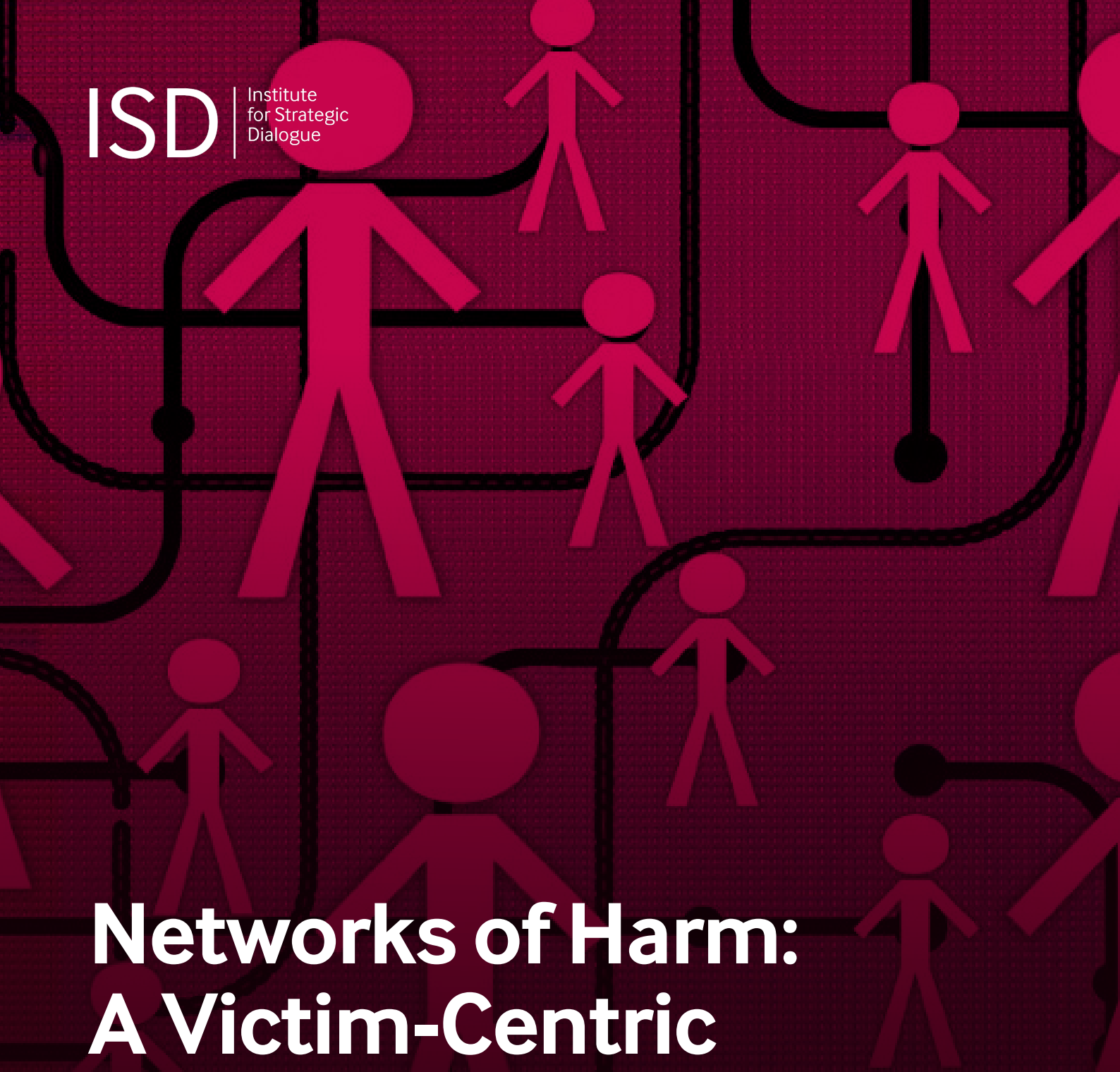


ISD | Institute for Strategic Dialogue

Networks of Harm: A Victim-Centric Information Resource on the 764 Sextortion Network

Content Warning: This resource contains graphic descriptions of self-harm, sexual content, abuse, cruelty to animals, and child exploitation. While efforts have been taken to minimise the inclusion of such material, examples and complete descriptions are necessary to provide those who may come into contact with 764 victims the tools to effectively recognise signs of abuse and offer support. If you suspect someone has been harmed by the 764 network, it is essential to approach them with sensitivity and awareness.

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org

Table of Contents

Executive summary 4

Introduction 6

Cross-platform dynamics of victimisation 8

Online pathways to harm 9

- Communities related to mental health disorders 9
- Online games 9
- E-girl subculture 10

Vulnerabilities in mental health communities 12

- Eating disorders (EDs) 12
- Self-harm communities 13
- Obsessive love communities 13

Tactics 15

- Account creation and target identification 15
- Exploitation 15
- Indicators 16

Key considerations 18

- Revictimisation 18
- Victim-perpetrator cycle 18
- CSAM considerations 19
- Vigilante actors 19

Resources 20

Executive summary

The 764 network is a loosely connected, transnational set of online groups that engage in sextortion and the glorification of violence. The network, comprising a constantly shifting landscape of splinter groups and offshoots, coerces minor victims into producing Child Sexual Abuse Material (CSAM). They then use that CSAM as leverage to force victims to perform acts of violence, animal abuse or self-harm. 764 members also engage in extensive swatting, harassment and intimidation campaigns to silence their victims. Since 2021, at least 50 members of 764 (or members of affiliated groups) have been arrested for sextortion, possession of CSAM or violent attacks. This report seeks to provide knowledge and resources to those who may encounter victims of 764 abuse, including parents, teachers, coaches, religious leaders, Prevent Delivery Officers and others.

