between 2018-2023

134,874
Total reports

22,479
Annual average

2018-2023
Received and actioned by Hotline.ie

There were 40,543 reports made to Hotline.ie in 2023, representing the most demanding year in the history of the service with roughly ten thousand more reports submitted than 2022. The chart above displays the general trend of increasing reports in recent years.

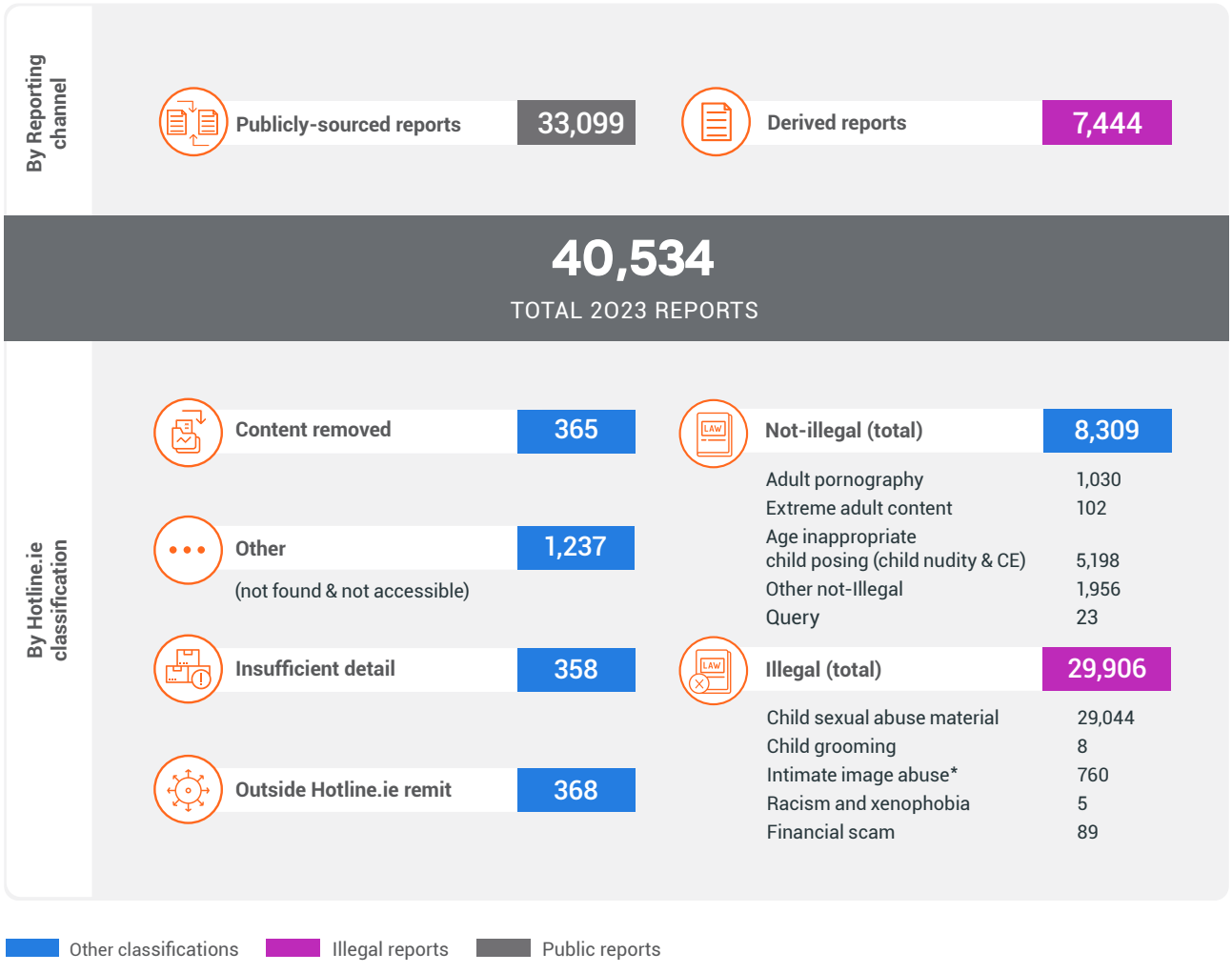
Although a stark increase, the numbers alone do not paint the complete picture. Reports submitted to Hotline.ie are dynamic in nature, across and even within the categories of material the hotline acts upon. A report can be a link to a single piece of content or a link to an entire chain of websites hosting hundreds to tens of thousands of images or videos.

Each of these reports are diligently assessed by a team of expertly trained analysts against the suspicion they were reported under and classified with respect to Irish law.

Hotline.ie analysts classified 29,906 reports as relating to illegal material. This represents 72% of the total which is a significant increase compared to just under half in 2022. This continues an ongoing trend of more and more potentially illegal material being accurately reported by members of the public.

Of the 8,309 reports that were determined to be not illegal 60% were related to child sexual exploitation that did not meet the threshold for child sexual abuse material under Irish law. While this material is not illegal, it is still harmful, placing a child in a sexually exploitative context and as such Hotline.ie acts to remove this material where possible.

Breakdown of reports



* Reports classified as insufficient detail, outside Hotline.ie remit, not accessible, and not found are termed "non-actionable reports" because our analysts cannot identify, access, or confirm the content. The "outside Hotline.ie remit" classification covers issues like copyright infringement or sale of drugs. "Content already removed" is used when a webpage shows that the content has been deleted, and our analysts cannot verify its legality under Irish law.

Online Child Sexual Abuse & Exploitation

38,435

suspected CSAM reports

29,044 were assessed as child sexual abuse material, referred to law enforcement and actioned for removal by Hotline.ie. 99.6% of assessed CSAM removed at source.

HELP US STOP REPEAT VICTIMISATION BY REPORTING AT **HOTLINE.IE**

Know the law

Child sexual abuse material is illegal under the Child Trafficking and Pornography Act 1998 as amended by the Criminal Law (Sexual Offences) Act 2017. Technology facilitated child sexual exploitation (child grooming) is also covered under a number of offences in the Criminal Law (Sexual Offences) Act 2017.

- Engaging in any sexual acts with a child under the age of 17 **is a crime.**
- **It is an offence** to knowingly produce, distribute, disseminate, print, publish, import, export, advertise, sell, supply, or make available child sexual abuse material, legally called "child pornography".

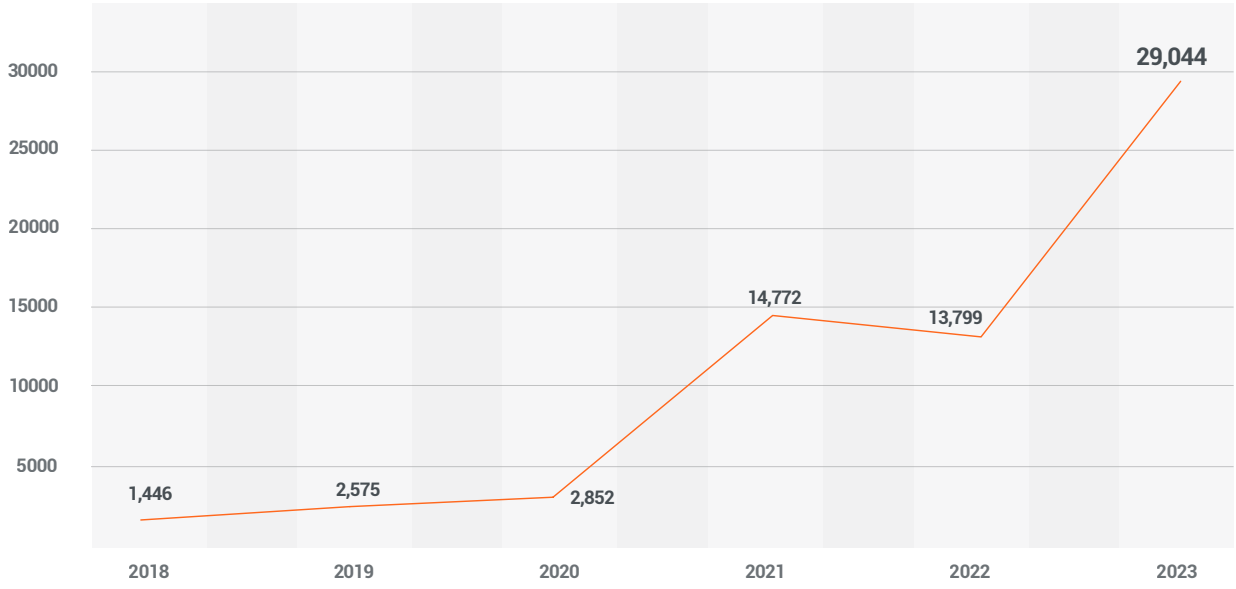
Did you know?

"Child pornography" is defined as **any visual representation** that shows a person who is or is depicted as being a child and who is engaged in or is depicted as being engaged in **real or simulated sexually explicit activity.**

- **It's a crime** to send sexually explicit images, videos or messages to a child under the age of 17.
- **It's a crime** to expose a child to sexually explicit acts or to pornography.

Statistics & findings

2023 volume of reports classified as child sexual abuse material



Total CSAM reports received and actioned by Hotline.ie between 2018-2023

64,488
Total reports

10,748
Annual average

2018-2023
Received and actioned by Hotline.ie

In 2023, there was an 110% increase in the amount of child sexual abuse material (CSAM) identified by Hotline.ie analysts. Of the 38,435 reports of suspected CSAM in 2023, 29,044 of them were determined to lead to child sexual abuse material compared to 13,799 in 2022. The increase is in line with reported global trends[1] and will likely continue in future based on the consistent increases shown over the last five years.

All Hotline.ie's reports are publicly sourced and as such the CSAM that is identified is reflective of the CSAM that is generally accessible to people. The numbers above are only a small slice of the amount of CSAM that is in circulation, either in publicly accessible locations on the internet, private locations on apps, or the vast quantities known to be shared on the dark web. However, by acting to remove the CSAM reported to us we safeguard people from further harm by dealing with the content people are most likely to stumble upon accidentally.

