# Internet Hotline Annual Report

INTERNET HOTLINE

Publication of the
National Media and Infocommunications Authority
on the Internet Hotline's activities in 2023

# Table of Contents

## Foreword by the President

Dear Reader,

As the President of the National Media and Infocommunications Authority, I wish to bring your attention to the annual report of our online information and assistance service, which is similar to the report published for the first time last year. It is worth reviewing the work we carry out year after year in order to come to the necessary conclusions from the trends emerging from the figures. The Internet Hotline legal advisory service was created in 2011 as one of the pillars of our social value undertakings in order to make the **internet a safer place for children and adults alike**. Our publication allows one to become familiar with the operation of the Internet Hotline, as well as providing insights into the day-to-day work of the service. Over the last 13 years, the Internet Hotline has dealt with over 17,000 reports, including a great number concerning child pornography, i.e. content related to the sexual abuse of children. Alarmingly, the number of reports requiring measures is increasing year after year, particularly in cases related to the online grooming and sexual extortion of children. It is also apparent that nearly every fifth report was related to some social media platforms.

The rapid and effective handling of violations committed on the World Wide Web **requires international cooperation**. This is why it is of particular importance that the Internet Hotline is a member of the INHOPE international network, which works to combat the online sexual exploitation of children. Thanks to our professional collaboration, we can take action more effectively against content that constitutes the sexual abuse of children.

It is the moral obligation of adult society to protect the younger generations, which is why the National Media and Infocommunications Authority makes the protection of minors one of its key priorities, so young people can be aware of potential online threats and be able to protect themselves and take action against any online violations.

Last year, the Internet Hotline reached out to over 1,700 people in person **through its transformative, educational and awareness-raising** activities. It has reached out to children, young adults, university students, educators, parents and child protection experts through interactive programmes, workshops and conference lectures, as well as round-table discussions.

The sheer existence of the Internet Hotline indicates that it is possible to take action against violations on the World Wide Web. Our thousands of cases attest to the fact that **it is worth asking for help and there is someone out there who cares**.

András Koltay
President
National Media and Infocommunications Authority



## Foreword by the Head of Internet Hotline

2023 was an important year for us, as there was more coverage on digital child protection and the exposure of children to online threats than ever before, which meant there was increased interest in the activities of the Internet Hotline. There was a great deal of interest in our experience, as domestically, over our 12 years of operation, we have amassed by now an unparalleled body of **specialised expertise and practice** in dealing with online violations. I am proud of my colleagues, as apart from dealing with the analysis of mentally extremely taxing, difficult content and their committed day-to-day work, they also visited a great number of schools, universities, conferences and professional events to report on their activities. In summary, I feel our now four-member team has performed well over the last year, for which I am **sincerely grateful** to them as well as to the Authority for backing us up with their full support.

However, the hotline is always about the reports. But what are these reports, exactly? These are sometimes distressed, desperate pleas for help, or preventive, warning signs to prevent others from suffering harm. In all cases, **we are honoured by the trust** the reporting persons place in us as they ask for our help or provide us with a warning. I am grateful for the fact that, in 2023 alone, there were 2,047 instances of a parent, child, everyday user or foreign hotline consciously and responsibly taking action for the sake of a better, safer online world. I continue to urge all internet users to help our work by contacting us **and filing reports, standing up for their own rights or those of their children whenever they are faced with online violation!**

Dorina Csalár
Head of Department

National Media and Infocommunications Authority • Hungary

INTERNET HOTLINE

# Basic information



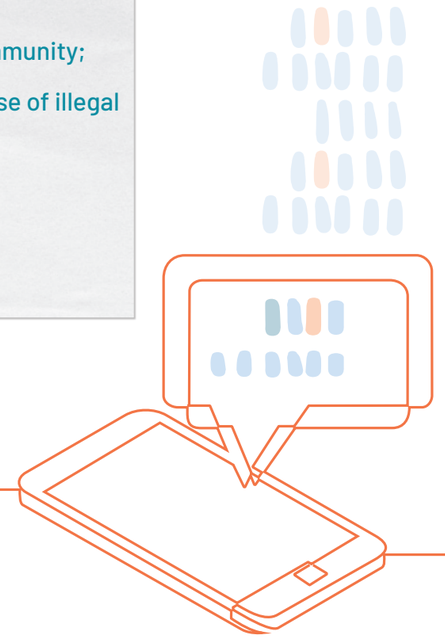
## Who are we?

The Internet Hotline (hereinafter IH) is an online information and assistance service operated by the **National Media and Infocommunications Authority** (hereinafter NMHH) since 2011 as a public interest service, working to make the Internet a safer place. Online content can be reported to the IH when the reporting person suspects that it is illegal or harmful to the development of minors. Over the past **nearly 13 years, we have handled more than 17,000 reports.**

## What can be reported?

At the IH, we receive reports about content available on the Internet in eight different categories:

- content published without consent;
- child pornography;
- online harassment;
- phishing content;
- racist content, incitement against a community;
- content promoting or encouraging the use of illegal psychoactive substances;
- content inciting or promoting illegal acts of violence;
- other content harmful to minors.





In the category of **child pornography**, reports can be filed on cases related to the online sexual abuse or exploitation of children, including content in which minors (whether real or not existing) under 18 years of age are displayed sexually in a highly indecent manner in sexually arousing positions.

In the category of **content published without consent**, reports can be filed in relation to images, videos, audio recordings or other personal data concerning a person or their child published online without their permission or consent. One of the common forms of content published without consent is intimate image abuse.

In the category of **online harassment**, concerned parties report on intentional, repeated online abuse taking place over an extended period of time, often in public. The harassment can be aimed at annoying, humiliating, shaming or even taking revenge on the victim. These can involve the use of fake profiles, profile hacking, defamation, threats and rumour-based websites.

Reporting persons can choose the **data phishing** category when they become aware of online content that is intended to deliberately mislead and defraud persons of their personal (name, address, birth data, username, password) or financial (bank account number, bank card identification data, PIN) data. These typically concern instances of online financial fraud.

Reports can be submitted in the category of **racist content, incitement against a community** in relation to content that incites hatred against some community or its member, or inciting others to commit violence based on some feature of the community. Such features may include membership of a particular national, ethnic, racial or religious group, gender identity, sexual orientation or disability.

**Content promoting or encouraging the use of illegal psychoactive substances** includes websites, e-mails and messages related to the trade in or encouraging the use of drugs.

Content inciting acts of terrorism, promoting or contributing to terrorism can be reported to the IH under the category of **content inciting or promoting illegal acts of violence**.

All forms of content that the reporting person deems to be harmful to the mental, spiritual, moral or physical development of minors and that does not fit into any of the other reporting categories can be reported under the **other content harmful to minors** category.

## Where and how to report?

Users can contact us (https://nmhh.hu/internethotline/) **via the form** available on the website (https://e-nmhh.nmhh.hu/e-nhh/4/urlapok/esf00120/) or **via e-mail** (**internethotline@internethotline.hu**).

When submitting a report by using the form, the reporting person does not have to provide their name and contact details and can submit their report anonymously. In the latter case, the IH staff will investigate the content of the report, but are unable to respond to the reporting person.

Partner hotlines abroad can report through the **ICCAM** system operated by INHOPE (International Association of Internet Hotlines), the international association against child sexual exploitation.

## Framework for operation and procedure

The rules governing the operation and procedure of the IH are set out in Sections 149/B to D of Act C of 2003 on Electronic Communications (hereinafter the Act on Electronic Communications) and the IH Rules of Procedure, which forms Annex 4 to the NMHH's Rules of Organisation and Operation.

At the IH, we investigate and provide legal assistance and technical advice for protecting public interests in the safe use of the internet. The investigation based on a report is **not an official procedure**, and we cannot exercise official powers or use official means in the course of our activities. The report does **not constitute a public authority case**. Accordingly, the IH cannot oblige anyone to remove the content objected to by the reporting person, nor can it impose a fine.

The Act on Electronic Communications also regulates the basic rules of data processing and data forwarding related to the reports, pursuant to which the IH has **statutory data processing authorisation** in relation to the reports submitted to the Authority.





## How can we help? What happens to the report?

Our primary goal is always to provide the reporting person with **the most effective assistance**, taking into account the specific circumstances of the case. Furthermore, we strive to ensure that the service provider that made the reported content (which is likely to constitute a violation) available remedies the situation as quickly as possible.

As soon as a report is received by the IH, we examine its content. The most important thing is to provide an exact URL (link) to the specific online content; without this, we cannot identify the objected online content as the IH has no possibility of reviewing the entire content of websites.