This resource will provide concerned parties with an understanding of how 764 members identify and exploit their victims, provide information on vulnerable communities often targeted by the network, list indicators of abuse (as summarised in the graphic), and outline several considerations for readers who are in contact with victims.

First, any reader in contact with a victim should consider the following guidelines.

- Professional help is essential
- Know they may be trapped in a cycle of revictimisation
- Be aware victims may also be perpetrators of abuse
- Abuse often spreads across multiple platforms
- Victim's devices likely contain CSAM, which creates a host of legal considerations

While nearly any minor (and some adults) active on social media may be targeted by 764 members, ISD research has identified several communities where 764 members seek out victims due to their vulnerability. The most prominent of these are the online gaming communities, those associated with mental health disorders, and the "e-girl" community. However, their activities are not limited to these groups, and once identified, victims are often tricked or coerced into moving to other online platforms. It is crucial to understand that the

Indicators of abuse

- Sudden, uncharacteristic changes in behaviour, appearance, or routine
- Sudden changes in sleeping or eating habits
- Sudden abandonment of previous social circles and friend groups
- Receipt of anonymous gifts (physical or digital)
- Sudden shifts in appearance or habits surrounding clothing (i.e. wearing long sleeves in hot weather)
- Scarring on the thighs or forearms, especially if the scars form a pattern
- Unexplained injuries, including cuts, scratches, bruises, or burns
- Scars or carvings which appear to form a word or symbol (cutsigns)
- Family pets or other animals being harmed or dying under suspicious circumstances
- Pets or other animals being uncharacteristically avoidant or fearful of a child

victimisation process (including target selection, grooming and extortion) often unfolds across multiple social media platforms and can differ considerably for each individual victim.

A review of "sextortion guides" (detailed instructions on how to target young users) produced by 764 members, along with extensive research on 764 social media channels, has provided ISD researchers with significant insight into how these sextortionists identify and exploit their victims. While the process will be unique for each victim, 764 members generally follow a basic pattern: first seeking to obtain compromising material from their victim (most commonly nude photos) by charming or deceiving them, and then using this material to exploit the victim. Although this pattern is common among extortionists of all types, 764 members often seek to create 'long-term victims', engaging in extended and complex attempts to coerce them into progressively more extreme acts.

The resource concludes with a section on key considerations. Confronting instances of sextortion, particularly those perpetrated by the 764 network, requires additional considerations to both preventing the revictimisation of those affected, and avoiding the involvement of vigilante groups or individuals that portray themselves as 'anti-extortion'. Those seeking to help victims should be aware of the legal repercussions of possessing or producing CSAM, as well as the very real possibility that victims of 764 sextortion may have been pressured or forced to extort others.

Introduction

Predators have victimised children using the internet since its creation, but the increasingly online social lives of young people and the influence of extremist organisations have created a toxic cocktail, fuelling new forms of abuse from a subculture of nihilistic violence known as the 764 network. The 764 network is a loosely connected, transnational set of online groups that engage in sextortion and the glorification of violence. Since 2021, ISD has documented at least 50 arrests worldwide of individuals linked to 764-inspired networks for crimes involving sextortion, child sexual abuse material (CSAM) or plots to carry out acts of targeted mass violence. The network, often identified as part of 'The Com' (a set of online threat actors engaged in extortion and cybercrime) and is actually comprised of a shifting landscape of splinter groups and offshoots, causes harm in three main ways:

1. 764 members trick, blackmail, or otherwise encourage victims who are minors to produce CSAM and then use that content as leverage to force victims to perform acts of violence, animal abuse, self-harm, and/or create more CSAM.

2. Members of the network engage in swatting, harassment and intimidation campaigns to silence victims.

3. Members or prospective members engage in acts of violence such as assault, animal abuse, and attempted murder to impress other members of the network and gain social standing.

764 and related sextortion networks operate on a global scale, with an estimated involvement of hundreds—if not thousands—of individuals across the world who have served as victims and/or abusers. Through ethnographic monitoring, ISD has observed groups on Telegram containing up to 15,000 users at once. Security agencies in all Five Eyes country–Australia, Canada, New Zealand, the United States and the United Kingdom–have warned about the dangers posed by subcultures of nihilistic violence adjacent to 764. As examples of the network's global reach, individuals inspired by or involved with 764 have plotted to murder a homeless person in the UK, carried out stabbing sprees in Sweden, planned an attack on a mall in in Washington, and stabbed a homeless woman in Minnesota.

Past research from ISD has focused on the structure of the network, its history and early Satanist and neo-Nazi influences, and the intersection of sextortion activities with glorification of mass violence.