Hotline.ie seeks the removal of CSAM that is hosted in Ireland and any CSAM that can be accessed by Irish residents that is hosted in international locations. Hotline.ie works with over 50 other hotlines globally as part of the INHOPE network to achieve this, however there are many countries that do not have a hotline and, in these cases, Hotline.ie takes direct action to remove CSAM. Irish law is expansive when it comes to what is defined as 'child pornography', in many jurisdictions, particularly outside of the EU, there can be significant differences which can present a challenge when analysts are attempting to have material removed. Despite this, 99.6% of the CSAM reported to Hotline.ie in 2023 has been removed.

Online child sexual abuse material could include but are not limited to:

- Videos or images depicting a child in sexually explicit poses
- Content displaying non-penetrative or penetrative sexual activity involving children
- Non-photographic content depicting sexual abuse of a child, such as cartoons or digitally generated imagery
- Stories describing the sexual abuse of a child

[1] https://www.inhope.org/EN/articles/inhope-annual-report-2023

The children in the imagery

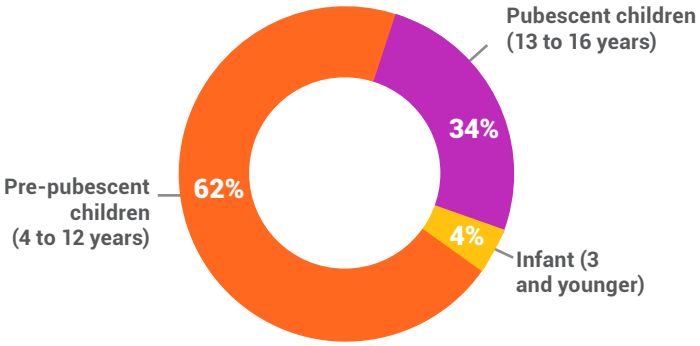
Gender breakdown

5% Boys

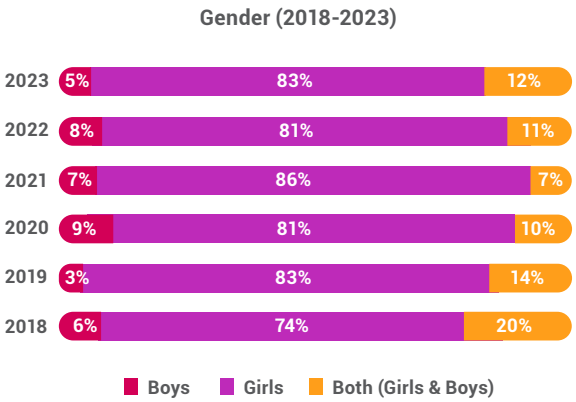
83% Girls

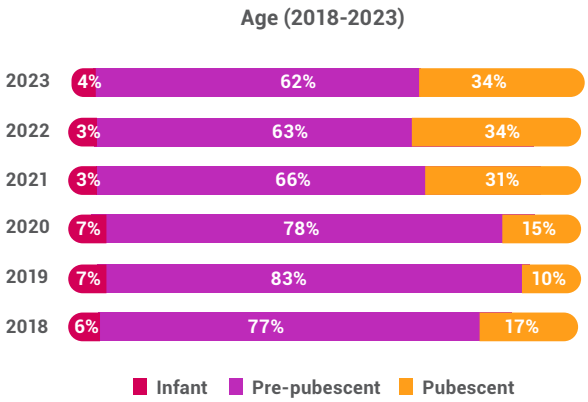
12% Both (girls & boys)

Age breakdown



Comparative analysis





CSAM findings and insights

> The way CSAM is shared online is constantly changing. There are always new methods of distribution, new types of material and new technology threatening to change the whole space. To keep up with this we need to monitor trends and be adaptable, we can't afford to rely on any one solution because it could all change overnight.

Sean, Senior Content Analyst

Self-generated CSAM

Self-generated CSAM are images or videos that a child appears to have taken themselves. These are usually produced using smartphone cameras or webcams and can either be a product of consensual sharing to other children or be the result of coercion by adults.

4,322 of the CSAM reports to Hotline.ie involved self-generated CSAM. This marks a 280% increase from the previous year and highlights a significant issue in children being sexually exploited after sending images or videos. 57% of the material displayed preteen children and 43% were in their early teens, 97% were female.

The reports primarily related to forums that were dedicated to sharing this type of material with evidence indicating that adults had groomed or coerced children into sexual acts on video and recorded them. There is often a clear financial aspect to the sharing of this material, with screenshots from the videos used to promote the material while the actual video is locked behind private payment.

The term self-generated CSAM only denotes that an analyst has identified the material as most likely being created by the child. It does not apportion blame to the child who has been sexually exploited.

Computer generated CSAM

Computer generated CSAM refers to material depicting children engaged in explicit sexual activity created using digital art tools. It can range from simple "hand-drawn" style cartoons to AI-generated imagery featuring photorealistic children. It also refers to material that has being digitally altered in some manner, such as face swapping or clothes removal through a nudify app.

One in ten CSAM reports in 2023 were found to contain computer generated images. While a 44% decrease from the previous year, Hotline.ie analysts have noted that the imagery is becoming more and more realistic and nearly impossible to distinguish from real imagery. With how rapidly the technology is improving, the use of AI to aid in digitally editing photos and in the generation of images is of real concern.

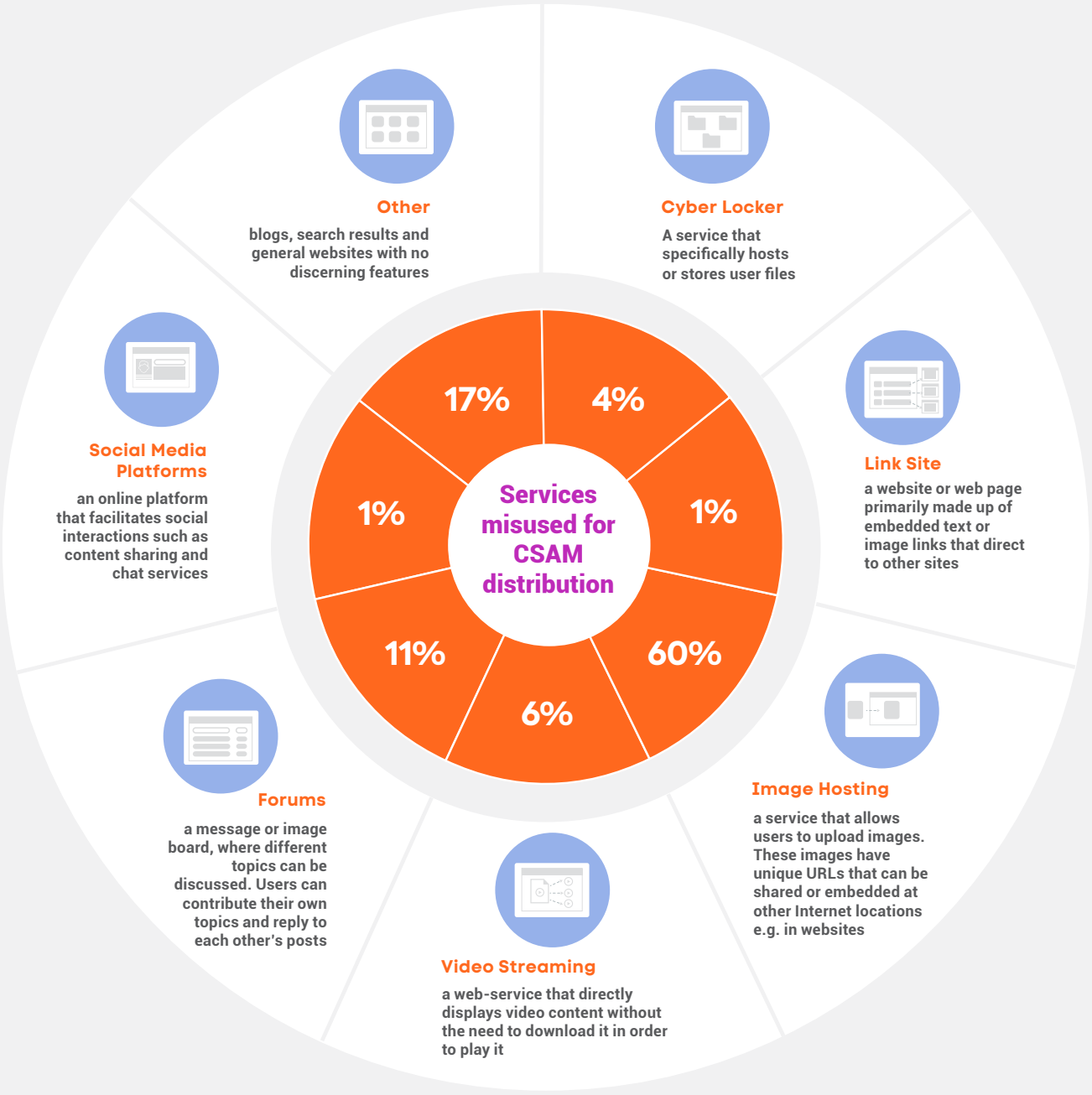
Hotline.ie Analyst insight

"The spamming of links to CSAM sites on social media is becoming concerningly widespread. Over the last couple of years, a new type of site has been seen that encourages people viewing child sexual abuse material to invite others by sharing the link to get a reward. This reward comes in the form of unlocking more material to view, the more people that use their link the more material they gain access to, it is like a game to these people without any consideration for the children who are the victims.

The growing concern surrounding such sites is how accessible and easy it is for the public to find whether that be on purpose or by accident. Young people who use social media daily are being exposed to these links and viewing Child Sexual Abuse Material involuntarily.

These sites are something we see every day and the concept is something that is hard for even us to comprehend. By acting in a timely manner, we can remove the content from these websites so that the public do not unintentionally witness such harrowing content.

Sarah, Senior Content Analyst



Disclaimer: The figures above show the resources misused to share CSAM based on Hotline.ie's public reports, as such they do not represent the full scope of CSAM distribution on the Internet.