We then examine the URL to see whether the social media site or other website concerned has its own reporting form or complaint management procedure. If so, we inform the reporting person and suggest that they should, if possible, first take action themselves, for which we provide them with the necessary assistance.

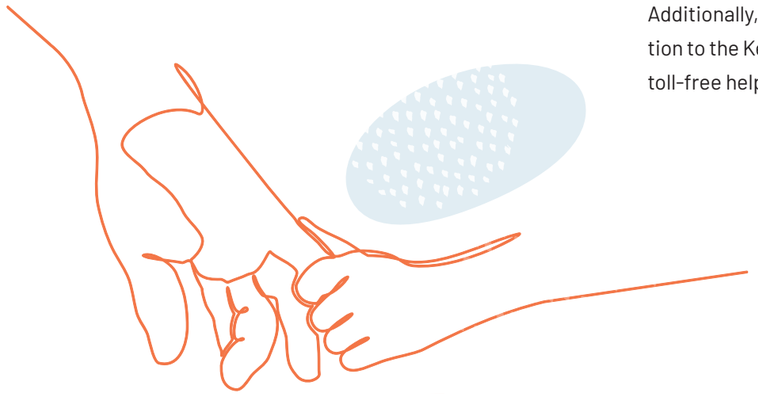
If the reporting person has previously submitted a report to the social media site, content or hosting provider but has not been successful, has not received a response or the site concerned does not have a reporting form, the IH will contact the site and request an investigation into the issue objected to by the reporting person.

In all cases, we inform the reporting person of the IH's procedure, the feedback from the social

media site and the content or hosting provider, as long as they have provided their e-mail address.

If the report raises the possibility of a criminal offence to be prosecuted other than upon a private motion, we will forward the report to the investigating authority within one working day of the detection.

It is important that each case is treated individually. If the report suggests that the reporting person is a minor, the IH will respond in a child-friendly manner, in a direct and friendly tone, and in a clear and understandable way for the child. In addition to dealing with online abuse, we encourage children who come to us to talk to an adult they trust so they won't be left alone with their problem. Additionally, in all cases, we also draw their attention to the Kék Vonal Child Crisis Foundation's 0-24 toll-free helpline (116-111).



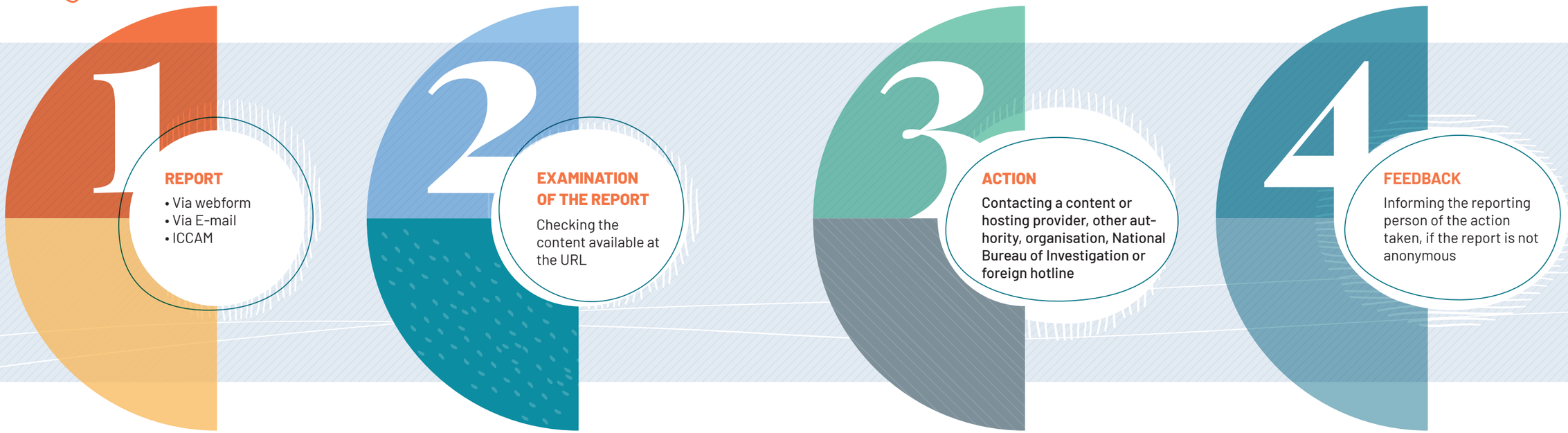




## In what situations are we unable to help?

The IH is not entitled to investigate:

- content appearing in media services and press products;
- unsolicited electronic advertising (spam);
- copyright litigation;
- consumer complaints about webshops;
- privacy notices, or the lack thereof;
- editorial information, or the lack thereof;
- illegal film downloading sites;
- and the investigation of online abuse that falls within the exclusive jurisdiction of another authority, court or other public body.



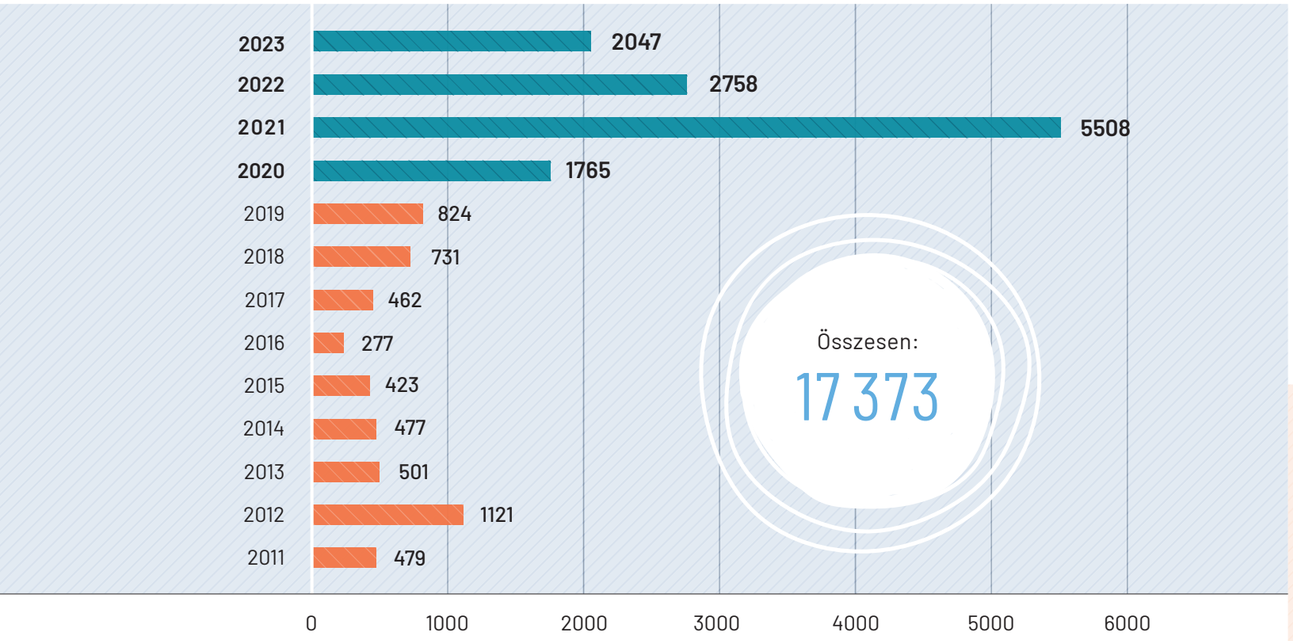
# Experiences in 2023



## Experiences in general

Focusing solely on the period since the launch of the IH in 2011, it becomes clear from the figures that **the last four years are of considerable importance** in the advisory service's history. The reason for this is that the number of reports has drastically increased since 2020, even though this activity peaked in 2021 and there has been a slight decline since then, the number of cases is still higher than before the coronavirus pandemic.

**Total annual number of reports received between 2011 and 2023**




However, the figures themselves do not show the tendency unequivocally experienced by the IH's analysts: year after year, there are a growing number of serious, more complex cases, and an increasing number of reports that necessitate more extensive investigation and measures based on the investigation that require more time and attention, as well as more intensive communication with the investigating authorities and also more extensive correspondence with the reporting person and the service provider in question. The work load of the analysts has clearly increased over the years. Partly due to this fact, a further analyst has joined the advisory service in 2023, which now has three full-time analysts.