This Resource addresses the challenge posed by the 764 network from a victim-centric perspective, aiming to inform parents, educators, coaches and potential victims about the network's practices and the warning signs that could enable early intervention and prevent further victimisation.

Drawing on ISD's observation of 764 social media channels and original documents such as 764 sextortion guides (which detail the methods used by network members to sextort minors. The Resource outlines physical indicators of abuse that might be visible to friends or adults in their lives, explores the intersection of mental health conditions and vulnerability to 764 abuse, identifies the online spaces where members seek victims, and highlights other factors that should be considered by victims and those supporting them.

If you suspect someone has been harmed by the 764 network, it is essential to approach them with sensitivity and awareness, while keeping the following considerations in mind:

Professional help is essential

Connect victims with mental health professionals trained in trauma care and with experience handling CSAM. Avoid self-styled vigilante groups, which may retraumatise victims, interfere with investigations or unintentionally cause further harm.

Know they may be trapped in a cycle of revictimisation

Even if abuse appears to have ended, victims may still be targeted or blackmailed with old material. Victimisation does not necessarily end with disconnection.

Be aware victims may also be perpetrators of abuse

Some victims are coerced into recruiting or abusing others. This does not erase their victimhood. Victims may possess CSAM (including self-produced CSAM) or have complied with illegal requests. Let them know support and safety come first, and that disclosing abuse will not automatically criminalise them.

Abuse often spreads across multiple platforms

764 members are active across nearly all social media apps, but the most prominent include Telegram, Discord, Roblox, X, Instagram, TikTok and Reddit. The abuse often takes place across multiple platforms. As hypothetical examples, victims may be initially contacted on Roblox, X (formerly Twitter) or Reddit then moved to other less-known platforms such as Telegram or Discord. However, this list of platforms is not exhaustive, and 764 activity has also been reported on Minecraft, Fortnite, Twitch, Steam, and Snapchat, among others. Victims (or perpetrators) may attempt to disclose conversations or interactions on a single app while concealing activity on another.

If you encounter CSAM

If you are supporting someone impacted by the 764 network, there is a high likelihood that CSAM (including self-produced CSAM) may be involved–either in their possession, on their devices or shared without their consent. It is critical to respond appropriately and legally:

Do not download, save or forward the content. Power down the device, disable any cloud syncing if possible, and–if you are able and comfortable doing so–report the situation to law enforcement immediately.

Cross-platform dynamics of victimisation

Victimisation by the 764 network often occurs across multiple online platforms, with members exploiting the unique features of each to identify, groom and extort victims. Understanding how different platforms are used is crucial for recognising abuse pathways and taking steps to prevent further harm.

Victimisation processes (including target selection, grooming and extortion) often unfold across multiple social media platforms and can differ considerably for each individual victim. For example, a 764 member may initiate contact with a victim on X, move the conversation to Telegram where grooming and extortion begin in earnest, and then broadcast images of the abuse on Telegram or Discord. In other cases, a victim may be initially contacted on Discord, moved to Roblox to simulate sexual activity, then to Telegram for further grooming and back to Discord.

Discord stands out due to its perceived versatility, with 764 members viewing it as suitable for multiple purposes: identifying potential victims, grooming them and ultimately broadcasting their abuse. For some individuals, the victimisation pathway may begin for example with a 764 member initiating contact with them on a gaming-related Discord server and end with acts of self-harm being broadcasted on a private Discord server. This multi-purpose use is unusual compared with other platforms, which 764 members generally employ for more specific tasks, such as victim identification.

Telegram remains the most important platform for coordinating activity and sharing sexploitation material to boost members' notoriety. In Telegram group chats, 764 members will frequently share conversations they are having with victims to gain clout or demonstrate active engagement in producing harmful content. Private Telegram chats are also used to circulate the usernames and identities of potential victims to coordinate exploitation.

ISD's research has identified 764 members using nearly every mainstream social media platform available. However, the most common include Telegram, Discord, Roblox, X, Instagram, TikTok, and Reddit. Based on ethnographic analysis, while less prominent, Minecraft, Fortnite, YouTube, Twitch, Snapchat, and a variety of more obscure platforms and online games are also used by the network. This list is not exhaustive, and 764 and related networks are constantly developing new ways to identify and exploit victims. Some platforms have implemented safety features intended to protect young users, but in most cases they have proven insufficient to prevent victimisation and cannot be relied upon by parents as the sole measure to prevent their children from these networks.

Online pathways to harm

ISD analysts have observed 764 members using a variety of social media platforms and online communities to both identify and target vulnerable youth. This section will outline the three most commonly exploited: those related to mental health disorders, online games and the e-girl subculture.

Communities related to mental health disorders

Online communities related to mental health disorders are a primary target for 764 members, as they often include vulnerable individuals who may already engage in self-harm or other risky behaviours. While many users participate in these spaces to manage a disorder or disorders, they can sometimes continue to engage in harmful behaviour, as well as seek validation from other social media users. Because 764 members prize graphic images of self-harm as proof of their exploits, they often target communities specifically focused on self-harm, eating disorders, suicide ideation and bipolar disorder, as also outlined in 764 manuals.

