

Change begins with reporting

Your safety, our purpose



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.

©2023, 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. (2023). Hotline.ie 2022 Annual Report. Dublin, Ireland

Designed by navigatebydesign.com



Co-funded by
the European Union

Change begins with reporting

Your safety, our purpose

Report now

Visit our secure and confidential web-reporting portal

hotline.ie/report

Learn more

Follow us on

[twitter@Hotline_ie](https://twitter.com/Hotline_ie)



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



44 MINS

Listen to:

Age, Sex, Location

RTÉ Radio 1 Documentary

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

Thank you

The team at Hotline.ie would like to express their deepest gratitude to all who have done the right thing by reporting suspected illegal content online.

Your actions have made a real and profound impact in protecting those who are at risk of harm, vulnerable or have been harmed online, especially children and young people.

We would also like to thank and acknowledge all those who we collaborate with in this space, our national partners, our sister hotlines across the globe, An Garda Síochána, and the wider global child protection community.

Finally, we would also like to thank our members and the European Commission, who co-fund Hotline.ie and make our work possible.

Thank you for your ongoing and unwavering support and trust in our work.

The team at Hotline.ie

Foreword: Minister for Justice

In 2022, Hotline.ie completed another year of its commendable and difficult work as a vital pathway for members of the public to securely, confidentially and anonymously report suspected illegal content online, and in particular child sexual abuse material (CSAM).

I am pleased, as Minister for Justice, to have the opportunity to write the foreword to this Annual Report. I note that in collaboration with An Garda Síochána, and overseen by the Department of Justice, Hotline.ie has been undertaking this important work for 23 years now, and always with the highest level of diligence and professionalism.

This Government has made prioritising online safety a key element in building stronger and safer communities, while recognising that there are many complex issues in this space.

That work continues, and there can be no doubt that it is necessary. Many of the figures and statistics in the 2022 Annual Report are shocking and I am very aware that behind these numbers are real people, very often children, who have suffered.

Hotline.ie received more than 31,000 reports in 2022, its highest number ever. This increase on the 2021 figures itself follows a massive surge in reporting between 2020 and 2021. While it is disturbing to see evidence of such crimes, I welcome the fact that such images have been rendered inaccessible and are being dealt with by appropriate law enforcement.

I know that this year's Annual Report looks at the concept that "change begins with reporting" and there can be no doubt that the 31,000 plus reports reflects increasing public engagement with the service. However, it also demonstrates the scale of the problem of online child sexual abuse material.

The majority of the reports – more than 29,000 – related to suspected child sex abuse material, with some 13,799 assessed by the Analysts at



Helen McEntee T.D., Minister for Justice

Hotline.ie as relating to child sexual abuse. This is a slight decrease on 2021. Each report can involve anything from a single image to thousands of images and videos. Each image is a crime. These are despicable acts and we must never become hardened or inured to these figures. I am absolutely committed to ensuring my Department plays its part in tackling these horrific crimes.

The Hotline.ie Annual Report also includes, for the first time, full-year statistics on intimate image abuse (IIA), or the non-consensual sharing of intimate images and videos. On the back of Coco's Law, the new legislation that I enacted early in 2021, my Department partnered with Hotline.ie to make reporting intimate image abuse as easy as possible for as many victims as possible. Once illegal content is reported to Hotline.ie, their experts assess the report and take on the necessary next steps, including getting the content removed from the internet.

This work is showing some very positive results. In 2022, Hotline.ie received 786 reports of suspected IIA, 514 of these reports Hotline.ie was able to action - contained active and publicly accessible online addresses - some 96% have been successfully removed at source, despite none of these being hosted in Ireland. This is encouraging.

Finally, I would like to thank the team at Hotline.ie for their vital dedication and to wish them well in their important and valuable work.

Welcome from our Chief Executive

This annual report provides a glimpse into the unwavering and relentless work of the team at Hotline.ie in the year gone by. Work that is essential and critical as it impacts on Irish children and people at times of vulnerability and even personal crisis.



Ana Niculescu Chief Executive

The digital world knows no “hard” borders which means criminal, abusive and exploitative content proliferates online and can be accessed from anywhere in the world, at any moment. Thus, Hotline.ie’s work of removing, at source, child sexual abuse and exploitation, non-consensual intimate images, racism and xenophobia, and financial scams, breaks the cycle of abuse, prevents repeat-victimisation, has an impact on a global scale and has been contributing towards the protection of countless children and people.

Continuously removing criminal and harmful imagery from the Internet, also challenges any notions that such horrible acts perpetrated on the most vulnerable in society, would ever be acceptable or tolerated.

Although the subject matter of this report might make for uncomfortable reading and, at times, it might even be hard to conceptualise that such acts can happen in the first place and the extent of the abuse, we hope it sheds light on these difficult societal problems and that you obtain a valuable insight into the important work of Hotline.ie.

One child, one person, is one too many. At Hotline.ie with each illegal image or video we remove from the Internet, we know it is one less instance of suffering, one less child or person being re-victimised, and one chance for an unknown child victim to be identified and rescued from a life of abuse. We measure our success not only in the number of reports and notices we issue and remove, but also in the lives we positively affect through our work.

“I am proud and grateful for their dedication and commitment to making a difference, day in and day out. Even the smallest progress can have a ripple effect”.



Partnerships play a vital role in our mission as well. Hotline.ie continues to work collaboratively and in conjunction with law enforcement, the Department of Justice, the Irish Safer Internet Centre, other support services in Ireland, sister hotline worldwide, tech companies, academia and other NGOs. Together, we amplify our impact and reach wider audiences to make sure the message of online safety, child protection, a more inclusive and positive digital world gets to every corner of society.

The work of Hotline.ie is a team effort, every single member of the team, regardless of their role, plays an important part; I am proud and grateful for their dedication and commitment to making a difference, day in and day out. Even the smallest progress can have a ripple effect.

We also acknowledge the challenges and complexities we face. We recognise that whilst steady progress has been made, there is still so much more to do.

The team at Hotline.ie is acutely aware that people often experience a number of other issues, difficulties and harmful content, contact and conduct online that we unfortunately cannot help with, as Hotline.ie specifically combats content online that is contrary to the law. However, we remain hopeful that critical pieces of legislation such as Ireland's Online Safety and Media Regulation (OSMR) Bill, and other changes to the digital regulatory landscape in prospect both at national and EU level, would accelerate and bring about tangible change, on a much-needed broader base.

We look forward to reporting further progress next year. Thank you!

Contents

- 1 About Hotline.ie
- 3 Journey of a report
- 4 What to report

05 Statistics and Findings



-
- 6 Context and the dataset
 - 7 Statistics & findings

32 Racism and Xenophobia



-
- 33 Findings & insights

09 Online Child Sexual Abuse & Exploitation



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

35 Financial Scams



-
- 36 Findings & insights

39 Partnerships



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

22 Intimate Image Abuse



-
- 23 Know the Law
 - 24 What is intimate image abuse?
 - 25 How can Hotline.ie help?
 - 26 Statement of purpose
 - 28 The people who have suffered from IIA
 - 29 IIA site types - where the imagery was found
 - 29 Outcome sought by the reporter
 - 30 Sexual extortion scams
 - 31 Signposting

-
- 44 Glossary of terms

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, Irish government, online services providers, and NGOs, 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; the values and victim-centred culture that led to our creation are just as relevant and true today. 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.

While we work closely with law enforcement and tech companies to quickly remove illegal material from the internet, 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.

The team at Hotline.ie works relentlessly to:



Reduce the prevalence

Reduce the prevalence of illegal content online, especially child sexual abuse material and technology facilitated sexual exploitation of children



Break the cycle

Break the cycle of abuse and exploitation



Prevent repeat-victimisation

Prevent repeat-victimisation of those who have suffered from abuse

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. We are also an integral part of the Irish Safer Internet Centre alongside Webwise, ISPCC-Childline and National Parents Council; and we are a member of the National Advisory Council for Online Safety (NACOS). Hotline.ie is a founder member of the International Association of Internet Hotlines (INHOPE) and works in partnership with 50 other hotlines on 6 continents to ensure child sexual abuse material is removed from the internet, at source, irrespective of where in the world the content is hosted.