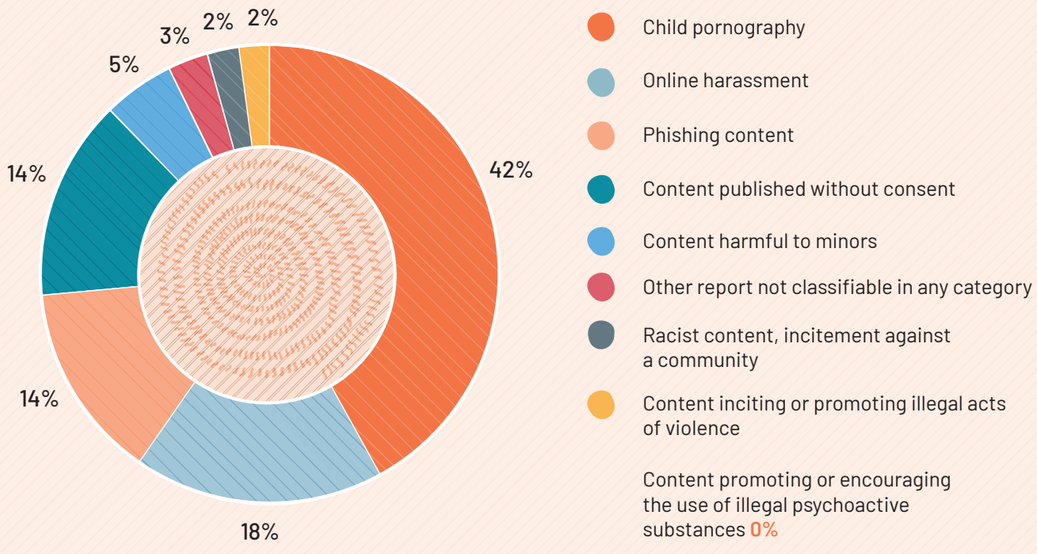
## Proportion of reports received in 2023 in the various reporting categories compared to the total number of reports

Just as in previous years, in 2023, **most reports were related to the online sexual abuse of children**, in the category of child pornography, representing **42 percent** of all reports. Given the high exposure of children to online threats, we expect most reports to be filed in the same category this year as well.

The greatest increase is in the proportion of reports of phishing content, which shows a 6 percent increase in the phishing content category compared to the previous year. The experiences of the IH show that the issue of online financial fraud is increasingly pronounced, as the perpetrators use often-changing and increasingly sophisticated methods; as such, we are continuously developing the effectiveness of our procedure.

The proportion of reports in the content published without consent and online harassment categories has also increased. The nature of the reports in these two categories remains unchanged in terms of the issues raised; however, there has been a significant increase in more serious cases requiring action.

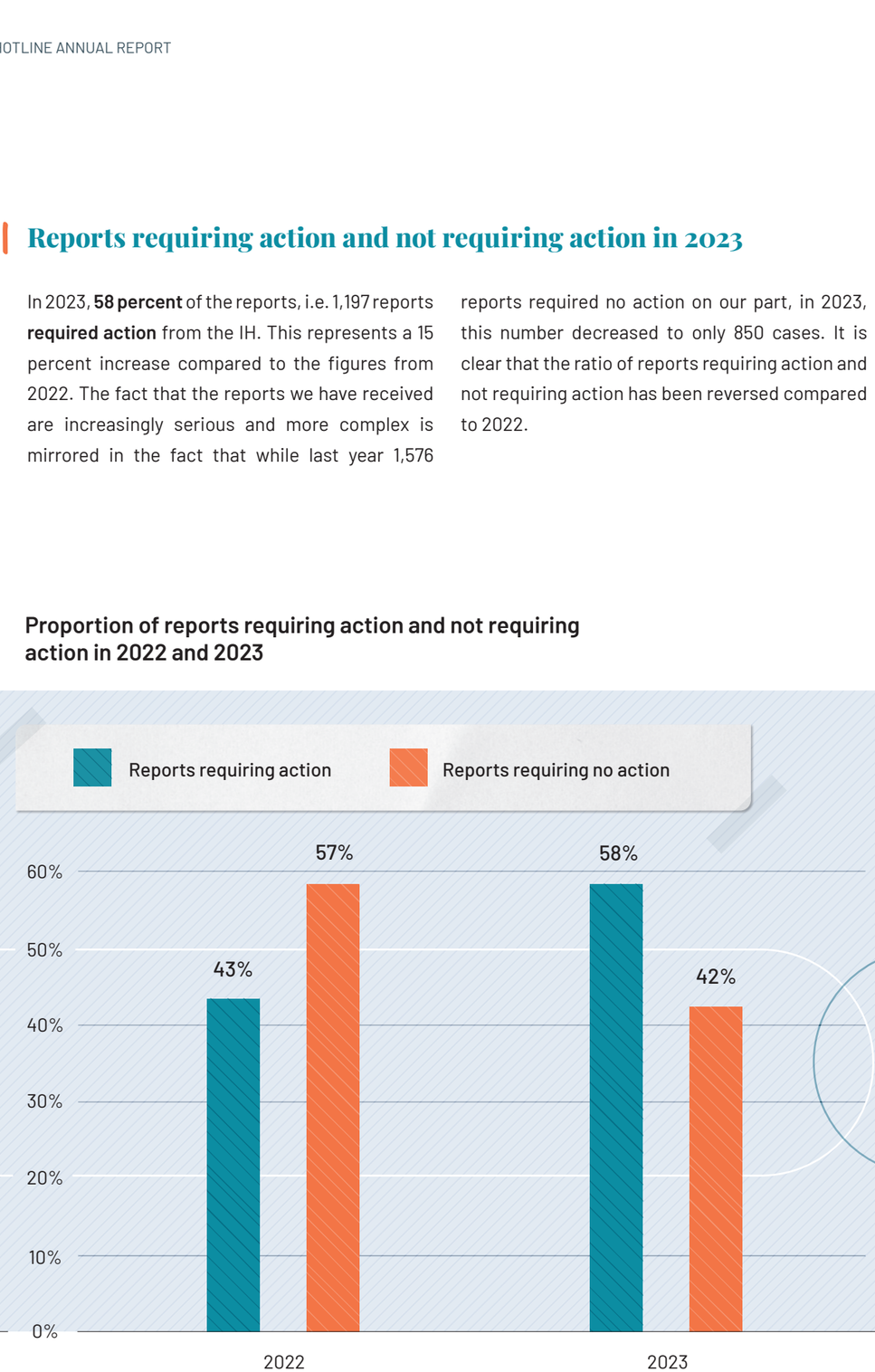
**Proportion of reports received in 2023 in the various reporting categories compared to the total number of reports**



## Reports requiring action and not requiring action in 2023

In 2023, **58 percent** of the reports, i.e. 1,197 reports **required action** from the IH. This represents a 15 percent increase compared to the figures from 2022. The fact that the reports we have received are increasingly serious and more complex is mirrored in the fact that while last year 1,576 reports required no action on our part, in 2023, this number decreased to only 850 cases. It is clear that the ratio of reports requiring action and not requiring action has been reversed compared to 2022.

**Proportion of reports requiring action and not requiring action in 2022 and 2023**








## Reports from parents

Even prior to 2023, reports were regularly received from parents on online violations impacting their children or online content that they believed to be detrimental to their child's development. However, last year there was **sharp increase in reports from parents**; 55 reports were filed in which the reporting person clearly acted in the capacity of the legal representative of their child by filing a report on an ongoing violation.

In terms of the categories of reports, the majority of the reports – over 70 percent – were filed in the category of content published without consent, along with reports in the categories of child pornography, online harassment and content harmful to minors.

**In the following, we will outline some of the more serious reports filed by parents:**

more parents indicated that their children had been tricked into providing sexual content through Snapchat and were then blackmailed by threatening to share the recording with their friends if they refused to pay

an adult man attempted to persuade a 13-year-old child to meet him in person for sexual purposes via Facebook Messenger