764 members identify victims through manual searches on platforms like X, Reddit and Discord, using keywords associated with these disorders. ISD analysts have observed 764 members collating lists of users on X whose biographies feature hashtags or other descriptors that identify them as suffering from mental disorders. One 764 leader bragged about their success rate on X, stating that the platform hosted hundreds of users who explicitly identified as engaging in self-harm, and claiming they found half their victims there.

Reddit is another prominent hub for semi-organised discussions related to mental health disorders. In one highly active subreddit centred around a specific disorder—which ISD is choosing not to name to avoid further attention— users were observed complaining about predators who attempted to manipulate them into producing self-harm content. One user even remarked that they were approached by someone who requested that they carve their name into their skin so that the abuser could use it as a profile picture. These attempts highlight the often crude and unsophisticated nature of 764's extortion efforts. Members of the network often try to contact as many potential victims as possible across several social media platforms. Instead of using sophisticated social engineering tactics, these actors attempt to cast a wide net in the hope that they can attract especially vulnerable individuals.

Figure 1. Screen capture from a TikTok video which garnered over 3,800 likes and 850 comments. Such engagement levels highlight the wide reach of material created by people seeking abusive online relationships.

While not nearly as common as unwitting victims of 764, ISD has observed numerous users who appear to be actively seeking exploitative relationships online, including with individuals involved in sextortion networks, and who participate in digital communities centred around this phenomenon. These users sometimes identify as suffering from mental health disorders and belong to communities that self-identify with "obsessive love" or abusive relationships.

Online games

Online gaming platforms popular among youth—including Roblox, Minecraft and Fortnite—are viewed by 764 members as some of the most productive hunting grounds for potential victims. In rarer cases, online roleplaying games known as Gacha games—which are popular in Asia but obscure elsewhere in the world—have also been used by sextortion networks. Certain users of these platforms may be targeted due to their perceived mental health vulnerabilities, especially if they publicise having these disorders on their profiles. However, the main draw for 764 to these platforms is their young user base. Children are seen as prime targets due to their inexperience recognising manipulative behaviour, and their lack of operational security, which

can expose them to doxing and extortion. Moreover, within 764, victimising young children functions as a perverse means of obtaining status, with younger victims generating more clout for the abuser.

This dynamic is particularly acute in Roblox virtual environments–termed 'games'–intended as venues for simulating sexual experiences. In 764-related group chats, users were observed discussing their plans to find victims in one of these games by engaging in 'ageplay'–a type of sexual roleplay that often occurs between a child persona and an adult persona. However, Roblox games do not necessarily have to feature sexual elements to attract 764 attention. They often target popular games geared towards socialisation, where players simply "hang out" and chat with each other in a customisable virtual environment.

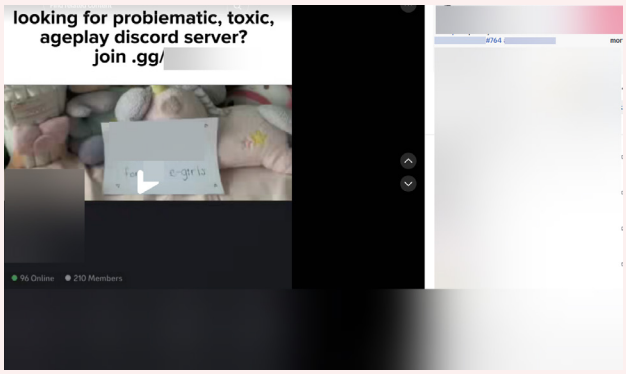
An aspect of Roblox exploited by 764 members is its virtual currency, Robux, which allows players to purchase upgrades such as in-game items and services. Members may offer Robux to gain users' trust or bribe them into committing acts of harm. In one 764 group chat, a member discussed having a monthly Robux budget dedicated to exploiting victims. While it is not always clear how 764 members acquire Robux in the first place, their collaboration with cybercriminals in the broader Com network may facilitate financial exploitation schemes on Roblox. The platform's financial components also enable other avenues of exploitation, such as hacking: one 764 member bragged that after hacking a 12-year-old's Roblox account and gaining access to sensitive payment information, they attempted to extort the victim into molesting his sister.

While less prominent than in Roblox, Minecraft and Fortnite are also cited by 764 members as useful platforms for finding victims. One 764 member alluded to the ease of exploiting victims on Minecraft, noting they could persuade minors to engage in self-harm without offering payment. Another member posted an image from Fortnite showing various user profiles containing information related to their age, sexual orientation and other details that can be exploited for targeting purposes. This suggests that some 764 members may be manually searching for and collating lists of users on Fortnite in the same way they do on X, where they canvass profiles containing certain hashtags and circulate them in group chats as a shared resource of potential victims.

Figure 2. On Roblox, a suspected 764 member attempts to initiate a sexual encounter with other users.

Figure 3. This image, which was circulated on TikTok, alludes to the use of virtual rewards (referred to by Roblox users as 'limiteds') by sextortion networks as a means of persuading victims to engage in self-harm.

Figure 4. A video posted on TikTok advertised a Discord server where 764-related networks can find e-girls and engage in sexual "ageplay".