Services misused for CSAM distribution

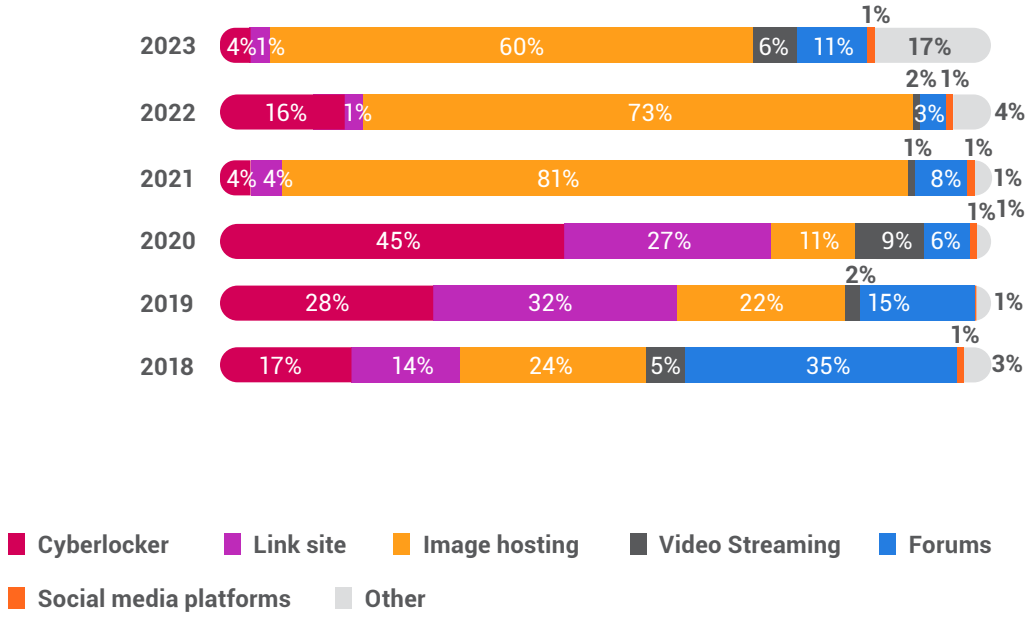
Most CSAM reports submitted to Hotline.ie concern publicly accessible Internet services. While some efforts are made to hide CSAM behind innocuous websites or using coded terminology, it is also commonly displayed openly depending on the service being misused. The majority of these reports involve small-to-medium platforms that are either dedicated to sharing CSAM or vulnerable to being misused for this purpose. Only one percent of the CSAM reported to Hotline.ie in 2023 was related to large social networking sites.

Different Internet services often inter-operate to facilitate the distribution of CSAM. For example, forums and message boards may use external image hosting sites to store and share illicit content, while file-sharing services (cyberlockers) can distribute larger volumes of CSAM. Links to these image hosts and file-sharing services are often posted on forums or chat platforms, creating a network of interconnected services that aid in the dissemination of CSAM.

Additionally, CSAM is distributed on the dark web, through private or encrypted channels, and via peer-to-peer networks. Hotline.ie analysts frequently encounter evidence of this interconnected distribution network. However, these services are more difficult to access and less likely to be stumbled upon accidentally, leading to fewer reports and underrepresentation in this report's figures. This complexity highlights the ongoing challenge in combating the distribution of CSAM across various online platforms.

CSAM is distributed on the dark web, through private or encrypted channels, and via peer-to-peer networks

Comparative analysis



In line with past years, CSAM was mostly found distributed on image-hosting services, with nearly two out of every three reports classified as CSAM related to their use.

There are many reasons why image hosts are used to distribute CSAM, firstly they're easy to use with simple ways to upload images and minimal or no personal information needed to do so, secondly many don't engage in proactively removing material and rely on requests from users, hotlines or law enforcement, and thirdly the images can be embedded into other webpages or linked to from anywhere, ensuring that the images will stay live if the primary website is removed.

There was a slight decrease in the proportion of CSAM shared on image-hosts compared to 2022, with more CSAM seen on video streaming services and forums. The rise in forums directly corresponds with the increase in self-generated CSAM seen by the hotline in 2023. The forums reported to the hotline were mostly dedicated to the sharing of this material, with any one of them possibly displaying tens of thousands of these images.

A significant rise in 'other' websites compared to previous years was also seen, this can largely be attributed to the rise of simple CSAM sites that incentivise their sharing by providing access to more CSAM through a referral scheme. These are categorised as 'other' as they are clearly distinguishable from other types of websites.

Hotline.ie Analyst insight

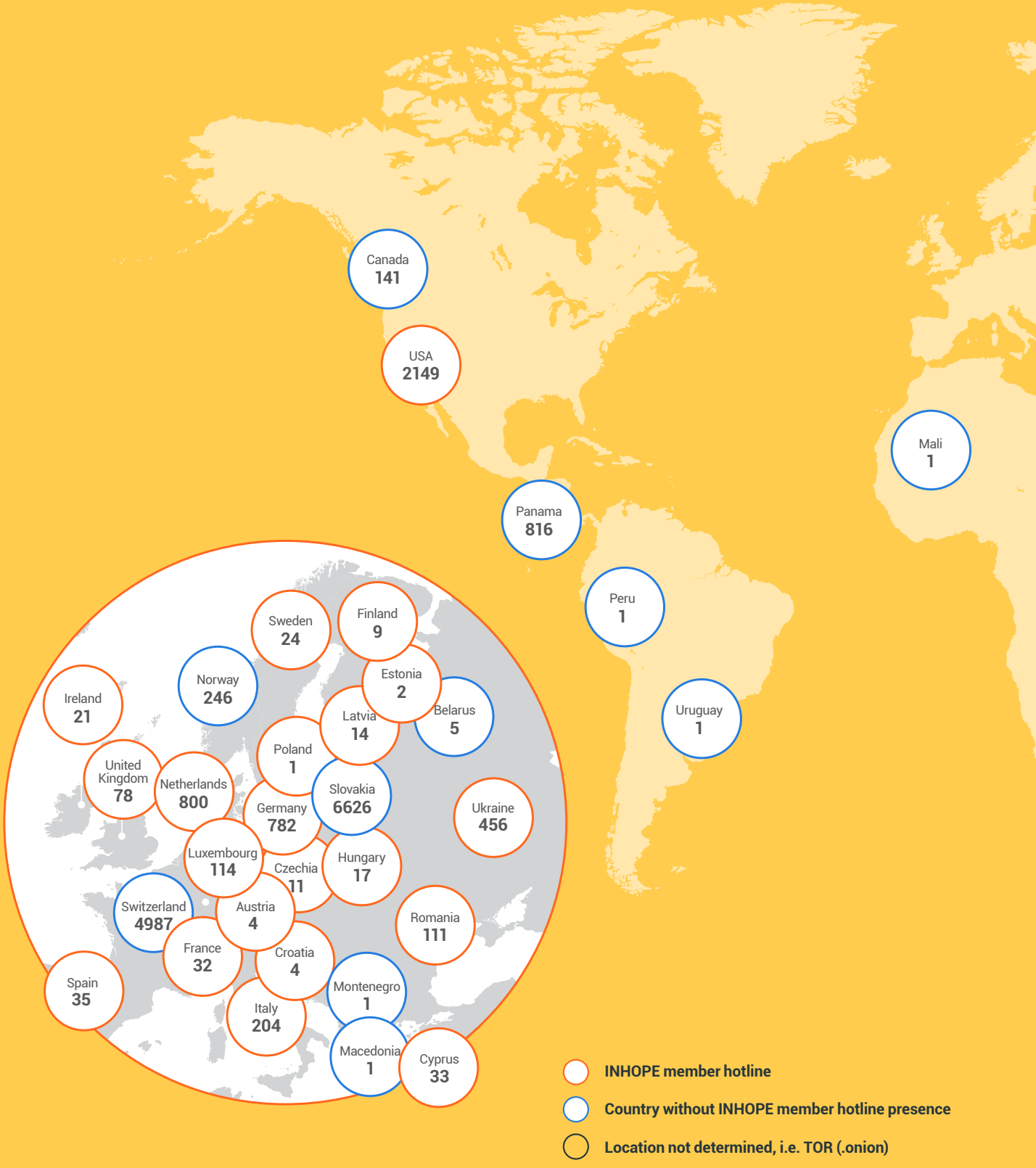
"We're seeing more CSAM being distributed through semi-private platforms like messaging apps, where users can join hidden groups. Access is often gained through links shared in forums or on social media. Once inside these groups, the content can spread rapidly. Because these spaces are more closed off, they make it harder for the public to accidentally come across the material, which means we receive fewer reports about this type of distribution.