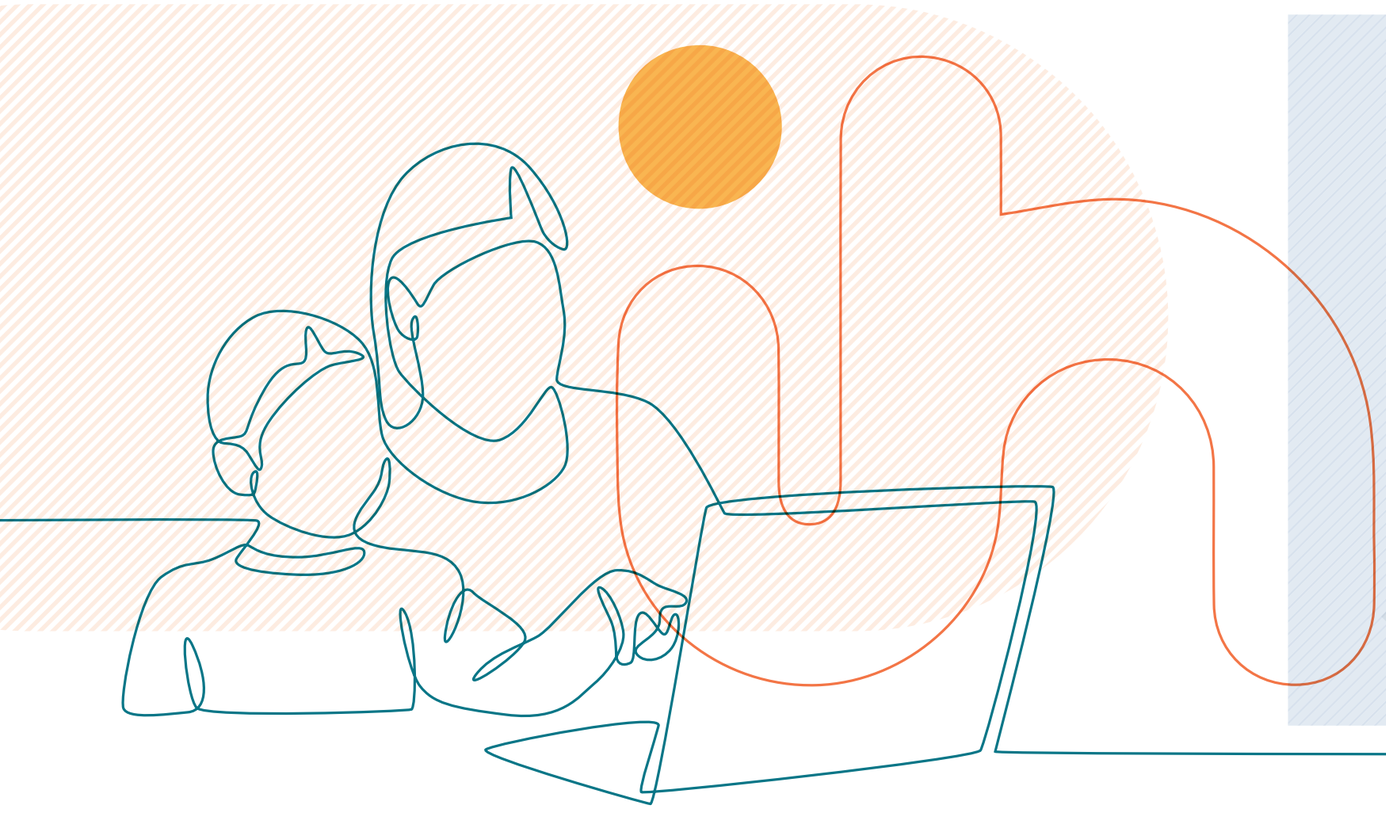
multiple reports were filed of family members sharing photos of a child on social media – including nude photos – or creating a profile on behalf of a child without the permission of the child's legal representative, in other words the child's parent

they attempted to trick an 11-year-old child into providing sexual content via Discord

more parents submitted reports of a video available through TikTok, which they considered to be harmful to minors

**We pay particular attention to reports from parents**. In all cases, when there is a possibility of the online sexual exploitation of children or a criminal offence to be prosecuted other than upon a private motion, we confer with the staff of the National Bureau of Investigation and act in cooperation with the Bureau. In multiple instances, we have liaised between the National Bureau of Investigation and the reporting parents. It is promising that several parents indicated that, concurrently with submitting a report to the IH, they also filed a police report.

Alarmingly enough, our experiences show that there is a continuous increase in the number of reports from parents concerning the online grooming of children and sextortion. However, these are still cases with a more fortunate outcome, as **the child** was safe, and **was not alone with their problem**; they **confided in their parents instead**, and they searched for a solution together.







## Developments in reports related to social media platforms in 2023

Of all the reports in 2023, **every fifth report** was related to some social media platforms.

Similarly, to the statistics from 2022, most of the reports received by the service in 2023 were related to Facebook. Whilst in 2022, the IH dealt with 141 reports related to Facebook, in 2023 this number increased to 186.

Apart from **Facebook**, reports were frequently submitted in relation to content available through YouTube, Instagram and TikTok.

Based on the reports, it is noticeable that the violations have multiplied in relation to the increasingly popular platform of Discord. In 2023, we received 17 reports related to violations on Discord.

**Distribution of reports by platform in 2022 and 2023**

| Platform | 2022 | 2023 |
|---|---|---|
| Facebook | 141 | 186 |
| YouTube | 29 | 71 |
| Instagram | 29 | 46 |
| TikTok | 12 | 30 |
| Reddit | 42 | 26 |
| Discord | N/A | 17 |
| Twitter | 9 | 9 |
| Snapchat | 4 | 9 |

# Key phenomena



## Sexting

Sexting is when two people send each other sexual content, usually photos and videos, of themselves or each other. This is not necessarily illegal; in the case of adults, it becomes a violation when the recordings were made without permission or published online without consent. The situation is different in the case of sexting between a minor and an adult, as certain conduct related to the pornographic recordings of minors under 18 years of age may constitute child pornography.

## Online grooming

Online grooming is the process during which an adult attempts to gain the confidence of a child online, typically through social media sites, online games or chatrooms.

Based on the reports submitted to the IH, we can differentiate between two different types of grooming:

**the first is when the adult creates a fake profile and approaches the victim as their peer;**

**the second and similarly frequent is when the groomer is present as an older friend, supporter or experienced mentor.**

The process takes place over a long period of time, based on a consciously developed strategy. The first step of getting acquainted with and befriending the victim is followed by the development and intensification of the relationship. The groomer's goal is to inspire confidence in the child and become their main emotional support. On the third level, the perpetrator seeks to determine how risky it is to continue the relationship, asking the child whether their loved ones or friends know about it. After evaluating the risks, the groomer seeks to isolate the victim from their surroundings in order to become the sole person they trust. Finally, at the end of the process, they might demand sexual content from the child or invite them to a personal meeting for sexual purposes.

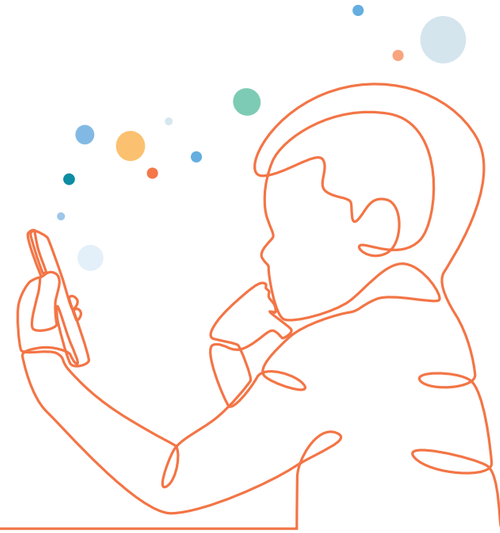


## Sextortion

The phenomenon of sextortion, which can impact children and adults alike, is not uncommon in reports related to cases of child pornography, content published without consent, or online harassment. Sextortion, a blend of the words "sexual" and "extortion" refers to the threat of sharing content of a sexual nature if the victim fails to satisfy certain demands. The perpetrators use various means, often manipulation, to get hold of the victim's recordings. With the obtained images, the perpetrator's aim is to obtain more pictures, demand money or persuade the victim to meet in person.

## Self-generated child sexual abuse material

In relation to the above-mentioned phenomena, it is important to distinguish self-generated child sexual abuse material, which children make of themselves, under duress, on a non-consensual basis. They do this, for example, due to peer pressure or as a result of online grooming or sextortion. The experiences of the IH analysts show that it is not uncommon for very young children to be persuaded to broadcast nude, semi-nude or sexually explicit content on a webcam or to create and forward such images of themselves to others.



## Artificial Intelligence-generated sexual content

The experience of hotline analysts shows that the changes brought about by Artificial Intelligence are also manifested in relation to the online sexual exploitation of children. This mainly refers to the way perpetrators use generative Artificial Intelligence to process previously acquired recordings of actual children to create content depicting child sexual abuse. Reports of this nature have only appeared sporadically in the practice of the IH, yet these figures are set to increase based on international trends. Although artificially created content does not represent the physical, sexual abuse of real children, such content is still harmful and illegal and the creation of such content is also punishable under the domestic Criminal Code.

## Intimate image abuse

A substantial part of reports submitted in the category of content published without consent comprise reports concerning intimate image abuse. Intimate image abuse is the sharing of intimate images or videos without the consent or permission of the person featured in the recording. The motivations for the abuse typically include revenge and humiliation. Although this is a serious legal infringement, the experience of the international hotlines shows that the intimate images of adults are frequently abused.