E-girl subculture

'E-girls'–young girls or women who have a distinct fashion aesthetic–have been frequent targets for exploitation and violence by members of 764. The term e-girl was initially used as a pejorative label to describe young women and girls who seek to cultivate a large online following, often through posts highlighting their physical features. By the late 2010s, the term evolved to describe a subculture that is viewed in a more neutral light, celebrating the individuality and creativity of e-girls while recognising their embrace of the internet and creation of online personas as a means of self-expression. E-girls are especially prominent on TikTok, Instagram, Twitch and YouTube, and are characterised by a cutesy and hyperfeminine aesthetic that blends fashion elements from emo, alternative, punk, anime and gaming subcultures. While some self-described e-girls engage in flirtatious and playful behaviour, it is essential to recognise that they are not inviting exploitation. Nevertheless, extreme misogynists and other harmful actors often target e-girls, threatening and harassing them, which can have severe offline consequences. In 2019, the term entered the public consciousness when a man murdered a 17-year-old described as an e-girl and posted images of her corpse on Discord. In recent years, 764 members have continued the disturbing pattern of harm against those associated with this subculture.

An early guide produced by a 764-adjacent network counselled readers to go on "any social media platform", find "ANY alt-girl" that appeared "weak or vulnerable", and extort them. E-girls remain a regular target of exploitation due to perceived vulnerability. ISD researchers identified an "e-girl directory" circulating on major platforms like Instagram and among extortion networks. This "directory" included usernames and photographs of girls on Roblox who were allegedly "easy to manipulate" into providing indecent images.

On TikTok, analysts identified numerous 764 member accounts following many e-girls, reflecting their interest in finding participants in this subculture. On X, 764 members have been observed initiating contact with e-girls, presumably with the intent to groom and extort them. A number of servers were also identified on Discord which explicitly marketed themselves as having e-girl members who were interested in engaging in ageplay on Roblox, but which otherwise had no explicit connection to 764; one of them had more than 1,100 members. Some Discord servers centred around e-girls were advertised on TikTok to draw the attention of sextortion networks, highlighting the cross-platform dynamics of victimisation in the context of 764.

Vulnerabilities in mental health communities

Mental health issues are often portrayed through a variety of behaviours that can increase a person's vulnerability to predatory advances both on- and offline. To understand why 764 targets specific online mental health communities requires more in-depth exploration of both the mental health issue itself and associated behaviours. ISD analysts identified three communities regularly targeted by 764: eating disorders (EDs), self-harm and obsessive love disorder. In some situations, these online communities can centre around recovery and shared experiences, but they often serve to maintain and/or encourage harmful behaviours.

This section primarily examines subcommunities that focus on maintenance and encouragement. These spaces have a high prevalence among teenage girls and their participants may have vulnerabilities that 764 members can weaponise to coerce them into severely harmful acts. To avoid exacerbating any existing mental health issues of individuals who participate in these communities or providing new ideas for harmful behaviours, ISD will not specify acts of self-harm or disordered eating observed within communities.

Eating disorders (EDs)

Of several different EDs classified in the Diagnostic and Statistical Manual (DSM), ISD analysts identified anorexia nervosa, bulimia nervosa and binge eating disorder as the conditions most commonly targeted by 764 members. Online ED communities predominantly consist of female users, and although not all users have a formal diagnosis, publicly sharing ED behaviours still increases their vulnerability to 764.

- Anorexia nervosa or 'anorexia' is the restriction of necessary food intake leading to a significant impact on physical health. Individuals may exhibit signs of social withdrawal, a strong desire to control one's environment and restrained emotional expression. A key feature of anorexia is an individual's fixation on their weight, resulting in their self-esteem being "highly dependent on their perceptions of body shape and weight."

- Bulimia nervosa or 'bulimia' is characterised by recurring episodes of binge eating followed by harmful compensatory behaviours to prevent weight gain, and self-evaluation that is significantly associated with weight or shape. These inappropriate compensatory behaviours can result in a multitude of medical health issues and social isolation.

- Binge eating disorder (BED) describes the presence of repeated episodes of binge eating with a sense of lack of control but without any compensatory behaviours. Binging can result in various medical issues, social withdrawal and feelings of shame, disgust, or embarrassment following a binging episode.

Online communities can be an important outlet for individuals suffering from eating disorders. However, some of these communities encourage disordered eating and exacerbate the vulnerability of participants. A key feature of anorexia and bulimia is the strong association between self-worth and appearance: those suffering from the disorders may participate in ED communities that encourage harmful body perceptions. Users often post their own photos and request negative feedback from others. These communities frequently feature complimentary photos of unhealthily thin women who are described as having the 'ideal' shape.

764 sextortion guides instruct members to initiate contact with young women suffering from EDs by complimenting their physical features, reinforcing the association between beauty and body shape. 764 guides direct members to create a direct association between themselves and their victim's self-esteem through continued compliments and criticisms. This means that if a victim refuses a request, the 764 member will insult their appearance and self-worth to reinforce this association. This could make it harder for victims to detach their self-worth from their online abusers, in turn making it more difficult to deny harmful requests as it could impact this new perception of self-esteem.