How we are funded

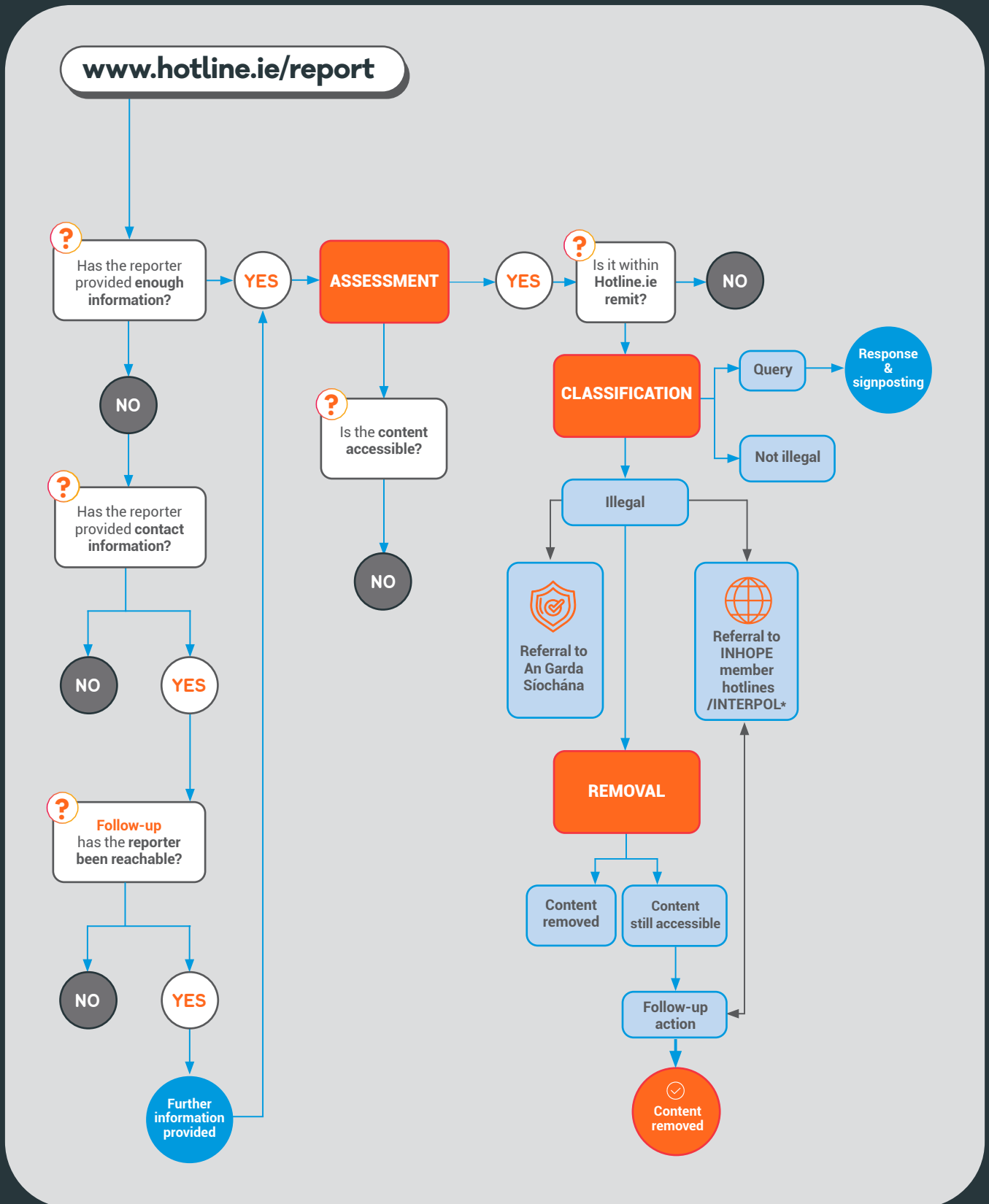
We are a not-for-profit and our work is co-financed by the European Union through grant aid and by our members, who are tech companies, search providers, mobile operators, hosting, and internet service providers. Our resources are finite, and we encourage others to play their part whether by reporting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

We care.

We remove.

WE DISRUPT.

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 reported directly to An Garda Síochána.

You can securely, anonymously and confidentially report to Hotline.ie incidents of:

- Child sexual abuse material (images, video, text, computer generated material)
- Activities related to the sexual exploitation of children, i.e. 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 or that appear to have originated from Ireland.

To create a digital world that is safe and inclusive for all, especially the most vulnerable in society, the importance of reporting cannot be emphasised enough. Through acting together, we can turn the tide on cyber-abuse, cybercrime and repeat victimisation.

While the rapid removal of illegal content online is extremely important to avoid further victimisation and minimise the perpetuation of online harms, of equal importance is a victim-centred approach, to ensure for example that the children in child sexual abuse imagery may be identified and safeguarded,

and the perpetrators brought to justice. This is also particularly true in respect of reporting intimate image abuse online, financial scams, and racist and xenophobic incidents.

Reporting is ultimately about regaining control and challenging the “normalisation” of harmful and toxic behaviours that can lead to desensitisation of real-life harm and suffering, through it can play your part for a safer and better tomorrow.

Additionally, reporting also provides an evidence-base that informs on areas for policy intervention, emerging online threats, and trends, and allows the development of tailored solutions for early intervention, awareness, and prevention education.

Hotline.ie’s Analysts diligently assess every report that is received. If the reported content is assessed and found to be potentially illegal under Irish law, removal is sought. Our Analysts work with partner organisations to ensure it is removed at source as quickly as possible and referred to law enforcement following applicable agreed processes and procedures.

We urge all members of the public to report any material they suspect to be illegal, even if they are unsure or have doubts. Hotline.ie Analysts are experienced and trained in identifying different methods and techniques that can be used to obscure illegal material, so any suspicion is thoroughly investigated. Even the slightest suspicion or feeling that something could be illegal should be reported, as often a website or page can appear relatively innocuous but can be hiding something more.

Statistics & findings

2022 saw 31,068 reports submitted to the Hotline.ie service

This is the highest number of

reports on record



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.

Hotline.ie will continue to stand firm and it is committed as ever to enhance its response to become even more impactful, strengthen its

partnership, continue to learn, and adapt within an ever-changing national and global ecosystem.

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, 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, 2022.

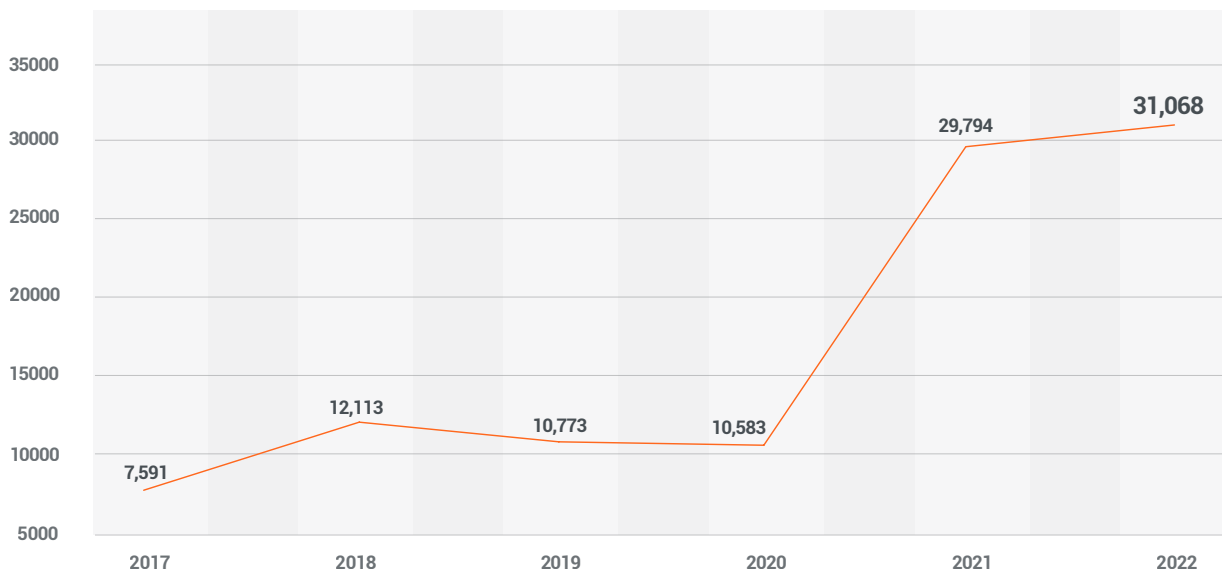
The figures and findings included in this publication are predicated on reports received from the public by Hotline.ie. Under current operational procedures, approved by the Department of Justice and An Garda Síochána, Hotline.ie is not mandated to proactively search for child sexual abuse material (CSAM) on the internet. However, when we receive a public report (i.e. website) and there is evidence, for

example other links being displayed using explicit terms or keywords commonly associated with CSAM suggesting further illegal content would be available on other linked websites, we can follow those links. If further illegal content is indeed 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

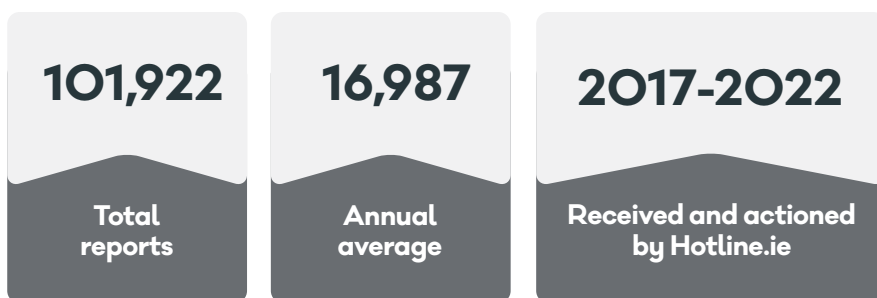
Annual volume of reports received by Hotline.ie



Annual volume of reports received by Hotline.ie

1 report = from 10(s) to 100(s) of images

Total reports received and actioned by Hotline.ie between 2017-2022



“94% of reports were of suspected child sexual abuse material”

2022 saw 31,068 reports submitted to the Hotline.ie service. This is the highest number of reports on record, following the 29,794 reports received in 2021, which at the time was a near tripling of reports from the year previous. The number of reports appears to have temporarily stabilised at this level after the massive surge in reporting that occurred between 2020 and 2021.