## Cyberbullying

Cyberbullying is based on a perceived or real dominant position, whereby the perpetrator harasses the victim intentionally, repeatedly, over a prolonged period of time in order to annoy, to humiliate or take revenge on the victim by the means of electronic communication devices. All this is not limited in space and time, and therefore the victim is constantly exposed to harassment, not just in the classroom during school hours within the classroom walls. Since the conflict is online and therefore in the "public eye", even within moments, a wider community or the whole school can witness it, which increases the victim's sense of shame greatly. Within the category of online harassment, not many reports are received about cyberbullying. Although the experience of the workshops held by the IH clearly shows that it is a common phenomenon among schoolchildren, it is not reported in significant numbers. Hotlines abroad have also confirmed the IH's findings that few minors seek for help in such cases. One of the reasons for this is that children believe they can resolve the situation themselves, for example by blocking and reporting the bully on the platform.


*The word cloud contains the responses of children asked during our workshops to the question of what they consider to be online harassment.*

# KEY REPORTING CATEGORIES



Number of reports received in 2023 in the different reporting categories and their proportion of the total number of reports

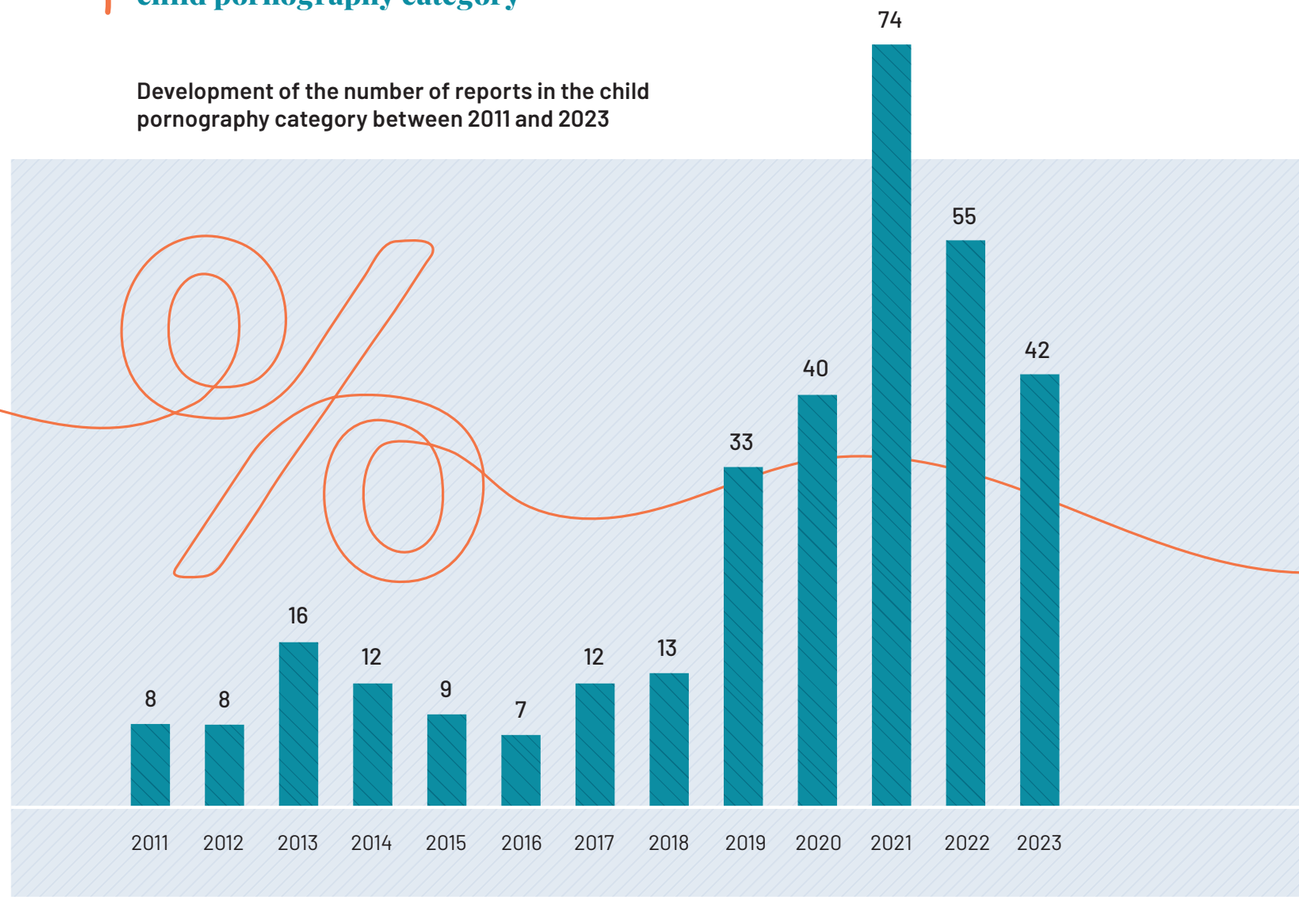
| Reporting category | Number of reports | Proportion |
|---|---|---|
| Child pornography | 850 | 42% |
| Online harassment | 375 | 18% |
| Content published without consent | 290 | 14% |
| Phishing content | 290 | 14% |
| Other ontent harmful to minors | 98 | 5% |
| Other report not classifiable in any category | 64 | 3% |
| Content inciting or promoting illegal acts of violence | 35 | 2% |
| Racist content, incitement against a community | 34 | 2% |
| Content promoting or encouraging the use of illegal psychoactive substances | 11 | 0% |
| Total | 2047 | 100% |

Based on the number and proportion of reports, it appears there were four main categories of reports in 2023: **child pornography, online harassment, content published without consent** and **phishing content**. These can be considered the key reporting categories, with the other four categories representing only 10 percent of all reports.



## Online sexual abuse of children: child pornography category

Development of the number of reports in the child pornography category between 2011 and 2023




In the category of child pornography, reports are received on conduct, phenomena and content related to the online sexual abuse and exploitation of children. First of all, it is important to clarify what is considered to be child pornography in the terms of domestic legislation before examining the other cases encountered by the IH above and beyond such content.

## What qualifies as child pornography in domestic regulations?

This category concerns **recordings of the sexual abuse of children**. In light of domestic terminology, pursuant to the Criminal Code of Hungary, child pornography content is defined as pornographic footage depicting a person under the age of eighteen, which depicts sexuality in a grossly indecent manner, in a way that is purposefully aimed at arousing sexual desire. Grossly indecent exposure means that the video shows the child's genitals or depicts the child engaged in a sexual act, either as an active or passive participant.

An important change compared to previous years is that, since the amendment to the act in 2021, child pornography can also extend to recordings that are not made of a real child, but which are realistic, i.e. deceptively similar to real content. These can include recordings in relation to which the ordinary observer cannot determine whether they feature real children or not. As such, Artificial Intelligence-generated child sexual abuse content may also be punishable. In the case of recordings of a real child, one of the requirements is that the child should be recognizable and identifiable, although the depiction itself doesn't necessarily have to be realistic, which means this could extend to paintings.

It should be noted that – in line with the practice of other INHOPE member hotlines, as well as the Luxembourg Guidelines established in 2016 by 18 international organisations – apart from the term child pornography, the IH also uses the term **Child Sexual Abuse Material**, as this, amongst other things, clearly and unambiguously expresses that **the act can never be considered consensual**.



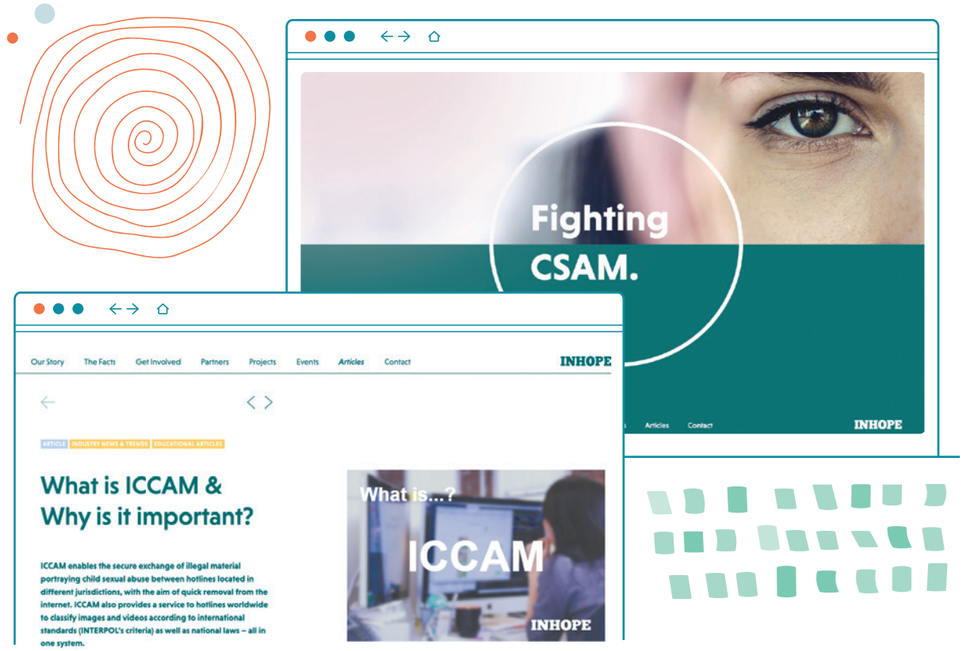


## Special procedures of the Internet Hotline

We **give priority** to all reports that may give rise to suspicion of the online sexual abuse of children. In the case of reports received in the category of child pornography, the IH takes the necessary action **within one working day** of receiving the report.