Alongside decreased self-esteem, the DSM outlines significant social isolation as a possible consequence of eating disorders. This increases the likelihood that individuals will search for social connection online, making them more active within online spaces and thus more accessible to 764 members. 764 guides also promote tactics to isolate victims, encouraging them to reduce interactions with friends and family should they seek help from others.

Eating disorders have some of the highest mortality rates across psychological disorders. This is likely why

764 targets those that suffer from eating disorders: perpetrators gain notoriety by coercing their victims into committing severe self-harm and in some cases encourage their victims to commit suicide on video.

Anorexia in particular carries one of the highest mortality rates amongst EDs, with a significant proportion of deaths caused by suicide. Studies have shown up to 33 percent of individuals have suicide ideation. This elevated risk is partially because individuals with anorexia are more likely to engage in more severe and lethal self-injury with the intention of death, making them particularly vulnerable to the escalating demands of 764 members who encourage severe acts of self-harm.

While anorexia has a higher percentage of completed suicides, both bulimia and BED possess a significant risk of death. This is in part due to the significant percentage of suicide ideation present in both, as well as the suicide attempts by those suffering from bulimia and medical morbidity in BED. 764 members exploit these vulnerabilities to manipulate victims into engaging in severe self-harm, sexual acts and suicide.

Self-harm communities

Self-harm encompasses a swath of methods used to inflict physical, psychological or emotional harm to oneself for the purpose of injury or suicide. Self-harm is not a standalone disorder but a symptom of other mental health issues. The self-harm communities targeted by 764 often focus on what clinicians call non-suicidal self-injury (NSSI). NSSI and suicidal self-harm behaviours overlap strongly but are distinguished by the intention behind the action: NSSI is "undertaken to feel better or cope" with emotions and does not indicate a desire to die, whereas suicidal self-injury is undertaken with the explicit intention of death.

764 members often target individuals in the self-harm community with past experiences of NSSI. By taking advantage of users who may already routinely engage in self-harm, 764 members believe they can manipulate their victims to produce NSSI content to share within the network. 764 guides instruct members to establish habits of self-harm in victims by requesting daily images evidencing the action. This often causes victims to incorporate acts of non-lethal self-injury into their everyday routine. Analysts also observed numerous users in online communities engaging in NSSI "competing to exhibit the most injuries", suggesting these users are more desensitised to sharing images of their injuries.

Alongside the physical injury, NSSI can "lead to feelings of shame, guilt or regret". Those who practice NSSI often avoid family and friends to prevent them from seeing their injuries. 764 members use these fears to socially isolate their victims further and coerce them into committing more severe injuries by threatening exposure and humiliation.

In addition, NSSI behaviours are often used to feel a sense of control with individuals determining the method, duration and severity of the injury. 764 members destabilise this perception by dictating each of these steps. Women often perceive NSSI as a controlled strategy to alleviate emotional distress. 764 members exploit this distress by conditioning victims to associate their anxiety with the 764 members' gratification. Over time, 764 members attempt to instil the belief that the only way their victim can alleviate their anxiety is by appeasing them through acts of self-harm. This reframes the victim's perception of control. While the physical act of self- harm still lies with the victim, the psychological perception of maintaining control shifts to the 764 member. This makes it more difficult for victims to feel capable of regaining control and detaching from the online abuser.

Obsessive love communities

764 members also seek out participants in 'obsessive love' communities where abusive behaviours and power imbalances are normalised. In the most extreme forms of obsessive love, participants believe that violence is a determining factor of a partner's love.

- Obsessive love disorder is a condition characterised "by an overwhelming and uncontrollable fixation on another person." It is not classified as a clinical disorder and is often an indication of other mental health issues including attachment disorders, obsessive compulsive disorder, delusional disorder and borderline personality disorder.

A key feature of obsessive love is the belief that "your romantic partner is essential to your own stability and happiness." 764 guides encourage members to cultivate this belief in their victims, meaning users who have already adopted this association are more desirable targets. Those who participate in obsessive love communities often hyper-fixate on a single individual, which can result in social isolation and increased emotional distress.

764 members attempt to create a superficial support system, built on insincere sympathy, in which victims believe that comfort is exclusively provided by their abuser. By providing constant reassurance after a victim has completed a requested action, 764 members

reinforce the victim's fear of abandonment, making it harder for them to disengage. This form of anxiety is a significant predictor of engaging in NSSI in women, further increasing their vulnerability to requests of self-harm.

Other features of obsessive love (such as frequent monitoring of a partner and the desire to control them) correspond closely with 764 extortion tactics. Online users with obsessive love disorder romanticise these behaviours, some picturing themselves as the obsessed party while others see themselves as the target of obsession.

Both roles present vulnerabilities to 764 methods. Those who desire to be obsessed over may be more susceptible to controlling tactics, believing they must accept their partners wishes, no matter how severe, to maintain the relationship and obsession. Conversely, users who wish to obsess over someone else may interpret acts of violence at the direction of a 764 member as expressions of love, signalling a willingness to sacrifice their own well-being for their 'partner'. In both cases, victims may be less likely to deny harmful demands.