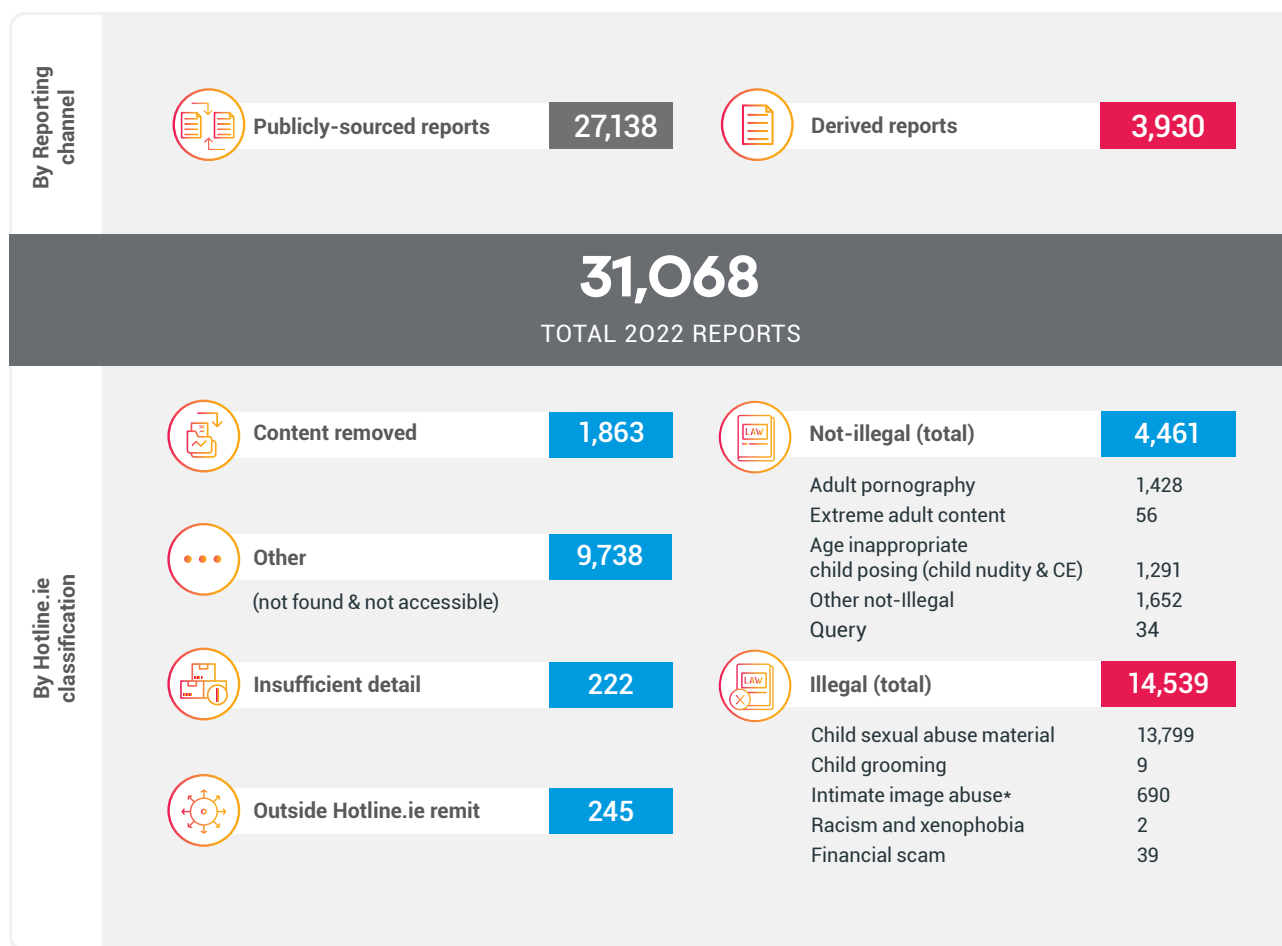
94% of reports were of suspected child sexual abuse material, in total suspected intimate image abuse, racism & xenophobia and financial scams made up 4%, and the remaining 2% related to queries about other potentially illegal activity online. All of these suspicions are investigated by Hotline.ie Analysts, however, due to a wide range of reasons not all of them are classified as leads to potentially illegal material.

2022 figures, following Hotline.ie Analysts' classification, reveal an increase in public reporting accuracy with nearly 1 in 2 reports found upon assessment to lead to potentially illegal material.

Our Analysts classified 14,539 reports as illegal (CSAM, intimate image abuse, racism & xenophobia, and financial scams). The last two years (2022-21) combined represent a 273% increase over the total for the preceding five years.

A report is an all-encompassing term used to describe a single reference point to suspected illegal online content. This means that any of the 31,068 reports submitted could have been a link to a single image or video, but it could also have been an entire website hosting or linking to hundreds of images or videos, or any other suspected material.

Breakdown of reports



Other classifications Illegal reports Public reports

* Reports classified as insufficient detail, outside Hotline.ie remit, not accessible, and not found, are collectively referred to as "non-actionable reports". This is because our Analysts do not have sufficient information to ascertain which content is being reported, how to access it, or the content may no longer be online or accessible. As such no further action would be possible. "Outside Hotline.ie remit" classification refers to any issues not covered by Hotline.ie's stated remit, such as but not limited to copyright infringement, sale of drugs, sale of documents or personal data etc. "Content already removed" is usually assigned when the reported webpage clearly indicates that the content was removed. This may occur when, for example, the content owner has deleted it; or it was in breach of the online service provider 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.

Online Child Sexual Abuse & Exploitation

29,086 suspected CSAM reports, of which 13,799 assessed

as child sexual abuse material, referred to law enforcement

and actioned for removal





Know the law

Child sexual abuse and material

it 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 also know?

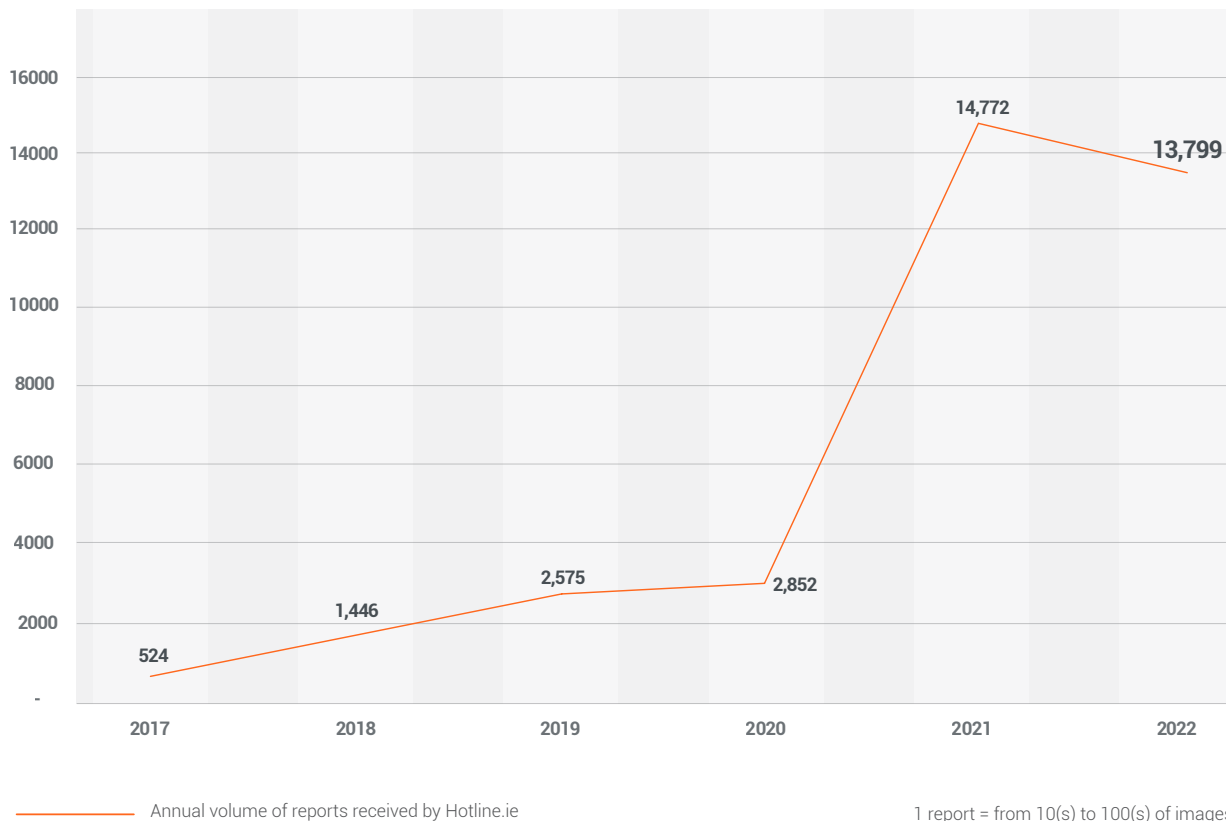
"Child pornography" is defined as **any visual representation** that shows a person who is or is depicted as being a child and who is engaged in or is depicted as being engaged in **real or simulated sexually explicit activity**. This would also include: e.g. cartoons, computer-generated animations or imagery, pseudo-photographs, to name a few.

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

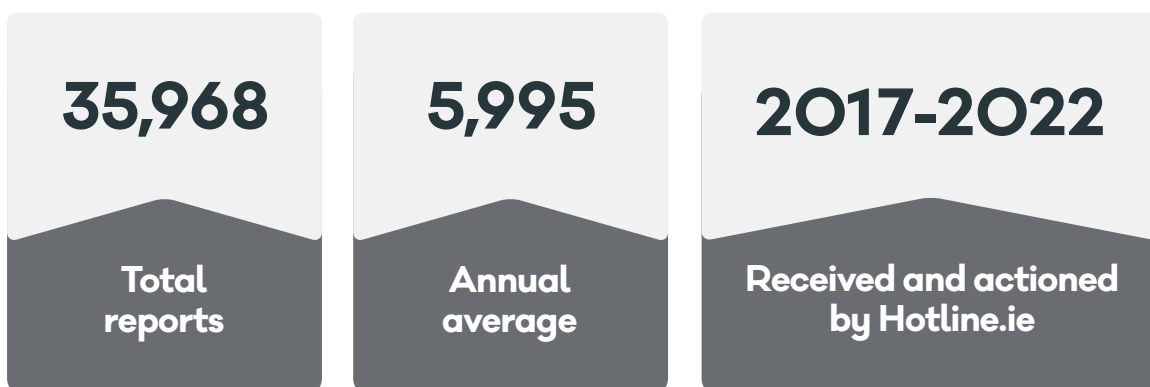
! **It's a crime** to expose a child to sexually explicit acts or to pornography.