If the reported content may constitute child pornography and is available on a Hungarian server, the report is forwarded to the **National Bureau of Investigation's Cybercrime Department** for further investigation.

If the reported content may give rise to suspicion of child pornography offences but is stored on a foreign server, we forward the URL included in the report to **the hotline of the country hosting the content**, requesting them to investigate the matter. We file our warning through the ICCAM system.




ICCAM is a secure software tool that can collect, categorise, make available and share URLs pointing to child sexual abuse material with hotline analysts for further action. ICCAM is used by INTERPOL in addition to the member hotlines.

## What are the experiences of the Internet Hotline?

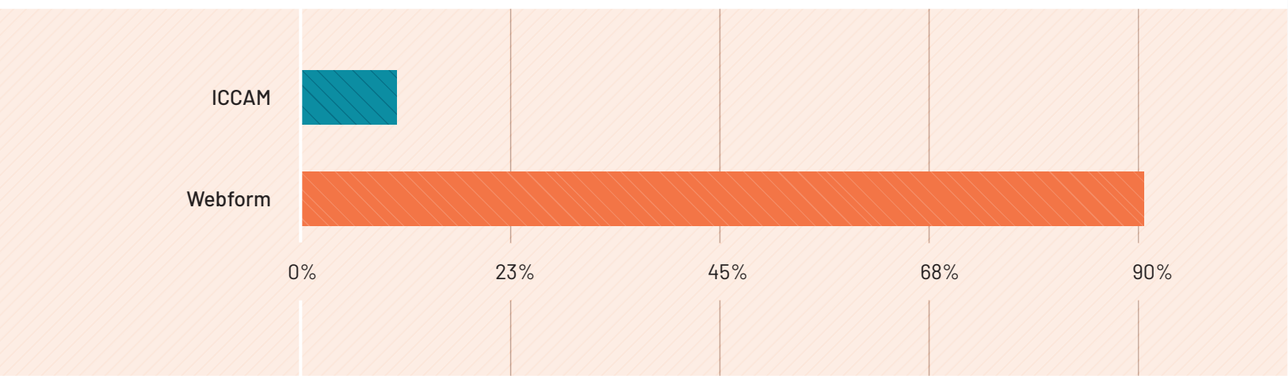
Since 2019, it has been a noticeable trend that **the highest number of reports were received** in the child pornography category, **in relation to the online sexual abuse of children**. Although the number of reports decreased in 2023, still **42 percent** of all reports were received in this category, for a total of **850 reports**. The downturn in 2023 was due to the fact that compared to previous years, fewer reports were received from foreign hotlines through the ICCAM system.

In the case of nearly 17 percent of the reviewed reports, so nearly **1 in 6 reports** received in the category of child pornography, based on the analysts' assumption, the content was **produced during sexting**. In the case of nearly 17 percent of the reviewed reports, so nearly **1 in 6 reports** received in the category of child pornography, the recording was determined as **having been lured** from the child **in the course of online grooming**.

The individual reports may contain multiple URLs leading to what the reporting person assumed to be the sexual abuse of children, which are individually examined by the analysts. In 2023, **1,434 URLs** were submitted to the IH for review from users and foreign hotlines.

**51.4 percent of the examined URLs, a total of 737, were classified as child pornography.**

**Number of reports received via form and e-mail and through the ICCAM system operated by INHOPE**






**The following statistics pertain to the URL addresses examined by the IH, based on which they were classified as child pornography.**

**Distribution based on the setting in which the content was recorded**

| | |
|---|---|
| home environment | 64.45% |
| indeterminable | 25.9% |
| photo studio | 11.1% |
| other public space | 8.9% |
| swimming area / beach | 3.6% |

**In terms of the reports processed by the IH, the most common countries providing hosting services**

| | |
|---|---|
| Hong Kong | 25.4% |
| Russia | 18.3% |
| USA | 10.7% |
| The Netherlands | 8.8% |

**By content type**

| | |
|---|---|
| indeterminable | 40.0% |
| image captured via webcam | 38.2% |
| self-generated content | 36.6% |
| cropped image | 17.6% |
| model photo shooting | 11.1% |
| nudist content | 3.4% |

**by sex of the victim**

| | |
|---|---|
| girl | 71,2% |
| boy | 2,3% |
| both | 2,4% |
| indeterminable | 24,1% |

**By age of the victim**

| | |
|---|---|
| 3–7 years of age | 3.8% |
| 8–12 years of age | 34.3% |
| 13–18 years of age | 50.0% |
| indeterminable | 11.9% |

## Online harassment category

The number of reports received in the category has increased compared to 2022, significantly impacting the proportions as well. Whilst in 2022, 13 percent of the reports concerned online harassment, in 2023, this figure has **increased to 18 percent**. The reports received in the category of online harassment typically object to profile hacking and the creation of fake profiles on social media platforms, alongside defamatory comments and posts on social media. Harassing, abusive, threatening or humiliating messages received through chat applications are also frequently featured in the reports.

## Content published without consent

In the category of content published without consent, both the number of reports and their proportion have increased compared to the data from 2022, with the latter showing **an increase from 10 to 14 percent**. The category typically includes reports concerning images, videos and other personal data published on social media platforms and other websites. 36 percent of the reports received in the category in 2023 were tied to social media platforms such as Facebook, Instagram, TikTok and YouTube.

Just as in previous years, last year also yielded **an exceptionally high incidence of intimate image abuses** within the category. In 2023, this represented one-third or **33 percent** of all the reports in the category compared to 39 percent in 2022. The analysts of the IH feel this tendency and high rate will most probably remain unchanged in the years to the come, as the number of violations is not expected to decrease.



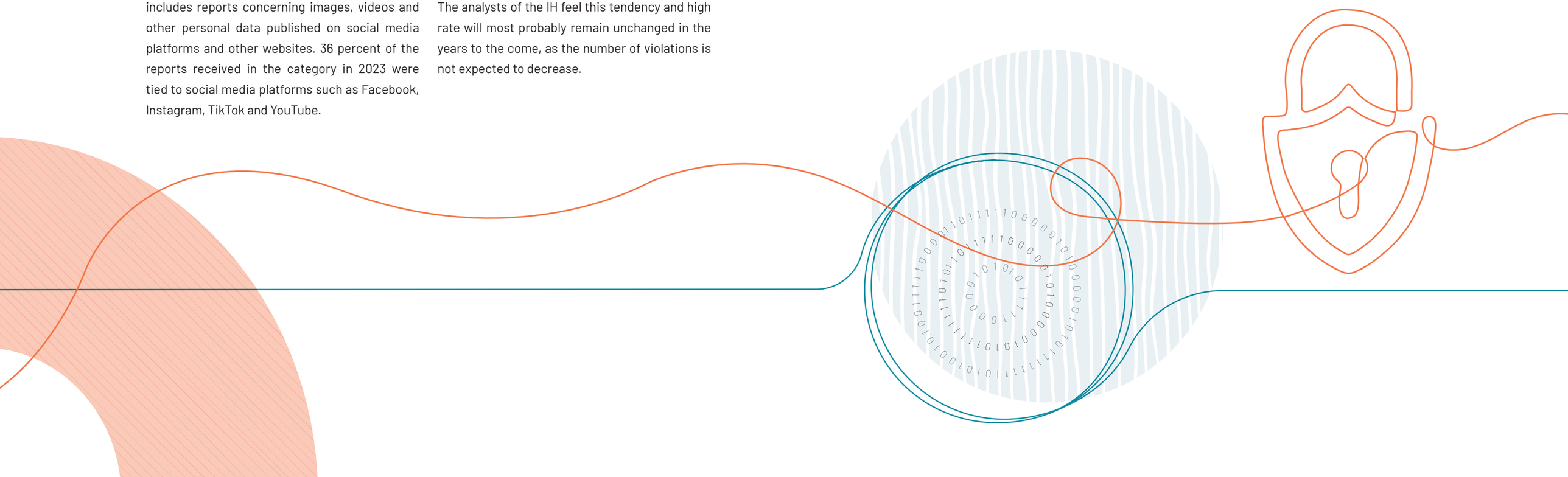


## Phishing content category

The greatest change has taken place in the phishing category. The incidence of such reports has increased from 8 to **14 percent, which means it has nearly doubled** since 2022. In 2023, the number of reports has reached its highest level since the advisory service was launched in 2011, with a total of **290 reports**.