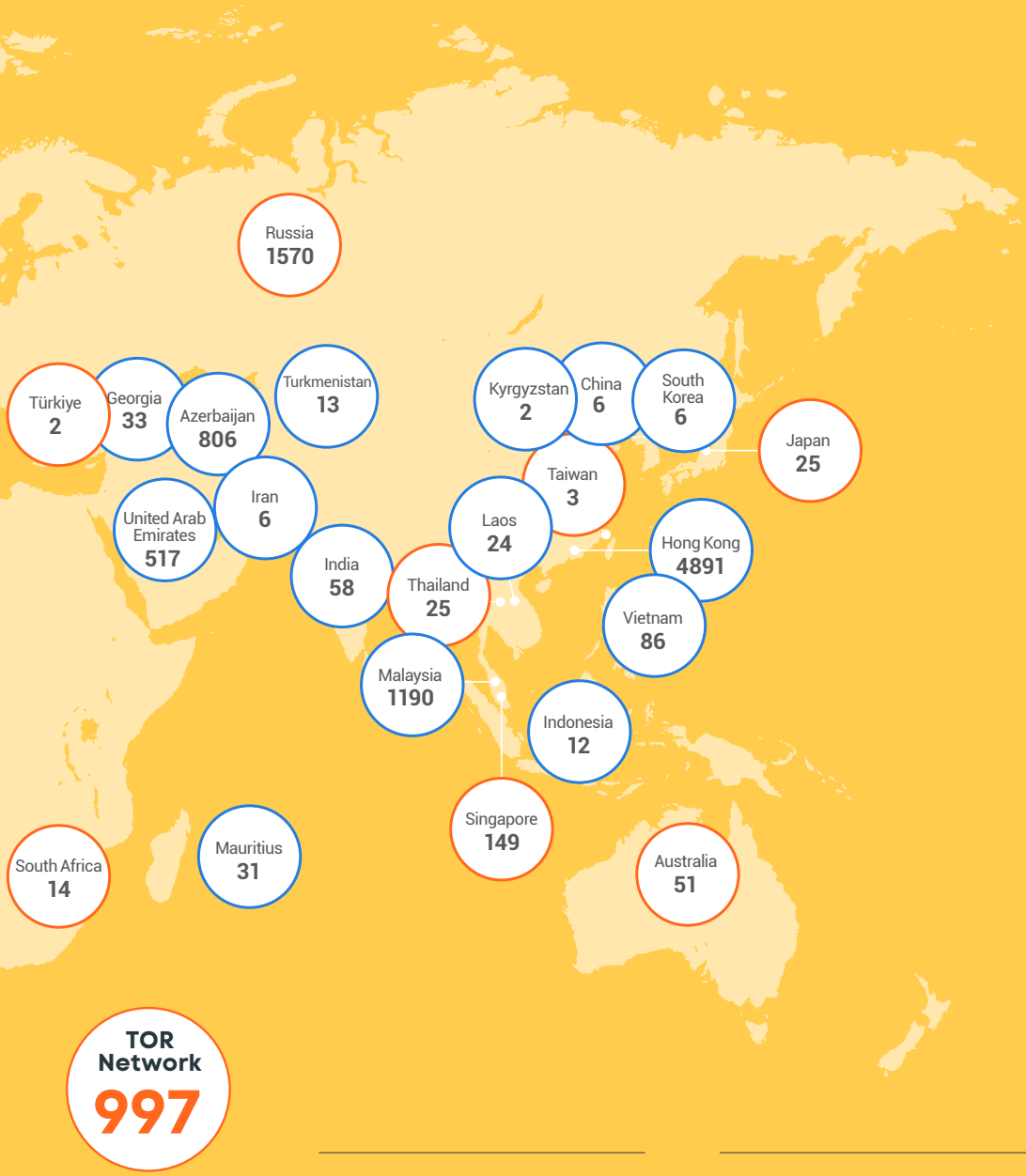
One challenge we face is that we can't proactively search for CSAM in these semi-private networks. This limits our ability to address the content early, leaving us reliant on reports from users who may only come across it by chance. By the time these reports reach us, the material has often been circulated extensively within the group.

Some platforms have taken steps to address this issue, improving their detection and removal systems. However, these semi-private groups remain a significant concern. The cross-platform element also seems to pose a challenge for moderation, a link that might look innocuous on one platform can pass undetected by automated detection tools, however it could be leading through several steps to illegal imagery hidden on another platform. This is one of the reasons why the human element is still so valuable in the fight against CSAM, a human can bring nuanced understanding and contextual judgment that automated systems cannot yet fully replicate.

James, Senior Content Analyst

Snapshot of CSAM hosting patterns





28,047
TOTAL REPORTS

997
1.6% LOCATION NOT DETERMINED (TOR NETWORK)

56
COUNTRIES COVERED

31%
OF ALL CSAM WAS HOSTED IN EU

Hosting Insights

In 2023, CSAM was traced to 56 different countries. This is twelve more than 2022 and the greatest number on record. This could be indicative of a wider distribution of CSAM or due to the greater number of confirmed CSAM cases reported to Hotline.ie.

Nineteen of the fifty-six were countries in the European Union and accounted for nearly a third of all confirmed CSAM. However, 22% of this was traced to image-hosting services operating in Slovakia.

Out of the top ten countries, which 79% of CSAM was traced to, only the USA (7%) and Russia (5%) had hotlines that were members of the INHOPE network, despite 30 of the total 56 countries having hotline representation. The role of hotlines is shown to be vital in creating and maintaining hostile online environments to child sexual exploitation and abuse.

There were 21 incidents of confirmed CSAM hosted in Ireland, with an average removal time of less than a day from the time that Hotline.ie received the report. The number of confirmed cases of CSAM hosted in Ireland remains low year to year, with a drop from 34 incidents in 2022.

Note: Distribution patterns are only a snapshot in time, and indicative of where the CSAM was hosted on the internet and not an indication of the level of CSAM production, consumption, or commercialisation within any one jurisdiction.

Hotline.ie Analyst insight

"It's a really difficult thing to talk about. Even working here, dealing with child sexual abuse material daily, the words don't come easily. It's something that a lot of people would prefer to ignore. I think anyone can understand or relate to that, it's horrific beyond imagination, it's easier to pretend it doesn't exist. But unfortunately ignoring it isn't helping anyone. We need to be able to talk about this openly and not turn away when it matters.

I can't commend enough the people who report CSAM to us, it would be so easy to click or swipe away the content, but they go to the effort to make sure something is done about it. I hope they truly understand the potential impact that making that report could have, preventing it from being seen by anyone else, stopping a child from being re-victimised, or even it leading to a child being identified and rescued by law enforcement.

The good news is I think things are changing, there are conversations happening now that weren't happening even five years ago. Society as whole is taking more responsibility for harms in online spaces. Hopefully this translates to more people reporting what they see when they see it.

Sean, Senior Content Analyst

Intimate Image Abuse

95%

successful cross-border removal rate

36% of reports of intimate image abuse were of sexual extortion scams.

HELP US STOP REPEAT VICTIMISATION BY REPORTING AT **HOTLINE.IE**

Know the law

- **The non-consensual sharing of intimate images or videos (intimate image abuse) is an offence** under the Harassment, Harmful Communications and Related Offences Act 2020 (also known as Coco's Law).

- **An intimate image of a person under 18, in certain circumstances, could constitute child sexual abuse material,** which is an offence under the Child Trafficking and Pornography Act 1998 as amended by the Criminal Law (Sexual Offences) Act 2017.

It is illegal to take or share an intimate image of someone without their consent

Did you know?

- **Even if a person gives consent** for an intimate image to be taken **it is still an offence** if it is subsequently shared without their consent.

- Even if someone **doesn't mean to intentionally cause harm** by sharing an intimate image or video without the person's consent **it is still an offence under the act.**

- **Digitally altered images** purporting to be of an individual, such as a person's face photoshopped onto another's body, can classify as intimate images abuse under the act.

- **"Upskirting" or "downblousing"** meaning the taking of photographs without a person's knowledge or consent, either from below their skirt or down their blouse, is an offence under Coco's law.

What is intimate image abuse?

The Harassment, Harmful Communications and Related Offences Act 2020 (Coco's Law) defines an intimate image in relation to a person as any visual representation made by any means including any photographic, film, video, or digital representation.

Examples of intimate imagery that could constitute intimate image abuse (IIA):

- **a person, for example, an ex-partner shares an intimate image of you on social media without your consent.**
- **a person digitally alters (Photoshops) an image of you with a sexually explicit image and shares it without consent.**
- **a person posting your intimate image/video on an adult website without your consent.**

In general terms "consent" is when a person agrees or gives unambiguous permission to another person to do something. Consent should be expressed freely, voluntary, and informed. In any given situation there should be room for the person consenting to say no and/or to change their mind.

Before Coco's law came into force in February of 2021, the act of sharing an intimate image wasn't an offence on its own.

Words matter, call it for what it is

Intimate image abuse is sometimes colloquially referred to as "revenge porn", however we strongly urge against the use of this term as it does not adequately capture the very nature and cause of this type of abuse.

This term is misleading as it:

- **implies the person responsible for sharing the intimate image without the victim's consent is a former partner that may have been wronged – while people who share intimate images without consent do so for many reasons and some may not even know the victim.**
- **implies the victim has done something wrong and deserves "revenge" – but no one deserves to experience this form of abuse.**
- **liken the images to legal adult pornography in which adults have given expressed, voluntary, and informed consent.**

Anyone can experience intimate image abuse. IIA is more common that one might think, it impacts people no matter their age, gender, ethnicity, socioeconomic background.

If this happens to you, remember that it's not your fault. You are not alone. There are supports available to help you cope with what has happened

How can Hotline.ie help?

Over the past year, Hotline.ie has made significant strides in providing crucial support to people affected by intimate image abuse (IIA).

- **Reporting and removal of non-consensual intimate images**

  Hotline.ie's web-reporting portal enables safe and confidential reporting and removal of intimate images shared without the person's consent.

- **Collaboration with the Garda National Protective Services Bureau (GNPSB)**

  Hotline.ie's collaboration with An Garda Síochána has been instrumental in dealing with cases where victims of IIA seek to have the matter investigated by law enforcement. By liaising with the GNPSB, we have provided a bridge between victims and the appropriate investigative authorities, ensuring that legal measures can be taken and justice pursued.

- **Signposting**

  Recognising the importance of comprehensive support, Hotline.ie has been proactive in providing referrals to relevant resources and support services available in Ireland. We understand that people affected by intimate image abuse often require specialised assistance, guidance, and counselling. By connecting them with trusted Irish organisations and services, we hope that all reporters get the support they need on their journey to healing.

- **Resources**

  Hotline.ie has continued to enhance its informative resources, particularly through the Intimate Image Abuse (IIA) Frequently Asked Questions (FAQ) section. This dedicated resource aims to provide an overview of key issues and terminology related to intimate image abuse.

- **Autonomy and comprehensive reporting, minimising re-victimisation**

  Hotline.ie offers comprehensive reporting to minimise re-victimisation. Collaborating with law enforcement and tech companies while maintaining independence, our web-reporting portal allows direct reporting from anywhere in the digital world. Victims can submit one report referencing multiple sources, sparing them from reliving abuse across various platforms.