Statistics & findings

2022 volume of reports classified as child sexual abuse material



Total CSAM reports received and actioned by Hotline.ie between 2017-2022



In 2022, Hotline.ie's world-class Analysts assessed 29,086 public reports submitted as suspected child sexual abuse material (CSAM). Among these, 13,799 reports were classified as CSAM, marking a 6.6% decrease from the previous year. Although this decline is relatively small compared to the overall report numbers in the past five years, it still represents a significant 130% increase over the average during this period. It's important to note that all reports were sourced from members of the public, as Hotline.ie is not mandated to proactively search the internet for CSAM.

Less than 1% of the confirmed CSAM was hosted within Ireland, and all of it was successfully removed within 24 hours. The majority of reported CSAM was hosted abroad, with over 50% hosted outside the European Union. Hotline.ie collaborates with international partners to ensure the removal of CSAM, but challenges arise in countries where such partnerships are absent, and CSAM laws may differ from Irish legislation or even be non-existent. Despite these complexities, 99% of the total confirmed CSAM was successfully removed.

Notably, a substantial proportion of suspected CSAM reports (31%) fell outside Hotline.ie's investigative mandate. This suggests the actual volume of CSAM reported to Hotline.ie may have been much higher but couldn't be accessed and assessed by our Analysts.

Instances of 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.

The children in the imagery

Gender breakdown



Boys

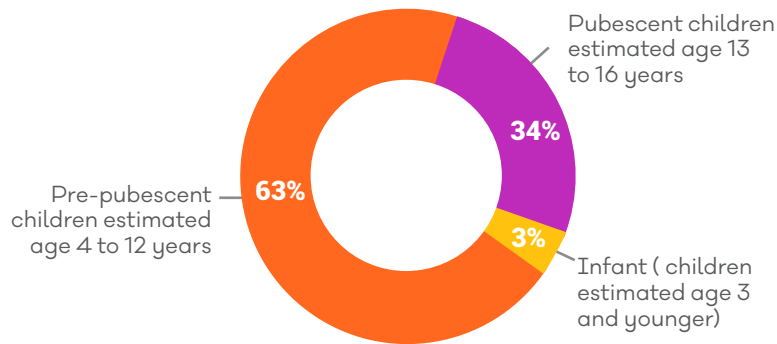


Girls

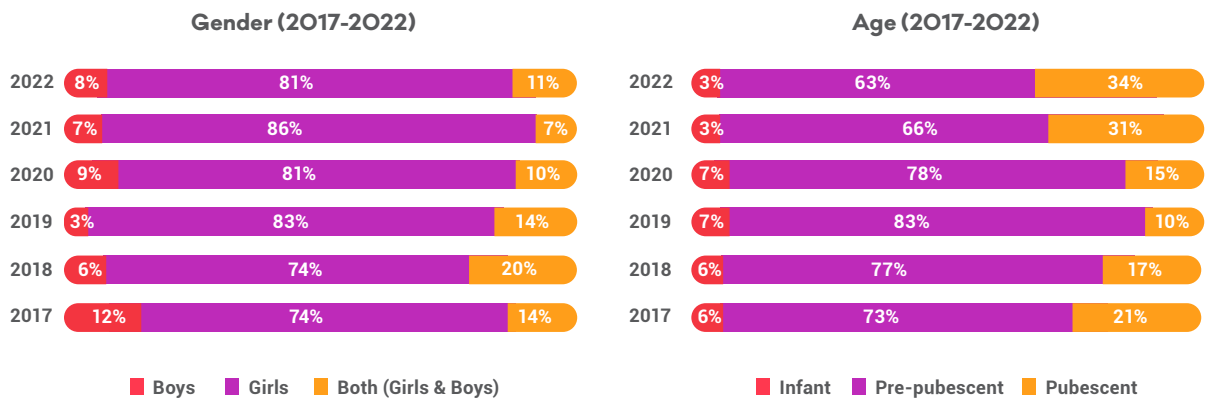


Both (girls & boys)

Age breakdown



Comparative analysis



CSAM findings and insights



The sexual abuse of children is not something a lot of people want to talk about, or even hear about, and given the abhorrent nature of it that's completely understandable. It is so distressing to some people that they would rather not acknowledge it exists, but unfortunately it does exist, and turning a blind eye to it will not help anyone. The people who submit reports to us have often been exposed to the worst material imaginable and in that moment of distress have chosen to do the right thing by reporting it. And so, we have a duty to them and the wider public, and of course the children themselves, to ensure that CSAM is removed but we also owe it to them all to raise awareness and keep talking about it. Silence only benefits the abusers.

Sean, Hotline.ie Content Analyst

A notable trend over the year was the significant rise in computer generated CSAM, with 37% of the CSAM reports seen also comprising of, or containing elements, of this material.

The term "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.

Computer generated CSAM was found to be more severe and depict very young child-like renditions. Two thirds of computer generated CSAM was found to display adults subjecting children to penetrative sexual activity, and bestiality or sadistic elements.

92% of the computer generated CSAM was also found to display depictions of preteens. As this material is computer generated there is virtually no limit to the scenarios that can be depicted.

It is important to note that under Irish law, namely under the Child Trafficking and Pornography Act 1998, "any visual representation" depicting the sexual abuse of a child is illegal, which includes computer

generated CSAM. In other jurisdictions, however, this type of material would not be contrary to law, most notably in the United States.

A common misconception in relation to computer generated CSAM is that it is harmless because it does not display a real sexually abusive situation involving a real child. However, there are many reasons why this material is harmful.

- It can be used to normalise the idea of sexual activity with or involving children.
- It can be provided to children by adults who are trying to groom them in an attempt to normalise the act and lower their defences.
- It could lead to someone searching for other types of CSAM

Research has found that the viewing of CSAM has been linked to encouraging people into attempting sexual contact with children. The University of Birmingham in conjunction with the Lucy Faithfull Foundation conducted a [survey](#) on the darknet that found that after viewing CSAM nearly half of the respondents attempted to contact children through online platforms. As such, no type of material that depicts children being sexually abused is 'harmless.'

Hotline.ie Analyst testimonial



When I started working at Hotline.ie these images were mostly drawn or somewhat crudely rendered animations, and they've steadily become more photorealistic over the years, but what we're seeing now since the advancements in AI generated art is deeply concerning. You'd often hear the argument that these images aren't of real children so it's not hurting anybody, well now any image of a child can be fed through an AI and be turned into CSAM. There are even communities out there creating new CSAM based on old videos of real child victims being sexually abused. It used to be the case where computer generated CSAM was limited to certain websites or forums but as we're seeing the CSAM becoming more realistic we're seeing it being mixed in with images of real children, and at times it can be difficult to tell the difference, especially if you're not expecting it. The rate that the technology is advancing at, it might soon be impossible to tell the difference at all.

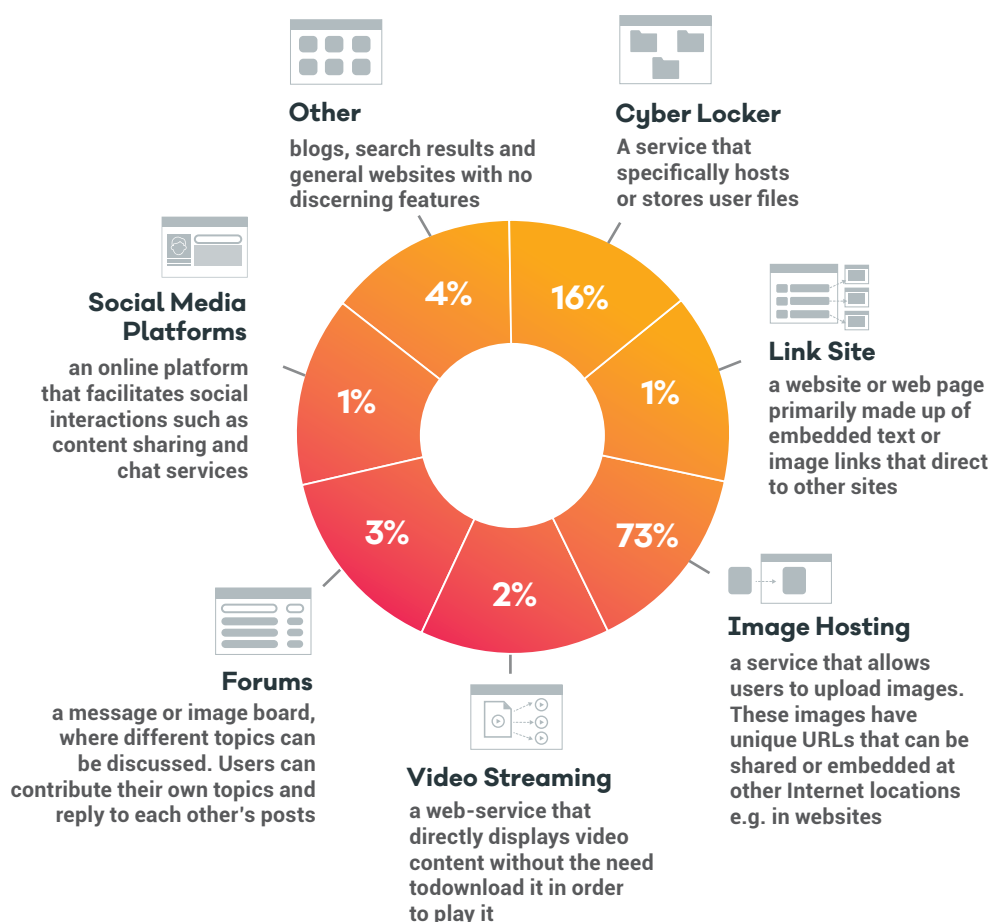
A lot of this technology is trying to implement ethical safeguards to prevent abuse like this, but as we've seen in the past with any technological development, that if it can be exploited, it likely will. It's made worse by the fact there are many jurisdictions where this material is not illegal, as it does not depict a real child or real sexual abuse. Thankfully Ireland is not one of those jurisdictions, but if this is not regulated soon there's a real risk this is going to get worse very quickly.