There is an important distinction between individuals who romanticise obsessive love in fictional settings and those who practice or seek it out in their real life. Many users who portray themselves as the object of desire in fictional obsessive love dynamics may do so with positive intentions: to regain a sense of control of their own violent experiences, push creative boundaries or feel less isolated. These users are more likely to be focused on recovery and retaining control over the fictional dynamic. In contrast, those who pursue obsessive dynamics in real life are more likely to encourage harmful behaviours and struggle to maintain control. The romanticisation of these dynamics in real-life contexts can partly be found in mainstream media with mass consumption leading to the normalisation of abusive relationships. 764 members exploit this normalisation by mirroring fictional manipulation tactics–framing boundaries as hurtful and reinforcing the belief that women are responsible for their partner's emotional stability. To avoid causing perceived harm, victims may override their own discomfort and comply with harmful requests.

Figure 5. This image, which was posted on X, was circulated by a user who identified as suffering from obsessive love disorder. The post was viewed nearly 7,000 times.

Tactics

While sextortion and extortion are used by a wide variety of actors, members of the 764 network generally follow a distinct set of tactics—many of which are shared through guidebooks distributed within the network.

Drawing on these guidebooks, as well as court records and other sources, this section provides an explanation of how members of the 764 network target, recruit, extort and control their victims.

This section also highlights the most readily observable indicators of a child's abuse by/involvement in the 764 network. Knowledge of these indicators allows those who interact with vulnerable minors the most (including parents, educators and mental healthcare practitioners) to proactively identify and report instances of abuse perpetrated by the 764 network.

Account creation and target identification

764 members provide incredibly detailed instructions on how to exploit victims and often tailor these approaches to specific types of targets. According to a sextortion guide authored by a 764 member, members of the network are encouraged to tailor their approaches to the specific platform they are using and their desired victim profile.

The guide first instructs prospective members to create tailored accounts which they will use to contact intended victims. As a result of this 'bespoke' approach, there is no one model for what a "764 account" looks like. On platforms where accounts are recommended to users (including Snapchat or Instagram), members of 764 are encouraged to match the age and gender of their account to demographics of their preferred target. This allows members to receive recommendations of possible target accounts.

On platforms without this feature (such as Tumblr and X), members primarily seek out victims through tagging systems. Insular communities and subcultures active on these platforms find like-minded individuals using tags which categorise posts by topic (such as #sh, #ed or #tcc). These tagging systems allow extortionists to easily locate targets in vulnerable communities such as self-harm/ED communities. These methods demonstrate that 764 members are often acutely aware of platform-specific limitations outlined in platforms' Terms of Service (TOS). For example, one guide recommends only messaging three individuals per Instagram account, as additional messages are flagged as spam by the platform.

764 also encourages members to "catfish" victims by portraying themselves as being especially attractive. The guide encourages prospective members to use the likenesses of famous TikTok personalities.

Another important piece of what the guide considers to be a "successful" attempt at extortion is using scale to increase the likelihood of success. Many methods utilised by the 764 network do not have a particularly high success rate, instead relying on casting as wide a net as possible to find victims. It explains that receiving explicit content from 10-15 targets out of 200 total is considered successful within the network.

Exploitation

764 members rely on a variety of methods to obtain sexually explicit content from victims. These extortionists generally first seek out victims on either Snapchat or Instagram (although the author of one sextortion guide notes that recent changes in Instagram's policies have made it a less advantageous platform for this purpose) by either sending mass messages requesting explicit content or slowly gaining the trust of potential targets before making a similar request. The first method relies on sheer scale, with the abovementioned guide predicting a success rate of between 2.5 and 5 percent based on 200 messages to potential targets. The second method, which requires a more targeted patient approach, is rarer but still observed.

Once a perpetrator has received explicit content from the victim, they simultaneously gather as much personal information as possible and work to gain the victim's trust. 764 members consider this initial phase of extortion both the most critical and the most vulnerable stage of the abuse cycle. Potential extortionists are encouraged to carefully plan the transition from posing as an online friend to making their extortionary demands.

A major concern is that during this transition, the victim is most likely to report the abuse. To combat this, 764 members are instructed to isolate targets from friends, relatives and other trusted figures before beginning their extortion. 764 guides also recommend that extortionists familiarise themselves with a target's schedule and

pattern of life to ensure that they are alone when the extortion begins. The guide also emphasises the importance of scale, stating "only 1 out of 50 [targets]… will be a long-term sextortion victim".

The first demand is often less extreme than future requests. Experienced extortioners seek to establish "long-term victims" that will continue to produce abuse material. In order to establish control, extortioners will request relatively benign material at first, prioritising their victim's compliance over receiving abuse material that will provide them clout in their network. These requests could include pictures of the victim in a state of partial undress holding a piece of paper with their full name, or other demands that, while still extortionary, are less likely to cause the victim to report the abuse. These demands are intended to establish an extortionary relationship and often, as with the abovementioned picture, create additional material that could be used as blackmail in the future.