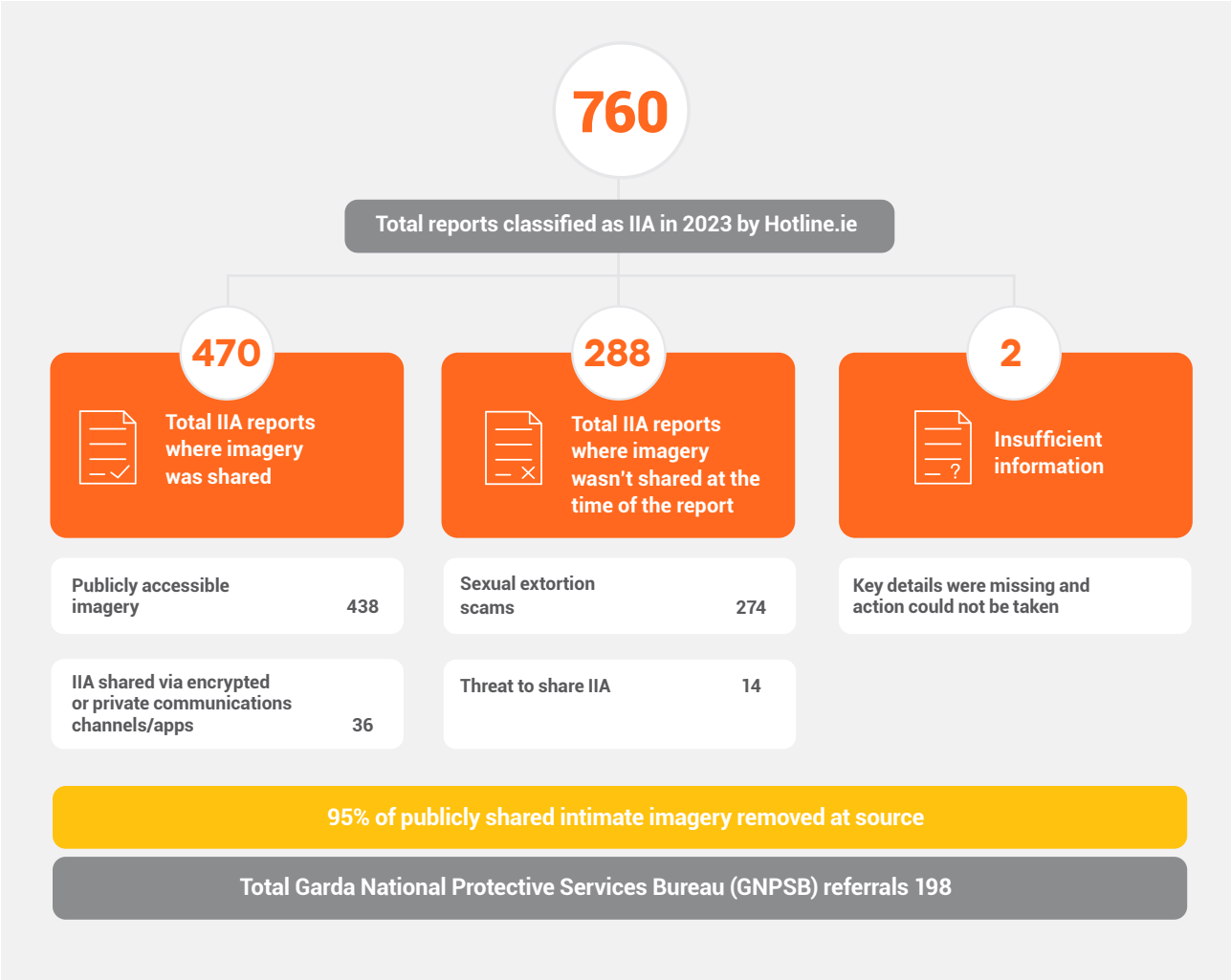
- **Handling complex cases**

  Hotline.ie's dedicated team of analysts possess extensive experience in addressing various forms of abuse. In cases involving under 18s, our analysts are well equipped in identifying instances that may qualify as child sexual abuse material or technology-facilitated child sexual exploitation, as opposed to IIA. We have long been at the forefront of handling such cases, our analysts have the expertise to navigate appropriate processes, procedures, and law enforcement channels effectively.

Statement of purpose

By outlining key trends and insights, we aim to raise awareness of intimate image abuse and the harm it can cause, as understanding the risks and consequences empowers people to navigate the digital landscape safely and be aware of their responsibility in keeping themselves and others safe. While malice certainly plays its role in intimate image abuse, it is also likely that a significant amount of people who share intimate images without consent might not realise the level of real harm inflicted, or even think about the consequences of their actions at all.

IIA Breakdown of reports



A report can receive multiple actions predicated on the outcome sought by the reporter and/or specific context e.g. removal, referral to AGS and signposting to other support services available in Ireland.

IIA are only forwarded to An Garda Síochána at the request of the reporter, unless the reporter is under the age of 18.

In 2023, Hotline.ie received 915 reports under the suspicion of Intimate Image Abuse (IIA) with 760 of these assessed and classified as IIA in accordance with the Harassment, Harmful Communications and Related Offences Act 2020. This is an increase from 689 reports confirmed as intimate image abuse in 2022.

470 IIA reports were from people who had their intimate images shared without their consent and wanted them removed. 92% of these had been shared in public online spaces where anyone could see their images, the remaining 8% related to imagery that had been shared without their consent through private messenger either peer to peer or in group chats. The number of images and videos shared are not currently captured by Hotline.ie and should not be conflated with the number of reports which only reflects the direct link an individual has submitted to be investigated.

Of all reports that were publicly shared, 95% were successfully taken down, a slight decrease from the 96% removal rate in the previous year. None of the content was found hosted on Irish services, while this is positive sign it means that the content was hosted in countries with different legal frameworks, many of which do not have laws prohibiting the non-consensual sharing of intimate images. This can present a challenge when seeking the removal of content and can mean that there may always be an unfortunate proportion of material that will not be removed until the laws in the jurisdictions change. Despite this, Hotline.ie continues to seek the removal of the remaining 5%. Furthermore, delisting requests have been sent to search engine providers to ensure any search results for this non-consensually shared material does not return any result, making it difficult to find.

The most significant increase from 2022 was the sharp rise in sexual extortion scams. There were 274 individuals who contacted Hotline.ie in 2023 who had fallen victim to sexual extortion scams. Nine out of ten were male, and 18% of were under the age of 18, with another 51% in the 18-24 age category. 99% of the sexual extortion scams were carried out through social media, often moving from one social media platform to another. A key component of these scams is gaining access to a 'friends' or 'followers' list that the scammer can threaten to share the intimate images to.

Partly due to the high number of sexual extortion scams, 63% of the total IIA reports submitted were from those as male, in stark contrast to 2022 where 85% of reporters were female. However, even when taking sexual extortion scams into account, 57% of the reporters as female, meaning a significant increase in the number of males reporting intimate imagery that had been shared publicly without their consent.

Throughout 2023, 198 intimate image abuse reports were referred to Garda National Protective Services Bureau (GNPSB), nearly four times the amount as the previous year. 63% of reporters sought to have their reports referred to the Gardaí, a significant increase from 11% in 2022. This is likely due to the increase in sexual extortion scams, as cases where content had been shared publicly, only 17% of reporters wished it to be forwarded to the Gardaí.

In 2023, Hotline.ie received 915 reports under IIA suspicion, with 760 of these assessed and classified as IIA