Sean, Hotline.ie Analyst

Another trend that Hotline.ie Analysts noted was the rise in websites that made use of invite links for tiered subscription access to CSAM. By its design, this would heavily incentivise the distribution of CSAM, whereas the more people someone could invite to the website the more CSAM they would be able to access and view. Options to pay by cryptocurrencies to get instant access to the different tiers of CSAM were also deployed. This trend is of particular concern as invite links were being distributed widely across social media and chat rooms without any context and with the risk

of leading anyone who followed the link to be potentially exposed to CSAM. Distributors of CSAM tend to try to avoid detection by the general public, using various techniques or places on the darknet that are only accessible to likeminded individuals or people in the know. However, these websites were encouraging people to share links with as many people as possible, with the likely intent to draw in those who would be willing to pay directly to access CSAM.

Services misused for CSAM distribution



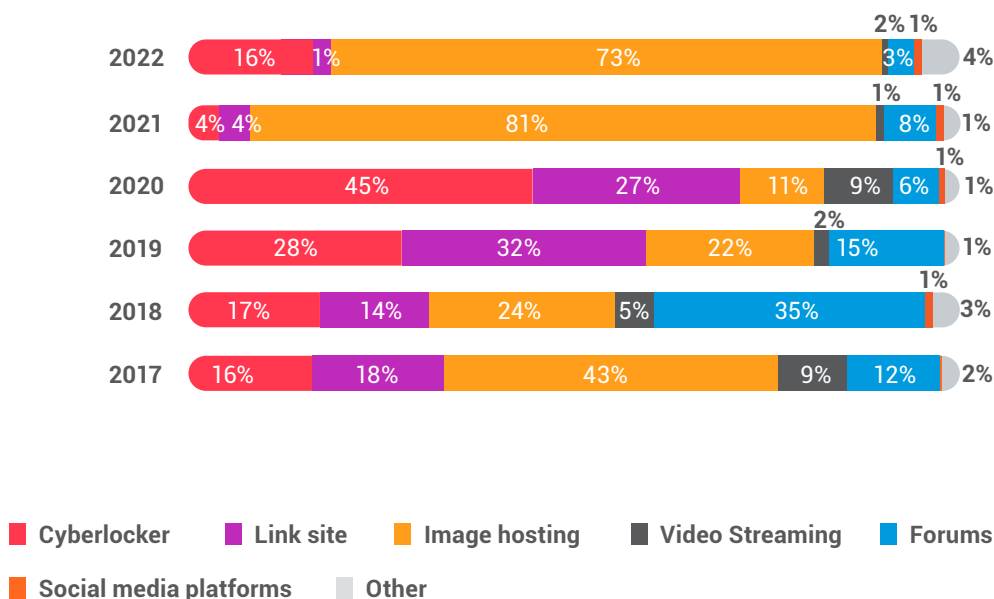
Disclaimer: While the figures above showcase the type of resources misused to share CSAM, they are only a snapshot, stemming from the assessment of all public reports made to Hotline.ie; should not be misconstrued as a complete picture of how CSAM is distributed across, on the Internet.

Of the total CSAM reported to Hotline.ie in 2022, 73% was being distributed on image hosts. This is a slightly lower proportion from the previous year with a larger proportion (16%) being shared in cyberlockers and a minor, but significant, number of reports related to CSAM being distributed in forums (3%). Each of these types of resources are used in different ways to facilitate the distribution of CSAM, forums are often centralised linking to both image hosts and cyberlockers, image hosts are used as to distribute CSAM widely across multiple websites from one secure location and cyberlockers are used to share vast amounts of CSAM hidden from public viewing requiring a download, often requiring a password.

As all Hotline.ie's reports are publicly sourced, the resources misused are representative of locations where members of the public are likely to accidentally stumble upon CSAM. However, there are also means of distribution that would be less accessible to the general public such as groups on messenger services or the darknet that would be

vastly under-reported. In the process of assessing reports Hotline.ie Analysts have observed signs that CSAM distribution is increasingly being facilitated through link sharing in semi-private channels. While these links tend to lead to image hosts or files in cyberlockers where material can be removed, if the location from which the CSAM is being linked from is not reported then it will remain active. For Hotline.ie, to be completely successful in taking down CSAM it means the removal of where the CSAM is being shared from and where the CSAM is hosted. Otherwise, there's the opportunity for those sharing the links to reupload the CSAM at a different location or for them to reshare the same links from a new location to the CSAM that hasn't been removed. As such, it is paramount that reporters include as much information in the reports that they submit, including where they were browsing before finding the link to the CSAM, as this significantly improves the chances that the entire distribution chain of CSAM is completely removed.

Comparative analysis



In 2022, CSAM distribution was traced to 44 different countries. This represents the greatest number of countries CSAM was traced to on record, with two more countries than the previous year.

As a continuation from previous years, the Netherlands was the country where CSAM was traced to the most, with 3,326 reports leading to material hosted on servers there. While this represents 23% of the total and is undoubtedly a significant amount of CSAM, it also is an encouraging downward trend that appears to have taken hold due to national efforts in combatting CSAM. However, the downside to this is that offenders have taken to hosting CSAM in other countries instead, which is possibly reflected in the growing number of countries that Hotline.ie Analysts are tracing CSAM to.

CSAM hosting was still found to be concentrated, with 86% of it located in eight countries, however the distribution of it was found to be more even in the top ten hosting countries than in previous years, with a 7% standard deviation from the average compared to 12% in 2021 and 10% in 2020, this is likely due to CSAM that would have previously been hosted in the Netherlands being distributed more evenly across other countries. Hotline.ie Analysts have noted certain forums or image hosts that had once been hosted by providers in the Netherlands have moved to other jurisdictions.

Notably, the amount of CSAM traced to within the European Union dropped from 54% in 2021 to 43% in 2022, with 36% of that traced to only two EU countries. There were also 31 reports of CSAM traced to Ireland in 2022, which is the highest on record. Two thirds of these related to Computer Generated CSAM which is illegal under the '*Child Trafficking and Pornography Act 1998*'.

“Another trend that Hotline.ie Analysts noted was the rise in websites that made use of invite links for tiered subscription access to CSAM”.