Data phishing is a form of online fraud where perpetrators try to trick users into providing sensitive information, such as personal or financial data. The reports received in the category referred to the widest range of phishing attempts. It is common practice for perpetrators to pose as financial institutions or various service providers – such as parcel delivery or streaming services – online.

The IH has already experienced in 2022 how **the incidence of reports related to online financial fraud is continuously increasing**; therefore, in reaction to this trend, in the autumn of 2022, it began to cooperate more closely with **the staff of the National Bureau of Investigation's Intelligence Unit**, maintaining **intensive cooperation** throughout 2023.



# Cooperation and other activities



## Our partners

### Hungarian National Police Headquarters (ORFK) National Bureau of Investigation of the Rapid Response and Special Police Service

The IH's main domestic partner is the National Bureau of Investigation; our analysts are in daily contact with their colleagues in the **Cybercrime Department**, particularly in relation to two categories: in the category of child pornography in relation to the online sexual abuse of children and, since autumn 2022, in the category of phishing content due to the increased number of reports related to online financial fraud. In December 2023, the NMHH and the ORFK entered into a **cooperation agreement**, concerning and strengthening the ties between the IH and the NNI.

Apart from the above, the IH contacts the investigative authority whenever a report raises the possibility of a criminal offence to be prosecuted other than upon a private motion.

### INHOPE

The cooperation between the IH and INHOPE looks back on more than a decade of history, after the advisory service joined INHOPE, the international organization fighting against the online sexual exploitation of children, in 2012, bringing together hotlines into a global network. INHOPE was established in 1999, with the participation of nine hotlines, and its main goal is still to make online content that qualifies as child pornography unavailable, as well as to aid the work of investigative authorities in uncovering criminal acts tied to such content. INHOPE regularly organises special, unique training sessions – occasionally with the involvement of Interpol – for hotline analysts, alongside the regular exchange of experience between the various hotlines. INHOPE currently coordinates the activities of 54 hotlines in 50 countries of the world.



### Integrated Right Protection Service

The Integrated Right Protection Service is responsible, among other things, for protecting the rights of children in specialized care by coordinating the work of child rights advocates. In the summer of 2023, the IH entered into a **cooperation agreement** with the Integrated Right Protection Service, in particular to ensure that its messages reach the most vulnerable children and to support the work of child rights advocates who work under heavy workload. The IH set out to present the activities and the range of assistance that the IH can provide to child rights advocates, as well as to enhance the experts' knowledge of safe internet use and online threats. As a part of this cooperation, the two organizations posted **awareness-raising posters** in nearly **4,500 public education institutions**. The goal of the posters was to remind children that their rights also apply online and, in the event of a violation, **they are entitled to protection and they have someone to turn to**.

The service also has an intense relationship with the Kék Vonal Child Crisis Foundation, the International Children's Safety Service, and foreign organizations including the British Revenge Porn Helpline and the American National Center for Missing & Exploited Children, NCMEC.

### Social media platforms

One of the tools for the IH to provide assistance effectively is the **well-developed partnerships** that provide it with **direct contact** and rapid access to the major social media platforms. As part of these efforts, some service providers operate **dedicated channels of communication** for those who join their partnership programs and provide **priority moderator attention** to content flagged by our organization.

Since February 2021, the IH has been the member of the **TikTok** Community Partner Program, which is a significant achievement as many of the platform's users are children, who sometimes spend several hours a day watching TikTok videos. Additionally, the IH is also a member of **Meta**'s partner program, which covers Facebook and Instagram, but it can also contact the employees of **Google** and **YouTube** directly as well. In June 2023, the IH was amongst the first to join **Discord**'s Trusted Reporter program. That latter development is of particular significance, as based on the experiences related to the reports, the IH felt that Discord's chatrooms can serve as the platform for the online grooming of children for sexual purposes and sharing child pornography content.

## Educational, outreach activities

As stipulated in the Electronic Communications Act, the IH's **task is providing information and shaping social attitudes**, which is typically fulfilled in the form of lectures. In 2023, the IH's colleagues **reached out to over 1,700 people** by discussing online threats and risks, as well as the possible solutions, and presented the work of the IH in the course of **more than 60 lectures**.

We regularly give lectures to children and young adults in public educational institutions, as well as to the students of higher education institutions and professionals working with children, including school psychologists and child rights advocates apart from teachers and parents. Additionally, the IH is regularly invited to professional conferences and round-table discussions.

The IH's lectures place great emphasis on interactive elements. The various online phenomena are presented to children through the IH's reports in the form of practical examples, cases and questions, which they deal with first in small-group, and then in whole-group discussions. This frequently leads to discourse or even debates and our experiences show that, through the individual cases, it is easier for them to identify with the victim's situation. Amongst other things, we seek answers to the following questions: Would you intervene if you witnessed online harassment? What would you do if someone misused your friend's intimate picture? **Would you ask for help if you fell victim to an online violation? How can you determine that the stranger you are chatting with is not well-intentioned? Do you agree that it is not the victim's fault?**

**"It answers all our questions and reminds us that you can still live a normal life even after making a mistake."**

**"We were told things we had never heard about before."**

**"It showed us solutions for various situations."**

*Feedback of children received on IH workshops.*





## What are the kids saying?

In the course of the lectures for children, we gain a great deal of insights into their attitude to certain issues and how they think about things, which is a highly useful experience. The IH strives to put this information to use in its day-to-day work and further lectures.

One of the typical forms of behaviour is that young people only share intimate recordings that constitute the violation of personal data or child pornography ***"amongst their pals"***. They are not aware of the risks, including the fact that it can be a criminal offence to forward certain content to a person, who then forwards it someone else.

It is a typical attitude for children to think ***they can handle these situations "on their own"***, as they assume that the adults don't know how to help and that they would simply report and ban the user in question as their way of solving the problem. They are also worried that their parents would prevent them from using a particular platform in the event of an incident. In many cases, the attitude of youngsters can pose a challenge, in that in certain situations it is worth asking an adult for help.

Many think these violations ***"would never happen to them"*** and that they wouldn't fall victim to online grooming, sextortion or online harassment. That is precisely why we present the questions related to the cases at hand as if the victim would be their best friend or younger sibling, as this scenario seems more realistic for them.

This former subject is also related to the phenomenon of **victim-blaming**, which is characterized by a *"they got what they deserved"* attitude. The initial reaction of most young people is to focus on what the victim did wrong and how they could have prevented the harmful situation from arising. The IH pays particular attitude to shape children's attitude to this issue. In cooperation with youngsters, we designed a poster based on a fictitious chat discussion, in which the victim-blaming attitude is replaced with positive, supportive messages

However, the shocking truth of the matter is that the things we rightfully consider to be extreme and severe happen so often to children that they consider them to be an *"everyday phenomenon"*. Practically all the young people we met had received unsolicited intimate images, had been approached for such images or know someone who has sent images of a sexual nature of themselves to others. As this happens frequently, it becomes an almost everyday phenomenon, which is why most of them shrug it off, even though this is not natural or acceptable and can even cause severe trauma.

The above-mentioned attitudes were present in all the school classes we visited. We continuously strive to tailor the subjects of our lectures according to these experiences and react to new suggestions and identified issues.