Those impacted by IIA

Gender breakdown

BASED ON THE REPORTER'S DISCLOSURE

35% Female

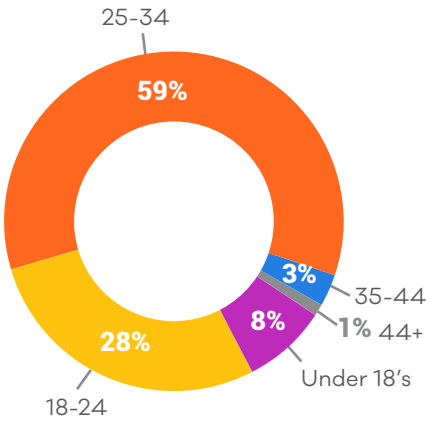
63% Male

2% Gender Diverse

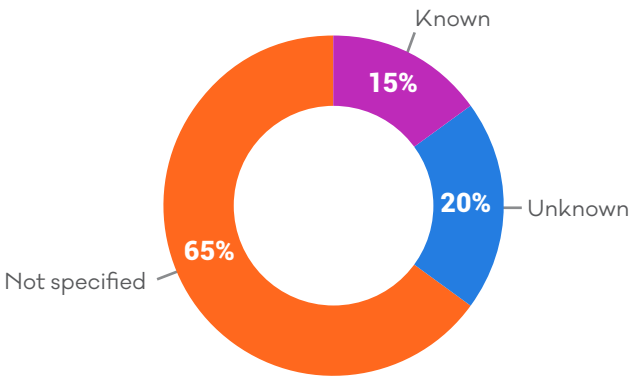
<1% Prefer not to say

Age breakdown

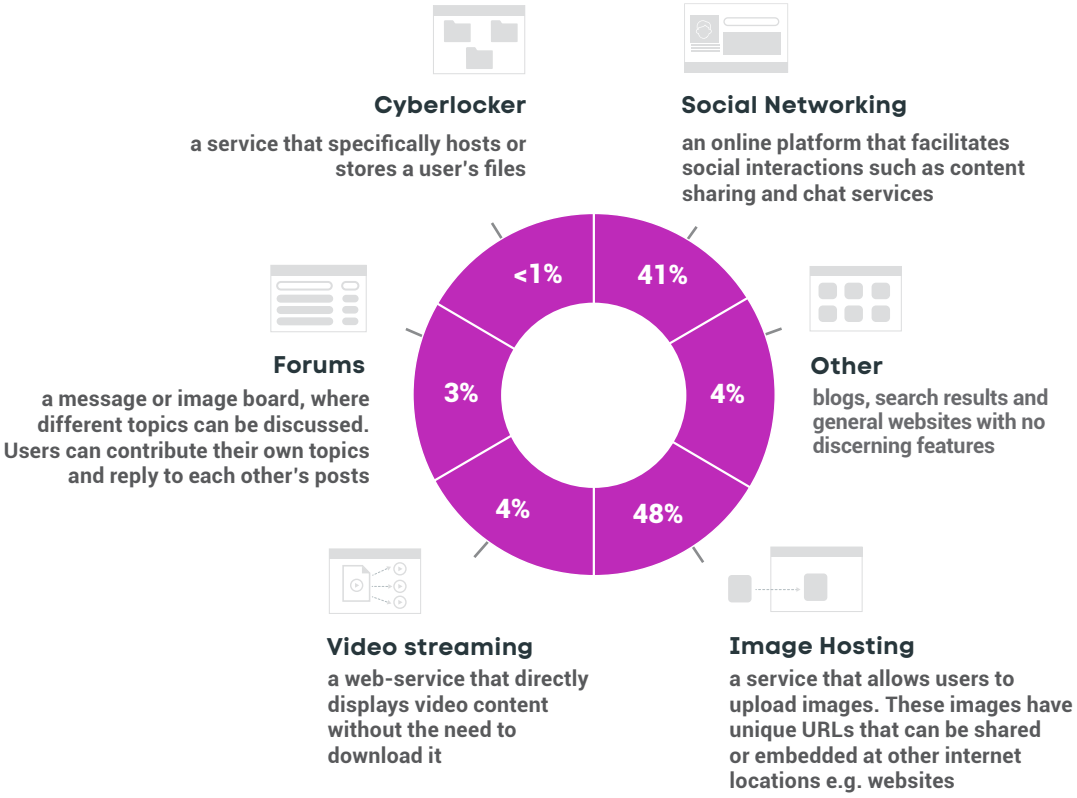
BASED ON THE REPORTER'S DISCLOSURE



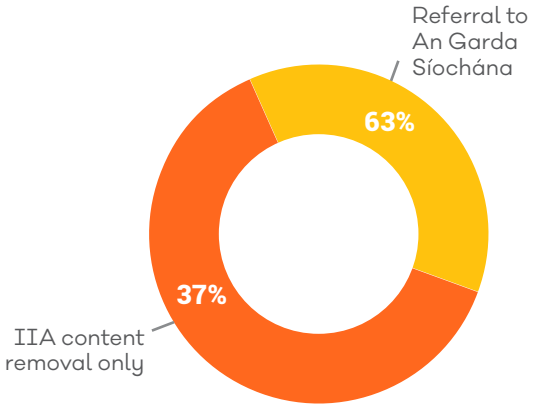
IIA perpetrator



IIA site types - where the imagery was found



Outcome sought by the reporter



Sexual extortion scams

The rise in sexual extortion scams is a global issue, not one localised to Ireland. Perpetrators of these scams operate individually or as part of criminal networks and are usually based in countries with no legal frameworks for this type of abuse or have lax cybercrime regulations. They may employ virtual private networks (VPNs), proxy servers, or other anonymisation techniques to hide their IP addresses.

What is it

Sexual extortion scams come in a variety of forms, but the most common type involves the scammer deceiving a person and enticing them into sending intimate images, which they then use to blackmail them by threatening to send them to family and friends.

What to look out for

- **A person you've never met in person contacts you online.**
- **The conversation quickly escalates sexually.**
- **They ask for your public social media accounts to try to gain access to your friends or family.**
- **They ask you to send nudes or go on a video chat to engage in sexual acts, making sure your face is visible.**
- **They send nudes themselves to create trust.**
- **They promise that no screenshots will be taken or can be taken (screens can always be recorded).**

The scams appear to operate across any websites with capability to send private messages, however Hotline.ie has received reports relating to Snapchat, Instagram, Facebook, Ome.tv, Reddit, and Kik. In most cases, it occurs cross platforms.

What to do

It's natural to feel overwhelmed or distressed when you are being blackmailed, and the pressure can be immense. Anyone can experience intimate image abuse, and it is important to remember that it's not your fault.

Hotline.ie recommends to following next steps

- **Try not to panic.**
- **Do not pay.**
- **Screenshot your conversations.**
- **Block and stop all contact.**
- **Report them to the online platform.**
- **Make all social media private or temporarily disable accounts.**
- **Report it to the Garda National Protective services Bureau at any Garda Station and to Hotline.ie.**
- **Talk to someone you trust about it.**

Perpetrators care primarily about money. The less time and effort invested in the extortion scam, the more likely they are to move on and not risk their accounts being banned by sharing intimate imagery. Unfortunately, however, there is never a guarantee that the intimate imagery won't be shared.

Signposting

Anyone can experience intimate image abuse. If this happens to you, remember that it's not your fault and you are not alone!

Intimate image abuse can have significant consequences upon your wellbeing. Fortunately, there are support services available in Ireland to help you cope with what has happened. To name a few:

Women's Aid/ Too Into You offers support to women affected by abuse, and advocates for justice and social change. It operates a 24 /7 national freephone confidential helpline. The helpline has fully accredited and specialised trained staff. **A telephone interpretation service facility covering 170 languages is also available.**

Women's Aid also offers an instant message support service, in addition to one-to-one support.

Website: www.womensaid.ie
Freephone: 1800 341 900
Email: helpline@womensaid.ie

Mens Aid Ireland is the only dedicated national service supporting men and their families experiencing domestic violence including coercive control. Men's Aid also offer counselling support to help you navigate through difficult situations. They have professionally trained counsellors and therapists who specialise in domestic violence trauma and family issues.

Website: www.mensaid.ie
Confidential national support line: 01 5543811
Email: hello@mensaid.ie

Rape Crisis Network Ireland is a specialist information and resource Centre on rape and sexual violence. RCNI have dedicated expert and specialist resources to support a wide programme of work for justice for victims of sexual violence.

Website: www.rcni.ie
Crisis Help: www.rapecrisishelp.ie

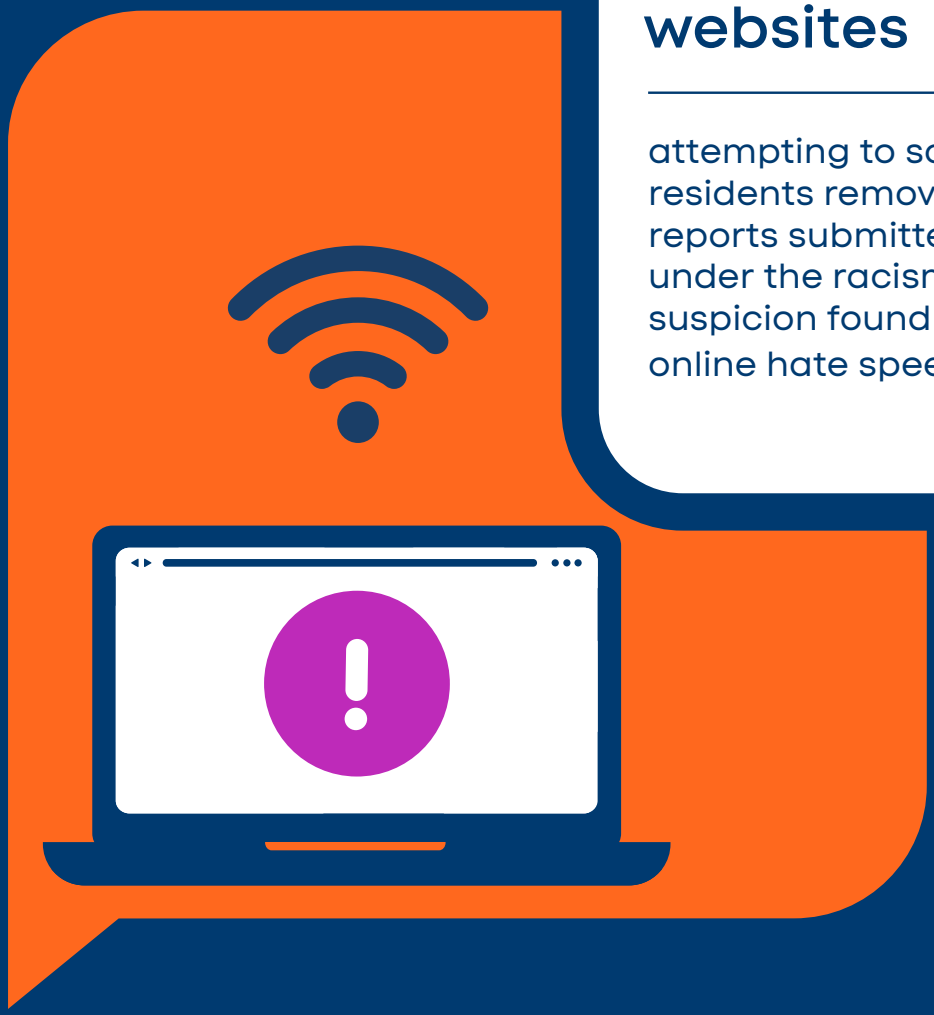
Safe Ireland offers a helpline, one-to-one support, court accompaniment, advocacy, outreach, and support groups. It collaborates with over 38 specialist frontline domestic violence services throughout Ireland. Safe Ireland provides safety information together with information on where to find help and type of supports available.

Website: www.safeireland.ie
Telephone: +353 90 6479078
Email: info@safeireland.ie

Crime Victims Helpline is the national support service for victims of crime in Ireland. They listen with empathy and without judgement, and by providing time and space for you to talk about your experience in confidence. The Crime Victims Helpline can provide information about the criminal justice system, about your rights and tailored signposting to local or specialist victim support services.

Website: www.crimevictimshelpline.ie
Phone: 116 006 **Text:** 085 1337711
Email: info@crimevictimshelpline.ie

Financial Scams and Racism & Xenophobia



89
websites

attempting to scam Irish residents removed. 37% of reports submitted by the public under the racism & xenophobia suspicion found to relate to online hate speech.