Hotline.ie Analyst testimonial

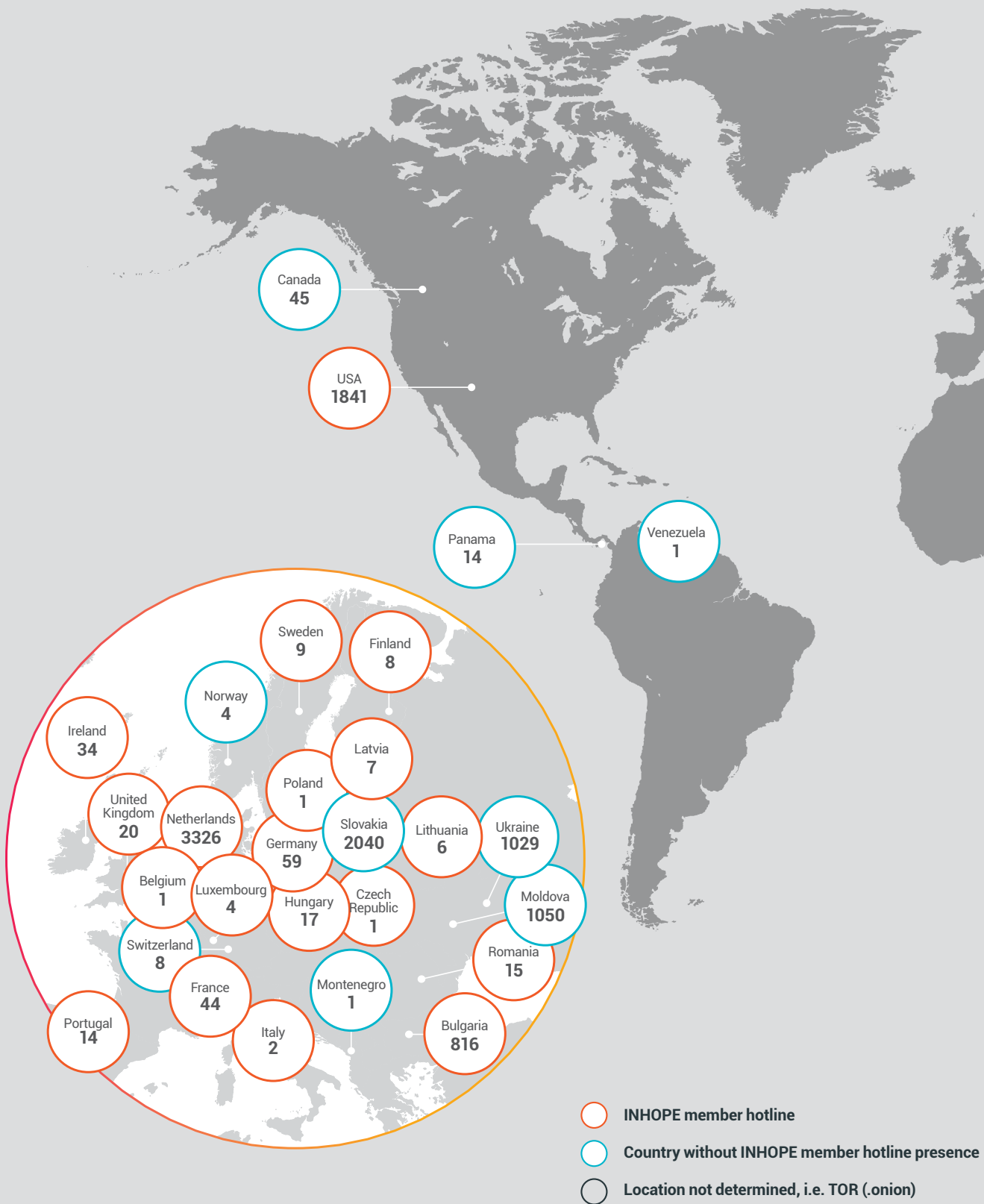


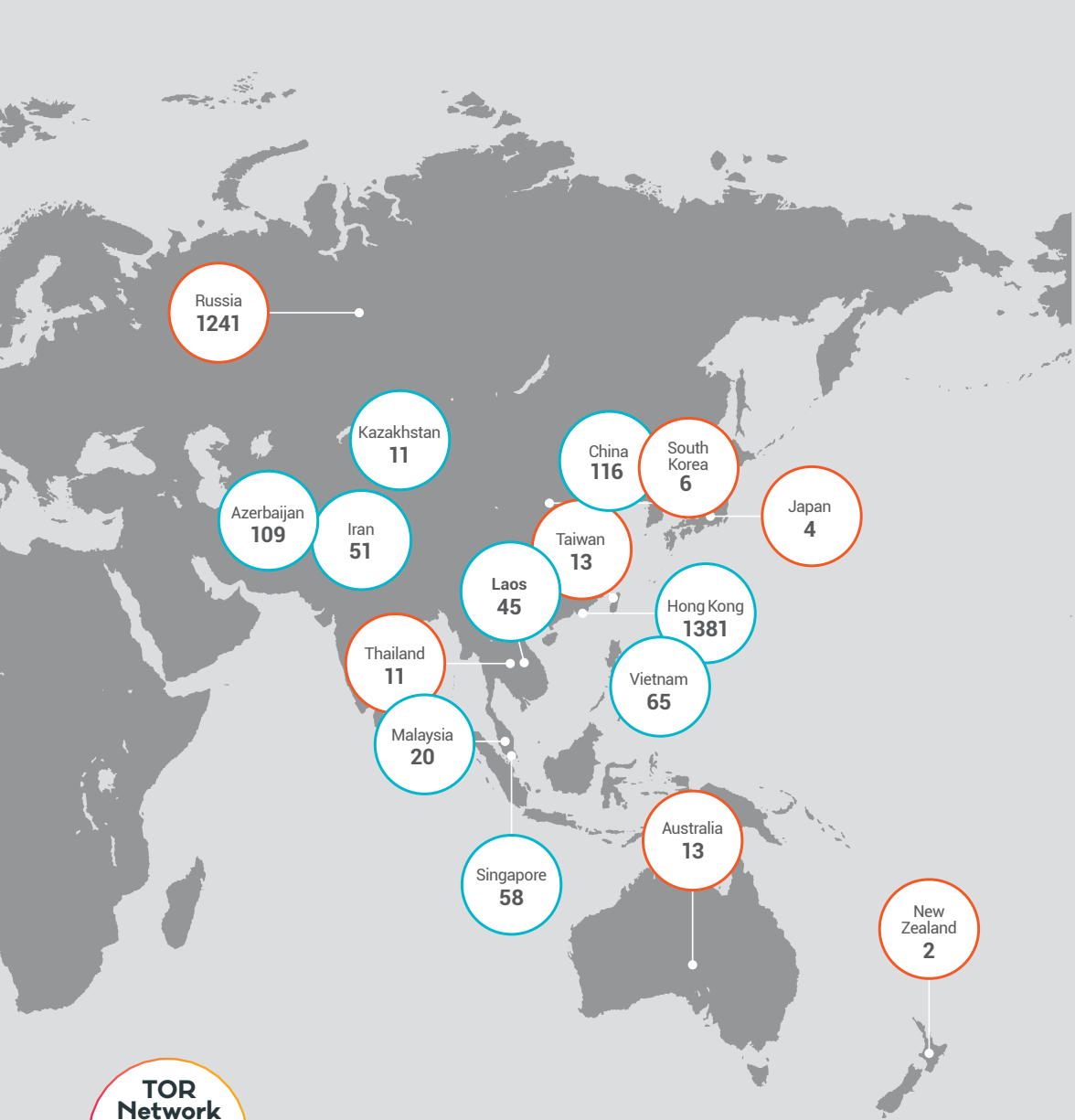
The work we do is tireless. Each day we get the worst kind of material removed from the internet, and by the next it could be back, hosted in another country with a different online service provider. It can seem relentless at times, working to remove it as it surfaces, but once it has been reported to us, we strive to ensure that any website distributing CSAM stays down. We do this to protect the children in the imagery from re-victimisation, we do it so nobody is further exposed to traumatising imagery, and ultimately, we do it to make the internet a safer place for everyone.

Countries with strong and cheap hosting infrastructure or countries with loose regulations are the most vulnerable to CSAM distribution. Removal is only part of the solution, realistically it won't end until there are no safe harbours left and the people behind the distribution are brought to justice. The only way to effectively achieve this is through collaborative effort between hotlines, law enforcement, online service providers and government, and of course, public will.

Alex, Hotline.ie Analyst

Snapshot of CSAM hosting patterns





TOR Network
236

13,563

TOTAL REPORTS

236

1.6% LOCATION NOT DETERMINED (TOR NETWORK)

44

COUNTRIES COVERED

43%

OF ALL CSAM WAS HOSTED IN EU

Intimate Image Abuse

96% successful cross-border removal rate

13% of the IIA reports of a sexual

extortion scam nature





Know the law

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

- ! Intimate Image Abuse is an offence under The Harassment, Harmful Communications and Related Offences Act 2020 (also known as Coco's 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.



Did you also 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 shares an intimate image without the person's consent **without the intention to cause harm** it is an offence under the act to do so.

- ! 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 2022O (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 constitutes 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 – whilst 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 than 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 An Garda Síochána**

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 An Garda Síochána, 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**

Whilst collaborating closely with law enforcement agencies and tech companies, Hotline.ie maintains its independence. Our web-reporting portal is distinct and designed to allow people to report incidents directly to Hotline.ie irrespective of where these may have occurred in the digital world. Thus, minimising unwarranted prolonged re-victimisation by streamlining the process and avoiding the need for multiple individual complaints to different platforms and providers to be submitted by the victim, which otherwise force the victim into reliving the abuse. We understand that online content can proliferate across numerous digital platforms, and our centralised web-reporting approach enables victims to submit one single report referencing multiple sources, saving time, effort and suffering.