## United Nations High Commissioner for Refugees

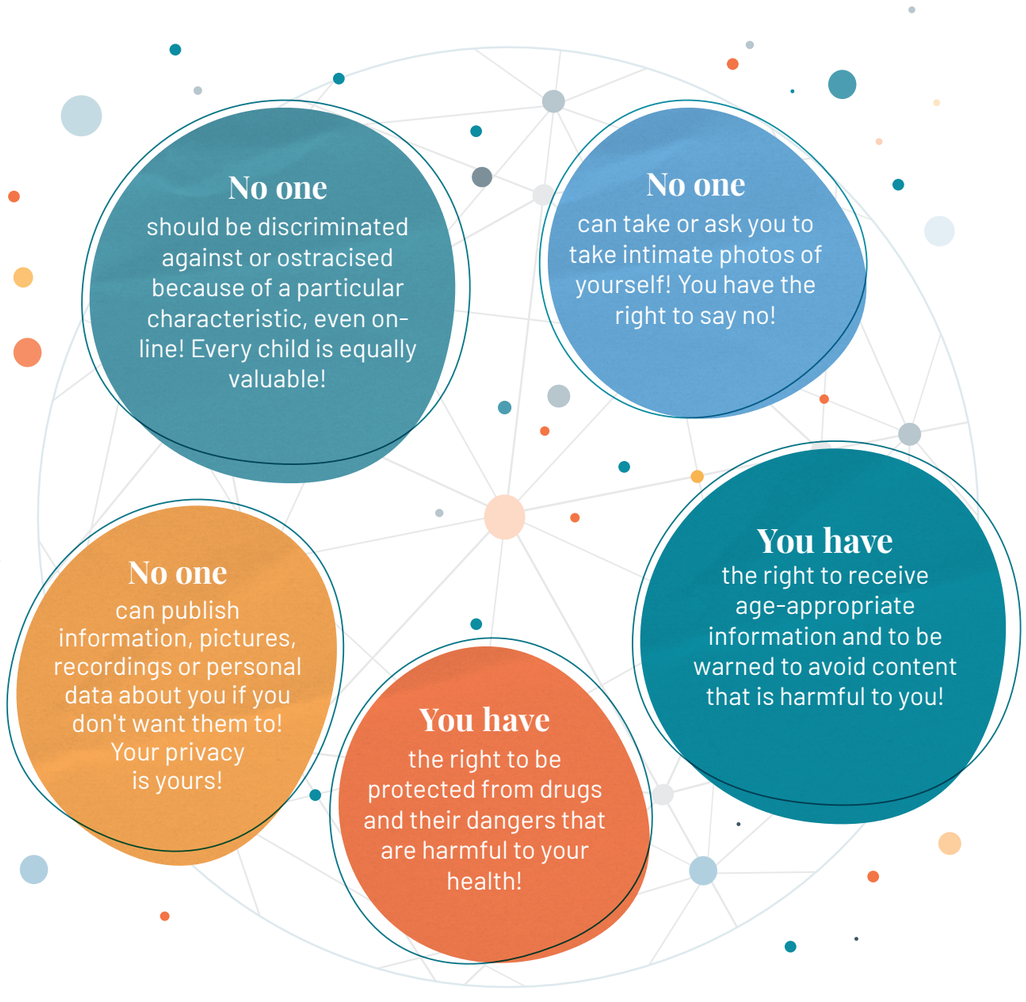
The United Nations High Commissioner for Refugees (UNHCR) issued **two publications, one for adults and one for young people**, to illustrate the online threats refugees are faced with, as well as the various related risks, challenges and protection strategies. The IH's staff helped to create these publications **as a professional supporter**, with their expertise in dealing with the management of reports. The materials in **Ukrainian and English** – which were published as part of the UNHCR's Budapest Office "Safe Online" campaign for refugee protection – were distributed in Hungary in more than 4,000 copies by 19 partner organizations.





## Child rights posters in schools

Amongst other things, the IH developed a series of awareness-raising school posters in cooperation with the Integrated Right Protection Service, which coordinates the work of all the child rights advocates in the country. The main goal of the posters was to remind children that their rights also apply online, and in the event of a violation they are entitled to protection and they have someone to turn to. The posters reached the students in nearly 4,500 public education institutions.



# Experiences, opinions



## The views of the Head of Department of the Internet Hotline on the importance of maintaining employee well-being

*"The day-to-day work of hotline analysts involves viewing content that may entail a psychological burden that lasts even beyond their working hours, which is why it is of particular importance for the NMHH to pay special attention to its employees' mental health. It can be extremely demanding for our analysts to deal with numerous extremely violent and shocking stories through the reports, therefore it is of crucial importance that they work in a supportive and safe work environment. Apart from the individual coping strategies of the analysts, it is particularly important that they all have access to organizationally supported services, such as group supervision sessions and individual psychological counselling. Scrutinizing the international best practices, we introduced a number of additional rules, particularly in relation to the analysis of child pornography and extremely violent content. For example, we decided that, on a single working day, they can work with child pornography material for no more than three hours and no more than eight hours a week. In relation to the analysis of violent content, we regulated that sound can only be played in exceptional cases only and listening to music is also contraindicated during the analysis. Additionally, single analysts cannot process violent content alone and are not allowed to work with extremely violent content within two hours of the end of their working day.*

## Experiences of a hotline analyst

*"We always handle reports of violations related to children as a priority, with a deadline of a single working day. Cases when we are contacted by the children themselves or their parents acting on their behalf are particularly sensitive and we often receive very desperate reports, asking for help. The reports often concern intimate recordings that the children were tricked into providing and they usually ask for our help when the child is being blackmailed with the images or videos that were published. We try providing immediate assistance for the victim in close cooperation with the colleagues of the National Bureau of Investigation, along with advice for the child's parent. These cases can be highly traumatic, but the reports sent by parents also come as some reassurance for the analysts, as they clearly show that the child is not alone with their problem and has a trusting relationship with their parents, which has allowed them to speak up at home and ask for help."*



### Lieutenant Colonel Gyula Péter

*Head of Department*
*Rapid Response and Special Police Services*
*National Bureau of Investigation*
*Cybercrime Department*
*Investigation Department*

*„The staff of the National Media and Infocommunications Authority Internet Hotline is an exceptional team that deals with the challenges of the online world with extraordinary directness, openness and determination. Their approach is solution-oriented and they always put the protection of the reporting persons and their correct information first. Despite the fact that we often think they know our answers in advance, they always approach us with respect and attention, whether they are dealing with fraud in the online space or any other professional issue. It is this kind of dedication and flexibility that makes them truly excellent partners for us."*

### pol. captain Judit FRIBÉK

*chief investigator*
*Rapid Response and Special Police Servicesí*
*National Bureau of Investigation*
*Cybercrime Department*
*Investigative Division*
*Child Protection Sub-division*

*„The close cooperation between the police and the NMHH Internet Hotline is vital in the fight against online sexual exploitation of children. The Internet Hotline can respond quickly and effectively to reports, while the police have the legal power to prosecute. Our cooperation will help to detect online abuse more quickly and bring perpetrators to justice sooner. It is important that the NMHH gives children and their parents the opportunity to report suspicious activities anonymously, helping to keep them safe online."*

### Dushica Naumovska

*Chief Operating Officer*
*INHOPE*

*„The combatting of online Child Sexual Abuse Material is a global problem requiring a global solution. As a long-standing member, the hotline, operated by the National Media and Infocommunications Authority of Hungary, has played a critical role in the swift removal of illegal content around the world. Their contribution to the INHOPE network is invaluable and we look forward to continuing our long term cooperation into the future."*

**Zoltán Nagy-Szakál**

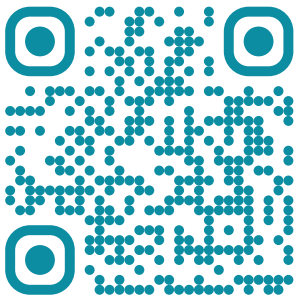
*Head of the Digital and Visual Culture Workgroup of the Merse Pál Szinyei High School of Budapest 6th District*

*„Protect your future today: be smart in the online world and keep your data safe" (ChatGPT)*

*"This was the motto of our Internet Safety Day, which was organized for the third time in 2024. This motto matched well with the contribution of the team of the NMHH Internet Hotline, which has participated in the Safety Day in the past two years. On both occasions, they gave 3-3 presentations on the Internet Hotline and its experiences. They shared the latest knowledge on internet scams and fraud, with a strong focus on how to avoid and prevent them. Our students were a bit sceptical about the lecture because of its serious title ("Dare to ask for help if you are a victim of online abuse! - The Internet Hotline experience"), but each time they left the lectures with new and useful knowledge. They were able to see more clearly how to protect themselves from online abuse, and to experience that there is help and someone to turn to. Thanks are due to the staff of the NMHH Internet Hotline Unit, who were always able to convey this knowledge in a professional way, but in a way that the children could understand, in the good-humoured, interactive presentations. We hope that this cooperation between our school and the NMHH will continue in the future."*

**Publisher:** National Media and Infocommuncations Authority, 1015 Budapest, Ostrom u. 23-25., Hungary
**Responsible publisher:** Dr. András Koltay, President of the NMHH

June 2024, Budapest



https://english.nmhh.hu/