HELP US STOP REPEAT VICTIMISATION BY REPORTING AT **HOTLINE.IE**

Findings & insights

Hotline.ie also receives reports about other illegal material, such as online financial scams that are operating in Ireland or otherwise targeting Irish residents, and racism & xenophobia under the Prohibition of Incitement to Hatred Act 1989. The hotline receives comparatively less reports on these topics than CSAM and IIA, however the potential for this content to cause harm, and the harm it may have already caused, means that each of these reports are diligently assessed and actioned.

Financial Scams

- **Hotline.ie received 414 suspected financial scam reports. 21% of these were assessed as relating to online scams targeting Irish residents.**
- **Hotline.ie actioned and removed 89 websites attempting to scam Irish residents.**
- **68% related to phishing attempts, such as websites that purported to be Irish financial institutions, An Post or the Irish Revenue.**
- **16% were fraudulent loan websites which falsely claimed to be regulated by the Central Bank of Ireland.**
- **15% comprised of online shopping scams that used cloned versions of websites of legitimate businesses and the offer of heavily discounted products to entice people into spending money for goods they would never receive.**

Racism & Xenophobia

- **128 reports of suspected racism or xenophobia were made to Hotline.ie in 2023.**
- **37% were found to be related to hate speech, with specific focuses on antisemitism, misogyny, and anti-immigration rhetoric. Only 5 reports were determined to potentially meet the threshold for illegality under the Prohibition of Incitement to Hatred Act 1989.**
- **In cases where hate speech or other racist or xenophobic related activity is identified and the material does not meet the threshold for illegality set out in Irish law, Hotline.ie alerts the responsible platform or website owner to it, as often these could be a breach of community guidelines or rules in place.**

FINANCIAL SCAMS

21%

OF SUSPECTED FINANCIAL SCAMS REPORTS WERE ASSESSED AS RELATING TO ONLINE SCAMS TARGETING IRISH RESIDENTS.

16%

OF REPORTS WERE OF FRAUDULENT LOAN WEBSITES WHICH FALSELY CLAIMED TO BE REGULATED BY THE CENTRAL BANK OF IRELAND

Identifying and avoiding financial online scams

In 2023, Hotline.ie saw a rise in reports regarding a wider variety of different types of scams which are becoming increasingly more sophisticated, presenting a challenge for the public to identify. In the following section, we'll explore the most common scams reported during this period.

Online shopping scams

Online shopping scams is a type of fraud where scammers pretend to be legitimate online retailers and use fake (cloned) websites, ads, or social media posts to deceive customers. They may offer great deals on popular or hard-to-find items, but either deliver nothing or poor-quality counterfeit goods. In some cases, they could also steal financial information.

Six tips on how to spot online shopping scams

1 Shop from trusted websites

Stick to reputable, well-known online retailers. Be cautious when dealing with unfamiliar websites, especially those with poor design or suspicious URLs.

2 Use secure payment methods

Choose secure payment options, such as credit cards or reputable third-party payment platforms. Avoid sharing financial information through insecure channels like email or unencrypted websites.

3 Check reviews

Before making a purchase from an unknown seller or marketplace, research their reputation, reviews, and ratings. Be wary of sellers with limited or negative feedback.

4 Beware of unrealistic deals

Exercise caution when encountering unbelievably low prices or deals that seem too good to be true. Scammers often entice shoppers with irresistible offers to lure them into fraudulent transactions.

5 Be cautious with personal info

Avoid providing unnecessary personal details to online retailers, legitimate sellers typically require minimal information to complete a purchase.

6 Verify website security

Look for "https://" and a padlock symbol in the website address bar, indicating a secure connection. Avoid entering personal or payment information on websites without proper encryption.

Phishing

Phishing is a form of cybercrime where scammers impersonate legitimate entities, such as banks, online services, or Government agencies, to deceive people into revealing sensitive information like usernames, passwords, or financial details. Phishing attempts typically occur through fraudulent emails, text messages, or websites that mimic trusted sources. A common example is delivery fee scams, where an individual receives a text message from someone impersonating a well-known delivery company, claiming a package is awaiting delivery. The message prompts the recipient to pay a small delivery fee by clicking a link that leads to a phishing website designed to steal personal and financial information.

- To identify phishing attempts be cautious of suspicious emails, messages, or websites.
- Check for spelling and grammar errors.
- Verify the sender's identity and avoid clicking on unfamiliar links or providing personal information.

The most prevalent Irish services that were being mimicked in phishing scams in 2023 continued to be Revenue, An Post, Irish banks, and eFlow the motorway toll service.

To safeguard oneself from falling victim to fraudulent practices, you should always verify whether a loan site is registered with the Central Bank of Ireland

Fake loan sites

Fake or unauthorised loan sites, often posing as legitimate lenders, may tempt people with promises of quick and easy access to funds without proper background checks or interest rate disclosures. However, dealing with these unregulated entities can have severe consequences, such as exorbitant interest rates, hidden fees, and potential identity theft.

To safeguard oneself from falling victim to fraudulent practices, you should always verify whether a loan site is registered with the Central Bank of Ireland, which maintains a public register of authorised financial service providers on its official website. It allows users to search for registered entities and ensures they adhere to the required standards and regulations.

When considering an online loan provider, take the following steps to ensure its legitimacy:

1. Visit the Central Bank of Ireland's website and access the register of authorised financial service providers.
2. Search for the name or company registration number of the loan site in question.
3. Verify the lender's authorisation status and check for any regulatory warnings or sanctions.

Hotline.ie reports, to the Central Bank of Ireland, any unauthorised lender that we become aware of through the assessment of public reports received through our web-reporting portal so these might be added to their alerts as applicable.

Cryptocurrency Scams

Out of 415 suspected financial scams, 150 of them were marked as outside Hotline.ie's remit, a significant proportion of these related to cryptocurrency scams which did not have an Irish link.

However, as these can affect anyone, it is important for the general public to be aware of these types of scams:

- **Dating app scams: scammers use dating apps to trick people into investing in fake cryptocurrencies.**
- **Social media cryptocurrency giveaway scams: scammers create fake social media posts that claim to give away cryptocurrencies such as Bitcoin.**
- **Fake cryptocurrency trading platforms: scammers create fake trading platforms that look like legitimate ones to trick people into investing in fake cryptocurrencies.**
- **Speculative Bitcoin investment schemes: scammers promise high returns on Bitcoin investments but then disappear with investors' money.**

Cryptocurrency scams are often difficult for law enforcement to investigate because of the anonymous nature of cryptocurrencies. Transactions are recorded on a public ledger called blockchain, but the identities of the people involved in those transactions are not always known. This makes it difficult for law enforcement to track down scammers and recover stolen funds, so it is pivotal to keep an eye out for them.

Under-reporting

The rise in suspected financial scams to 415 is of significance, however they are still vastly underreported to the Hotline.ie service. A key factor to this is individuals feeling worn down by the sheer number of scam attempts they encounter, leading to a decreased willingness to report them. Additionally, the increasing sophistication of scams makes them harder to spot and report accurately. However, despite this, it is vital that these scams are reported. Even if you do not fall victim to one, someone else might and by reporting you could prevent this from happening. The sooner a report is made, the quicker a fraudulent website can be removed, drastically reducing the chances of someone being scammed.

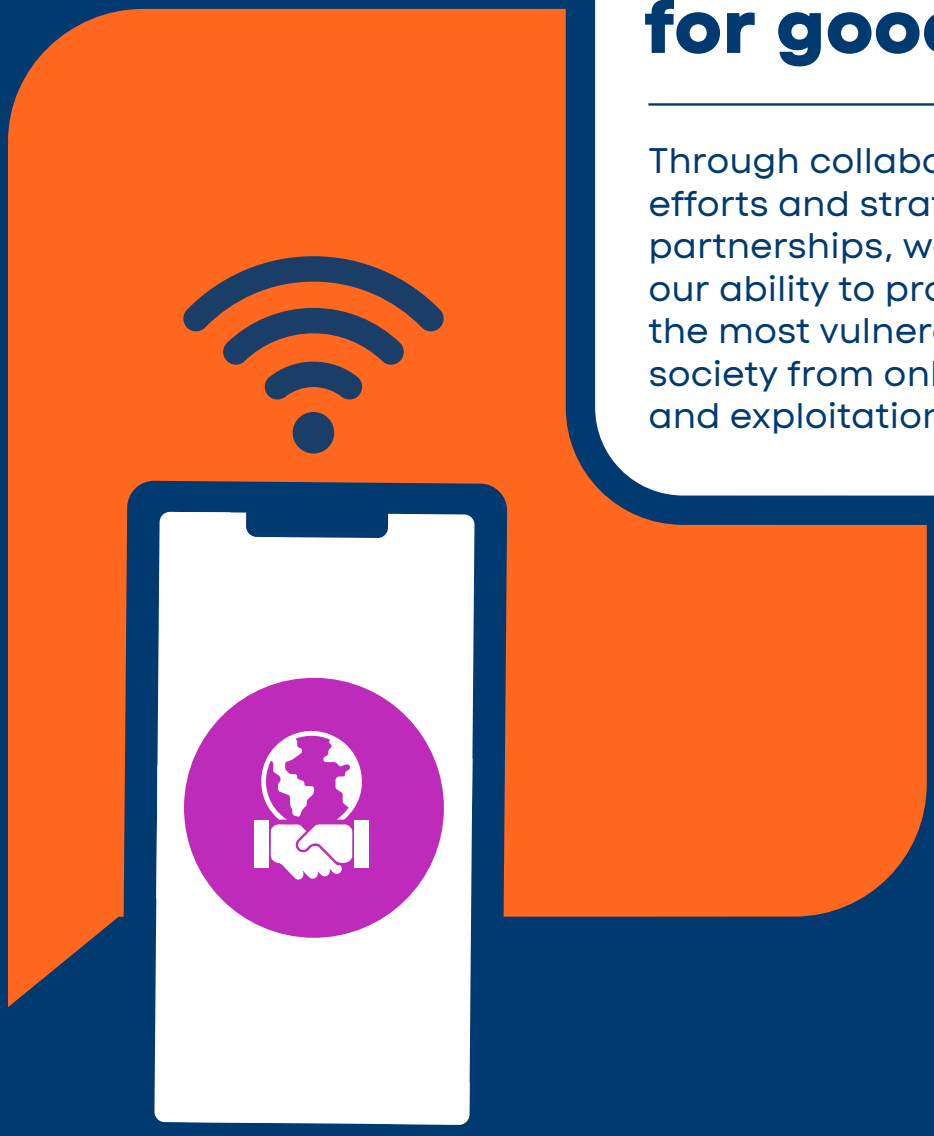
Cryptocurrency scams are often difficult for law enforcement to investigate because of the anonymous nature of cryptocurrencies

CRYPTOCURRENCY SCAMS

415

OUT OF 415 SUSPECTED FINANCIAL SCAMS, 150 OF THEM WERE MARKED AS OUTSIDE HOTLINE.IE'S REMIT

Partnerships



Collaborating for good

Through collaborative efforts and strategic partnerships, we bolster our ability to protect the most vulnerable in society from online abuse and exploitation.