- **Handling complex cases**

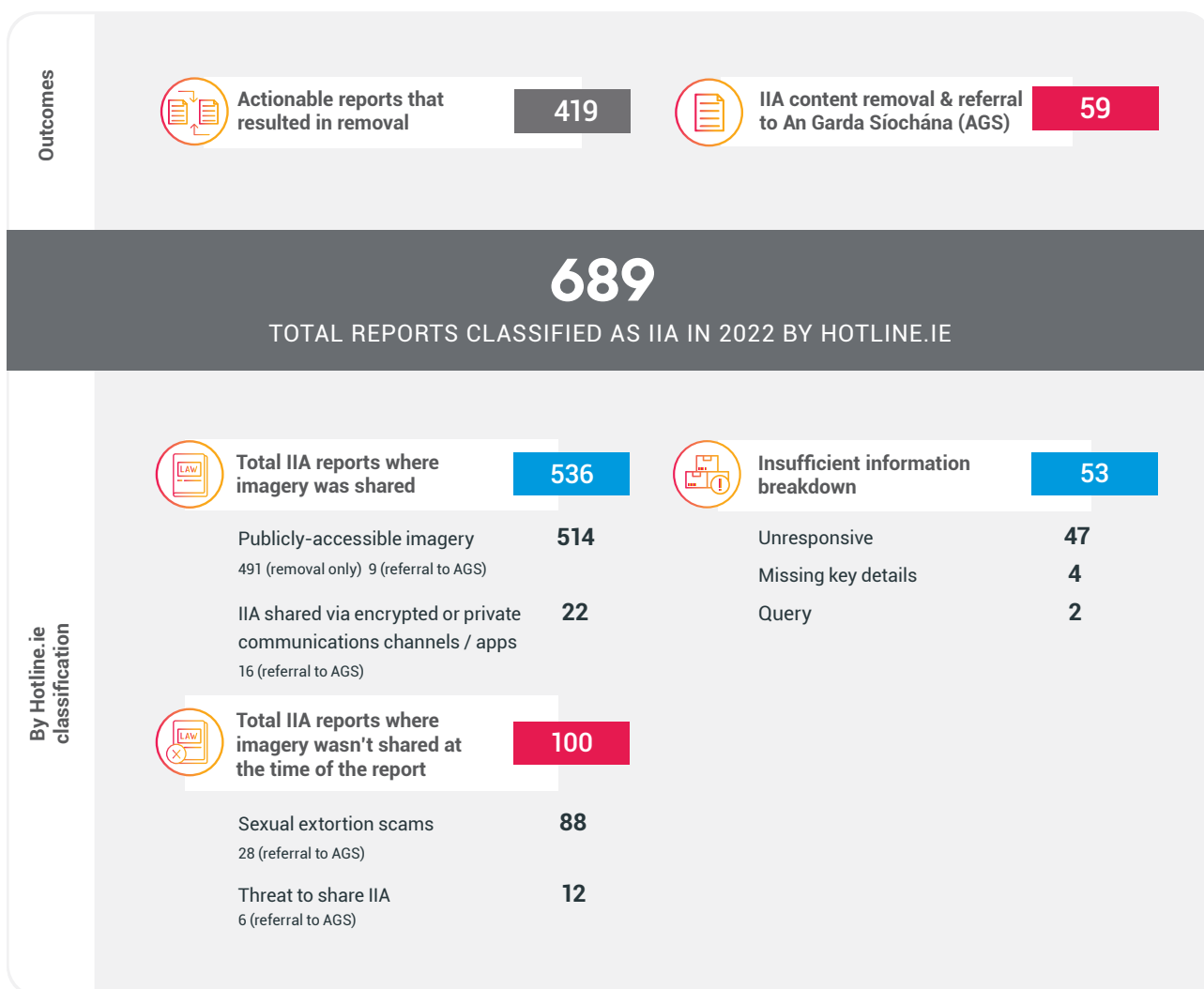
Hotline.ie's dedicated team of Analysts possesses extensive experience in addressing various forms of abuse. In cases involving under 18s, our world class Analysts are well equipped in identifying instances that may qualify as child sexual abuse material or technology-facilitated child sexual exploitation, 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 the aim is to raise awareness of intimate image abuse and the harm it can cause to a person's life. 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. Whilst 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.

In 2022, Hotline.ie received 786 reports under IIA suspicion, with 694 of these assessed and classified as IIA.

514 IIA reports related to publicly shared images or videos. This means content shared without consent online, and accessible to anyone through e.g. a URL, such as a video uploaded on an adult video streaming website or a social media post. 96% were successfully removed. One of the primary challenges to IIA removal, for example, whilst it is illegal content in Ireland, it may be that in the country where the website is hosted an equivalent of the Irish law does not exist and as such the online service provider in the said country does not feel they must comply with Irish law and remove the content. On a case-by-case basis there may be other options available, and that is why it's important for Hotline.ie to have a way of contacting the reporter to discuss as applicable.

The remaining 4% e.g. online service provider unresponsive or missing contact information. In these cases, delisting requests are sent to search engine providers so that any search results for the non-consensually shared material does not yield a result, meaning people will not be able to find and access it, that's unless they have the IIA specific URL hosting the content.

Further 22 reports related to images and videos that had been shared privately, meaning images or videos that had been sent via private messenger apps or within privacy focused apps that a third party cannot access. The material in these situations is often shared from one personal device to another and as such Hotline.ie cannot enact removal.

Under the Harassment, Harmful Communications and Related Offences Act 2020 the threat to share intimate images is also an offence. Hotline.ie received 100 reports referring to IIA threats made

primarily with the purpose of extorting the victims. In 2022 Hotline.ie Analysts noted a surge in sexual extortion scams, where people, mostly young men, were deceived into sharing intimate images of themselves. As soon as intimate images were shared, the person at the other end would reveal themselves to be a scammer and threaten to share the imagery online unless payment was made.

9 out of 10 reporters of sexual extortion were male; however, it is also important to note that generally intimate image abuse was found to predominately affect females with 85% of all IIA reports being submitted by those who identify as such.

58 reports lacked key details required to make the assessment and take further action, information which could not be gathered as the reporters were unresponsive to any communication or otherwise provided fake or incomplete contact details.

Only 11% of reporters sought to have the matter referred to An Garda Síochána for investigation, with the majority seeking content removal only. Hotline.ie also signposts reporters of IIA to other support services available in Ireland, such as mental health organisations, domestic abuse services, the Crime Victims Helpline to name a few. The services signposted to are tailored to the specific needs of the reporter.

In 2022, Hotline.ie received 786 reports under IIA suspicion, with 694 of these assessed and classified as IIA.

The people who have suffered from IIA

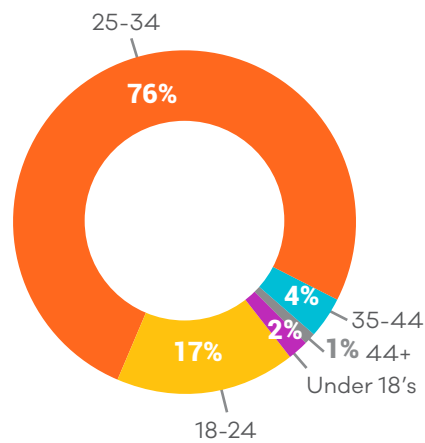
Gender breakdown

BASED ON THE REPORTER'S DISCLOSURE

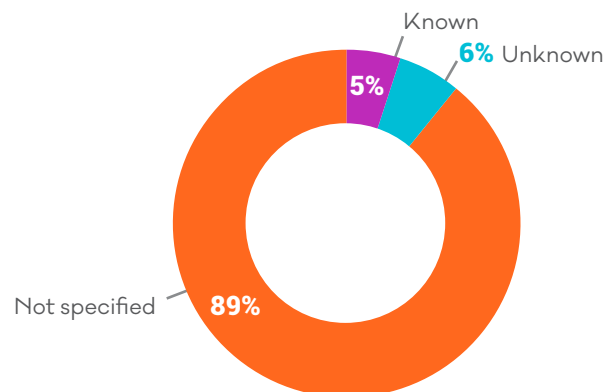


Age breakdown

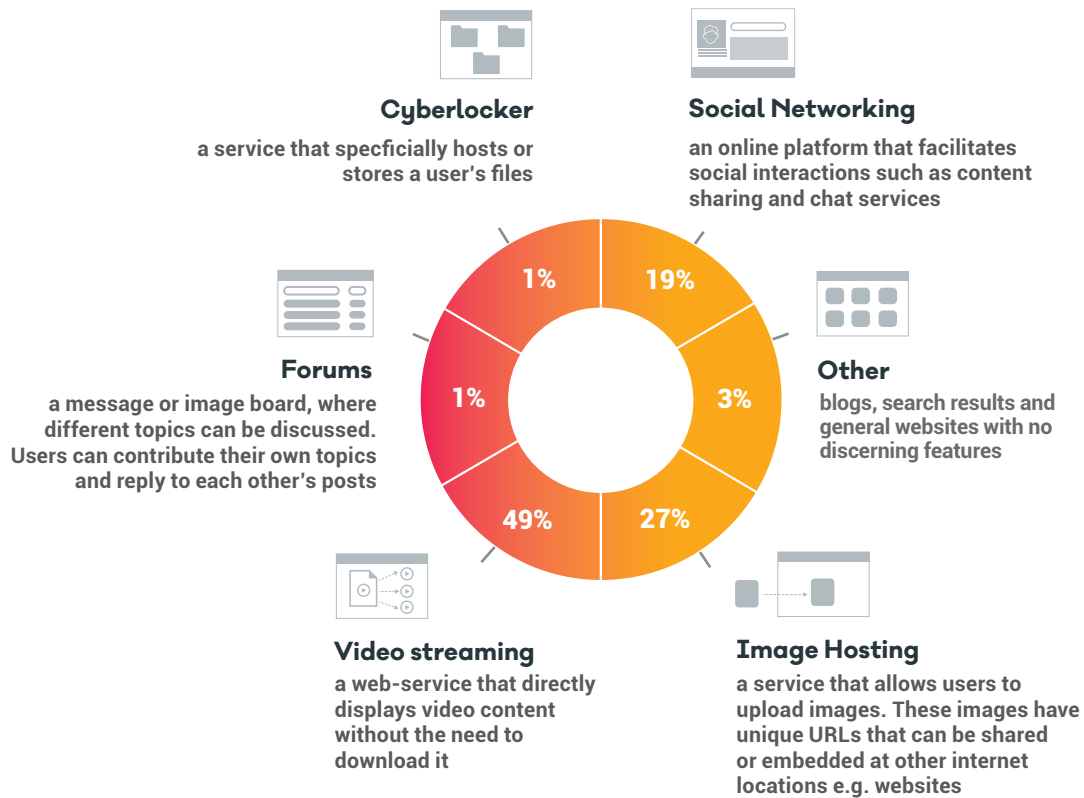
BASED ON THE REPORTER'S DISCLOSURE



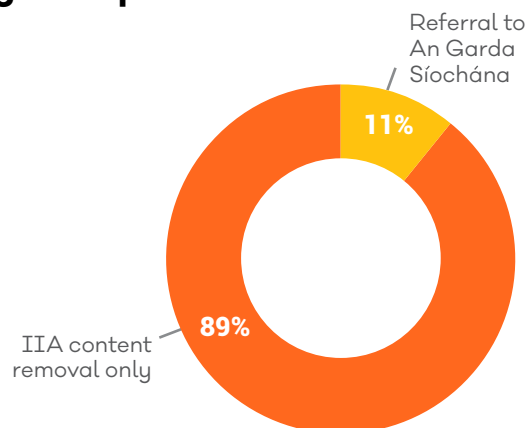
IIA perpetrator



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, Omegle, 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 Gardaí 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

Women's Aid 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

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

Racism & Xenophobia

26% of reports submitted under racism & xenophobia

suspicion by the public, found to relate

to online hate speech



Findings & insights

Between 2017 and 2022 there have been 652 reports of suspected racism & xenophobia reported to Hotline.ie, with 108 of them occurring in 2022. Only 2 reported websites were determined to meet the threshold for illegality under Irish law for incitement to hatred, as it is an extremely high one. Neither two websites were hosted in Ireland.