Building partnerships for tangible impact

Working in partnership for good

Since 1999, Hotline.ie has provided a secure and confidential web-reporting portal for Irish residents to report suspected illegal content, including online child sexual abuse, non-consensual sharing of intimate images, racism, and financial scams. Each piece of harmful content removed represents a step towards reducing suffering and re-victimisation. Our work would not be possible without the support of member tech companies and EU grant aid funding.

Our focus is on protecting Irish people, especially children and young people, from online sexual abuse and exploitation. We collaborate with partners across law enforcement, government, academia, tech companies, NGOs, and international organisations to make the internet safer for all. Our dedicated team of highly skilled, police-trained, and internationally certified analysts assess every report against rigorous standards and Irish law. With values rooted in openness, excellence, care, respect, and protection, we work tirelessly to fulfil our mission.

Our skilled analysts meticulously review public reports, sifting through countless images and videos to uncover actionable leads

INHOPE

Hotline.ie is a founding member of INHOPE, the International Association of Internet Hotlines, which unites over 50 hotlines worldwide. This includes all EU Member States, the UK, Russia, South Africa, North & South America, Asia, Australia, and New Zealand. INHOPE's mission is to eliminate child sexual abuse material online by supporting and enhancing the work of its member hotlines. INHOPE collaborates with INTERPOL to conduct regular joint content assessment training sessions for hotline analysts, ensuring consistency in the assessment process across all levels.

An Garda Síochána

Combatting online child sexual abuse material demands a comprehensive strategy. Swift removal of such content is vital, alongside the identification and protection of victims and the pursuit of perpetrators. Collaborating closely with law enforcement is paramount to this effort. Our skilled analysts meticulously review public reports, sifting through countless images and videos to uncover actionable leads. Content deemed likely illegal under Irish law is promptly reported to the relevant authorities at the Garda National Protective Services Bureau. It's essential to clarify that while our triage process is integral, it is not a substitute for criminal investigation. Determining the legality of content remains the prerogative of the courts. Our role is to facilitate the identification and removal of illegal material, leaving the legal proceedings to law enforcement.

Irish Safer Internet Centre

Hotline.ie forms a crucial part of the Irish Safer Internet Centre (SIC), a collaboration between ISPCC, Webwise Ireland, Hotline.ie, and NPC Primary. Together, they proactively identify emerging online threats and deliver evidence-based services, resources, and programmes to support children, young people, parents, and teachers comprehensively.

The Irish SIC provides

1. Ireland's primary national channel for securely and confidentially reporting suspected illegal online content at **www.hotline.ie.**
2. Round-the-clock, free confidential listening services for children up to 18 in Ireland, offered by ISPCC at **www.childline.ie.**
3. Free and confidential helpline services for parents and guardians, alongside online and face-to-face training courses, provided by NPC Primary at **www.npc.ie.**
4. Webwise, the Internet Safety Awareness Centre, develops youth-oriented resources and training programmes on digital citizenship, online wellbeing, and cyberbullying. They also coordinate Irish Safer Internet Day events at **www.webwise.ie.**

Hotline.ie would like to thank all those who have supported our mission and work in 2023. Supports comes in many ways, some of our members provide addition in-kind support over their membership fees, and to that end we would like to especially acknowledge and thank Blacknight Solutions.

As a not-for-profit, our resources are finite and we encourage others to play their part whether by reporting suspected illegal content online to Hotline.ie, funding us, or collaborating on the development of best practices, technology, and research. Your support contributes to tangible change, helps us remain agile and ultimately enables us to enhance our impact for the protection of countless children and people within Ireland and abroad.

Our members

The work of Hotline.ie is actively supported by 21 companies whose invaluable contribution shows their commitment to combatting illegal online material and particularly the distribution and proliferation of child sexual exploitation online.

Glossary of terms

An Garda Síochána: Ireland's National Police Service.

Child sexual abuse images/videos/imagery/content/material: any representation that shows a person who is or is depicted as being a child and who is engaged in or is being depicted as being engaged in real or simulated sexually explicit activity. We use the term "child sexual abuse" material/imagery to reflect the very nature and gravity of the content that we deal with and challenge any notion that such acts may have been carried out pursuant to the "consent" of the child.

Computer-generated or "virtual" child sexual abuse: in the context of child sexual abuse and exploitation this refers to wholly or partly drawn, artificially or digitally created and/or altered sexualised images of children, and it is illegal under Irish law. This can include, for example, cartoons, drawings, computer-generated animations or imagery, pseudo-photographs (e.g., where the computer-generated image is almost indistinguishable from that of a real living child), stories, etc.

Child-Grooming: in the context of child sexual abuse and exploitation, "grooming" is the short term for the solicitation of children for sexual purposes. It refers to the process of establishing/ building a relationship with a child, sometimes by using digital technologies, with the view to lower their inhibitions, manipulate, and sexually exploit and/or abuse them.

Child "self-generated" or "self-produced" sexual material: term used to refer to sexually explicit imagery or videos taken by children and/or adolescents (under 18 y.o.), and primarily used as a descriptive term to convey how the image came to be. In some cases, such content may be produced voluntarily and initially shared without malicious intent as part of developmentally appropriate exchange between adolescents. However, there are situations in which harm is caused e.g., when a child or adolescent is coerced into producing such content; when the imagery is scraped by "collectors" and misappropriated, etc.

Commercial CSAM: child sexual abuse material that in the professional opinion of the Hotline.ie Content Analyst has been produced, distributed, or intended for the purpose of financial gain - whether directly through membership fees, traditional payment methods and cryptocurrencies or indirectly via digital advertising networks or other methods.

Content already removed* classification is assigned when the reported webpage clearly states that the content was removed. This may occur when, for example, the content owner no longer wishes to make it available and has deleted it; the content was actioned in the meantime through other means; or it was in breach of the service provider/platform terms & conditions. In this event, our Analysts have no way of knowing beyond any reasonable doubt whether the content would have been potentially illegal under the Irish law, and as such the only classification that can be assigned is "content already removed".

Dark web or dark net: is the hidden part of the Internet, namely the part of the web whose contents are not indexed by standard web search engines, and which requires special software, configurations or authorisation to access. It can be accessed using Tor which is anonymity software that makes it difficult to trace users' online activity.

End-destination service: is an digital service or platform where CSAM is being hosted or accessible at e.g., a video streaming website, or image host, etc.

End to end encryption (E2EE): a method of securing online communications, wherein the content of each message is visible only to the sender and recipient. Broadly speaking encrypted data is only "readable" by those with decryption keys. E2EE prevents unintended users, including third parties, from reading or modifying data when only the intended reader(s) should have this access and ability.

Gateway service: a digital service or platform or website that (re) directs, leads, or links to CSAM e.g., a forum post sharing a link to a third-party website.

GNPSB: An Garda Síochána to Garda National Protective Services Bureau (GNPSB).

Not accessible* classification assigned when our Analysts cannot access the online content that is being referred e.g., the domain is not found to exist, if a website or cyberlocker requires payment to access, etc.

Not found* classification is recorded when, for example, a 404 error "page not found" is returned.

Notice and Takedown (NTD): is the process through which CSAM is referred by Hotline.ie for removal from the Internet by the tech companies who may be hosting or providing access to the illegal content in question.

Other not-illegal* classification is applied when the content does not breach Irish law and does not fall into one of the common Hotline.ie classifications; for example reports pointing to news articles, videos of children arguing on the playground, etc.

Repeat-victimisation or re-victimisation: is what happens to a victim when their abuse is recorded e.g. images/videos, uploaded and shared online. Each repeat viewing and sharing of the content constitutes a perpetuated violation of the victim's rights and prolonged suffering. The prevention of re-victimisation is at the heart of Hotline.ie's work. With each illegal reference (website, image, video, etc.) that we remove from the Internet, there is one less instance of re-victimisation.

Report: in the context of Hotline.ie work, the term is used to refer to a "single" publicly sourced reference of suspected illegal content online (e.g., a website) received by Hotline.ie. In most cases this "single" reference may contain, display, or lead to hundreds of items (e.g., images, videos, lists of hyperlinks to other webpages, etc.).

URL: an acronym for "Uniform Resource Locator". A URL is the specific Internet location where a file is saved. For example, the URL of the Hotline.ie Code of Practice is: https://www.hotline.ie/library/hotlineie-code-of-practice-2020.pdf

Query: in certain cases, queries submitted to Hotline.ie may progress to a full report. Members of the public who may wish to submit a query or receive a report acknowledgement and a response should ensure to include an email address with their report. Any personal data relating to a non-anonymous report will be deleted within ninety days from completion of the assessment of the report. For more details, please read our Privacy Statement available on www.hotline.ie

Webpage: a document which can be viewed using a web browser. A single webpage can hold many images, text, videos, or (hyper) links: where many websites will have several webpages.

Website: it is a set of related webpages typically served from a single web domain. Most websites consist of several webpages.

Your Voice Matters

Hotline.ie is here to help: **www.hotline.ie/report**

Designed by navigatebydesign.com
Printed by soonerthanlater.com