Of the 108 reports, 26% were found to be related to hate speech, with specific focus on antisemitism and misogyny. 14% related to the war in Ukraine and the refugee crisis. 6% were of threats or harassment made against people due to their status in minority groups. 28% were of adult pornography videos that involved abusive racist elements.

The legal framework under which Hotline.ie can action this type of material for removal is underpinned by the Prohibition of Incitement to Hatred Act 1989. However, the Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022 which was initiated in the Dáil in November, aims to repeal, and replace

the hate speech provisions in the 1989 Act. In relevance to the digital landscape, the Bill proposes to criminalise any intentional or reckless communication or behaviour that is likely to incite violence or hatred against a person or persons because they are associated with a protected characteristic.

Real-world examples of material that currently would not constitute an offence under the 1989 Act e.g. a website that exists to encourage discrimination based on a person's gender and champions the use of violence against them; public social media posts calling for the use of violence against a specific individual due to their nationality.

26%

OF REPORTS WERE FOUND TO BE RELATED TO HATE SPEECH, WITH SPECIFIC FOCUS ON ANTISEMITISM AND MISOGYNY.

14%

OF REPORTS RELATED TO THE WAR IN UKRAINE AND THE REFUGEE CRISIS.

6%

OF REPORTS WERE OF THREATS OR HARASSMENT MADE AGAINST PEOPLE DUE TO THEIR STATUS IN MINORITY GROUPS.

28%

OF REPORTS WERE OF ADULT PORNOGRAPHY VIDEOS THAT INVOLVED ABUSIVE RACIST ELEMENTS.

INAR Member

In 2022, Hotline.ie joined the Irish Network Against Racism (INAR) in our ongoing commitment to combat racism and xenophobia online. INAR is a prominent organisation dedicated to eradicating racism in Ireland. Through advocacy, education, and community engagement, INAR works tirelessly to promote inclusivity, equality, and social justice for all individuals regardless of their ethnic background.



Contact details:

Irish Network Against Racism (INAR)

Website: www.inar.ie

Phone: 01 8897110

Social: @INARireland

Resources



Responding to Racism Guide (ENAR Ireland, 2019)

This guide provides you with information about how and where to report racist incidents, including racist discrimination, racist crimes and hate speech online, as well as how to go about finding redress and how to use existing legislation to address racism.



Crime Victims Helpline Ireland

Website: www.crimevictimshelpline.ie

Freephone: 116006

Text: 085 133 7711

You can also request a call back through their webform. The Crime Victims Helpline is a listening and support service for victims of crime in Ireland. The Helpline also provides information about the criminal justice system, your rights, and signposting to local or specialist support services and other resources in the community.

Financial scams

37 websites attempting to scam Irish residents

or purporting to be Irish services

were taken down



Findings & insights

In 2022, there were 321 suspected financial scams reported to Hotline.ie; of which 39 websites were confirmed to be operating financial scams targeting Irish residents or purporting to be Irish services and were successfully taken down. These referred primarily to online shopping scams (55%), phishing websites (29%) or fake loan sites (16%).

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.

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.

5 Be cautious with personal info

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



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.

- 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 2022, were Revenue, An Post, Irish banks, and 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 321 suspected financial scams, 134 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 321 suspected financial scam reports represent a 48% decrease from 2021. The number of reports had surged in 2021, it is possible that as people became savvy to certain types of scams that had arisen, such as 'smishing' and parcel delivery scams, they were less likely to report on it. Hotline.ie believes financial scams tend to be massively underreported, and we would like to encourage the public to report any website or suspicious links so that these may be actioned before someone becomes a victim. As Hotline.ie can only act to remove this material from the internet, if you have been defrauded, contact your bank and local Garda station as soon as possible with any information or evidence you might have.

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

Partnerships

Working collaboratively, in partnership for good

enhances exponentially national and global response

to tackle online crimes against the most

vulnerable in society



Building partnerships for tangible impact



Working in partnership for good

For 23 years now, Hotline.ie has been providing Irish people and residents with a secure and confidential web-reporting portal where they can report suspected illegal content such as: online child sexual abuse and exploitation, non-consensual sharing of intimate images and videos, racism and xenophobia, and financial scams. With each piece of illegal and harmful content we remove from the internet, there is one less instance of suffering, of re-victimisation.

Protecting Irish people and especially children and young people from sexual abuse and exploitation online and preventing repeat-victimisation is at the heart of everything we do.

Hotline.ie works collaboratively with a diverse mix of partners in law enforcement, Government, academia, tech companies, NGOs, and international partners to make the internet a safer and a more inclusive place for children, young people, and adults alike.

Hotline.ie's work relies on compassionate and resilient human Analysts, who are highly-skilled, police trained and internationally certified, and who assess every single report that we receive, against rigorous standards and by reference to Irish law.

Everyone on the team at Hotline.ie, works with a sense of relentless determination and commitment which is unique to our organisation. Our values act as a reminder of the important work we do, we are open, we strive to be the best at what we do, we care, we respect, we protect.

Our work is supported and co-financed by our members (tech companies) and by the European Union through grant aid funding.

Hotline.ie is a founder member of INHOPE, the International Association of Internet Hotlines. Today, INHOPE brings together over 50 hotlines in 46 countries worldwide (all EU Member States, the UK, Russia, South Africa, North & South America, Asia, Australia, and New Zealand), united in one mission, eliminating child sexual abuse material online. INHOPE exists to support and enhance the work of member hotlines. INHOPE and INTERPOL hold regular joint content assessment training sessions for hotline Analysts to ensure consistency of the assessment process on all levels.

To that end, all Hotline.ie Analysts receive certification after the completion of INHOPE/ INTERPOL training sessions. In addition, member hotlines have access to an extensive programme of webinars delivered by experts in topics relevant to our work. INHOPE also provides a forum where we can exchange information and experience on matters such as health and safety for hotline staff, standardised reporting of statistics, and emerging operational challenges. We actively participate in INHOPE Task Groups and share our expertise, whilst drawing from the collective multi-disciplinary expertise within the INHOPE network.

In 2014, INHOPE launched the Quality Assurance Programme (QAP) with the view of ensuring enhanced compliance and an optimal standard of hotline operation by existing and new members alike. Since the inception of the INHOPE QAP, Hotline.ie has been assessed twice by independent experts and each time found to be compliant and exceeding the minimum standard requirements and has been awarded the INHOPE Quality Assurance Certification for excellent hotline service and standard of operation. When Hotline.ie Analysts classify content as illegal under Irish law and trace

the online origin of the content in question as being hosted in a country with an INHOPE hotline presence, our Analysts alert the relevant hotline through the EU-funded secure international CSAM report management system (ICCAM). If there is no hotline presence in the hosting country, the CSAM report will be subsequently dealt with through appropriate law enforcement channels.

Tackling online child sexual abuse material requires a multipronged approach. It is crucial to affect rapid removal of CSAM from the internet, while ensuring the children in the images may be identified and safeguarded, perpetrators identified and brought to justice. That is why working in partnership with law enforcement is of utmost importance. Our highly skilled Analysts sift through thousands of public reports leading to hundreds of thousands of images and videos to identify quality leads. The content classified as most probably illegal "child pornography" under Irish law is notified to the relevant unit of the Garda National Protective Services Bureau as per agreed procedures. We use the term "probably illegal" as only a court of law can make a judgement as to whether something is definitively illegal under the law. As such, Hotline.ie's triage function should not be misconstrued as criminal investigation which together with evidence gathering to support criminal proceedings is a matter for law enforcement alone.

Hotline.ie is also integral part of the Irish Safer Internet Centre (SIC). The Irish SIC is a unique partnership bringing together ISPCC, Webwise Ireland, Hotline.ie and NPCP. The partner organisations work together to identify emerging online threats, take direct action against them through the delivery of evidence-based services, resources, and programmes, while providing support to children, young people, parents, teachers, with an end-to-end approach.

The Irish SIC provides:

1. Ireland's primary national channel for the public to securely and confidentially report suspected illegal content online see www.hotline.ie
2. 24/7 free confidential listening services for all children up to the age of 18 in Ireland, delivered by ISPCC www.childline.ie
3. free and confidential helpline service for parents and guardians, delivered by the NPCP; they also provide online and face to face training courses for parents – see www.npc.ie
4. Internet Safety Awareness Centre, Webwise, who develop youth-oriented awareness raising resources and training programmes that promote digital citizenship and address topics such as online wellbeing, cyber-bullying and much more. Webwise also organise and coordinate the annual Irish Safer Internet Day events - see www.webwise.ie

Hotline.ie would like to thank all those who have supported our mission and work in 2022. Supports come 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; and we receive critical Grant aid support from the European Union.

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 even abroad. Our work continues every day.

Our members

24 companies, including some of the giants of the internet world through to smaller online service providers operating in Ireland, chose to actively support Hotline.ie in our mission to tackle the distribution and proliferation of child sexual abuse and 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 a 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.

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.

Change begins with reporting

Your safety, our purpose

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