After the initial extortionary relationship has been established, the perpetrator's next task is to further entrench their power over the victim. The sextortion guide recommends that extortionists accomplish this through constantly occupying a victim with tasks. Extortionists are instructed to gradually increase the severity of their requests, starting with basic and inoffensive requests, to "contribute[s] to the victim's developing a pattern of obedience," as stated in a guide. The guide notes that sudden jumps in the severity of requests may cause a victim to be "taken aback and… more resistant to the demand".

764 sextortion guides recommend maintaining a constant presence in the life of a victim and "creating false hope" to maintain control and prevent reports to law enforcement. Perpetrators are instructed to offer sympathy or benefits—termed "olive branches"—to victims throughout the extortion process, to convince victims that they are also getting something out of their extortionist and that they can eventually use this information against them. Another goal of this practice is to weaponise victims' desire to contact law enforcement into a means of extending their sextortion: perpetrators may slowly reveal personal information about themselves to victims to make them believe that they will eventually have enough information to report the extortionist to law enforcement. In some situations, extortionists will explicitly tell a victim that more personal information will be revealed after a set period or upon completion of a specified task. This process of moving the goalposts is an important piece of maintaining the relationship between the extortionist and extorted.

Indicators

Research on childhood trauma consistently highlights sudden emotional, behavioural and social changes as potential indicators of exploitation. Trauma in children and young adults often manifests through withdrawal, irritability and mood swings, alongside other disrupted routines such as changes in eating and sleeping patterns. These shifts may reflect heightened anxiety, attempts to manage new external pressures and evolving coercive and controlling relationships.

In online grooming contexts, this frequently coincides with distancing from longstanding peer groups and the prioritisation of new 'online friends'. Material 'grooming markers', such as unexplained gifts or monetary tokens may serve as tangible signs of coercive control and manipulation. In digital environments and platforms such as Roblox, these markers can include virtual currencies which may be deployed by 764 groups as both inducements and leverage over their victims.

764 exploitation often leaves victims with visible indicators of abuse. These include sudden, uncharacteristic changes in a child's behaviour, appearance or routine, for example:

- A victim inexplicably becoming withdrawn, moody or irritable.
- They may change eating or sleeping habits. This can sometimes be framed as accommodating new "online friends", with previous social circles and friend groups suddenly abandoned for these new digital acquaintances.
- Another possible indicator is the receipt of anonymous gifts which can be physical or digital (including gaming currency such as Roblox).

Sudden shifts in appearance/clothing can also indicate possible involvement in 764. Children may begin wearing long sleeves or pants in hot weather to disguise the effects of self-harm. However, this indicator is not as reliable for individuals who have been known to engage in self-harm in the past who may already dress in this manner.

The acts of violence and self-harm that victims of the 764 network are coerced into provide the clearest physical indicators of their involvement or victimisation. These indicators include:

- Scarring on the thighs or forearms of a child, especially if the scars form a pattern,

- Fresh injuries including cuts, scratches, bruises, burns, or other wounds.

It is important to remember that often the self-harm perpetrated within 764 spaces is more extreme than other forms of 'cutting', and that indicators of 764-linked self-harm are more complex and varied than scarred forearms. If scars or carvings from a child's self-harm appears to form either a word or symbol, it is possible that they were directed to do this to create a "cutsign"–or a distinctive word, name or symbol–as a sign of ownership for their abuser.

Victims are also often extorted into committing animal abuse. This can be identified by family pets or other animals being harmed or dying under suspicious circumstances, or animals being uncharacteristically avoidant or fearful of a child.

Finally, the 764 network uses swatting to intimidate and control victims; this involves law enforcement being called to the home under false pretences and can have potentially lethal consequences. A case of swatting can possibly indicate a child's involvement in the network and warrants further inquiry.

Key considerations

Confronting instances of sextortion, particularly the variety practiced by the 764 network, requires additional considerations to both prevent the revictimisation of those affected, and to avoid the involvement of vigilante groups or individuals that portray themselves as "anti-extortion". Those seeking to help victims should be aware of the legal repercussions of possessing or producing CSAM and confront the very real possibility that victims of 764 sextortion may have been pressured or forced to extort others.

Revictimisation

In some cases, victims' personal details are disseminated across perpetrator networks, exposing them to further abuse. Perpetrators may compile content (including sexual images, personal data and evidence of self-harm) into publicly accessible folders known as 'lore books'. This information may also be shared on doxing sites such as DoxBin.

Victims are often targeted by multiple perpetrators and abuse can resume even after periods of apparent inactivity. The persistent availability of previously shared materials allows for cyclical victimisation, particularly among those who have not yet engaged with law enforcement.

Further harm can also come from well-intentioned actors. Journalists, researchers and content creators may inadvertently retraumatise survivors by sharing their stories, images or abuse materials without consent. This issue deserves careful public attention but must be approached responsibly. ISD recommends that those working in this space adhere to trauma-informed guidelines, such as those provided by the Western University as well as the former Dart Center for Journalism and Trauma.

Lastly, these networks thrive on visibility and sensationalism, so naming specific groups or perpetrators may inadvertently help them reach new victims. Keeping the "Oxygen of Amplification" principle in mind is essential for responsible research and reporting.

Victim-perpetrator cycle

Those victimised by the 764 network often become perpetrators of sextortion themselves. This can occur because they are forced to do so or because these behaviours have been normalised in their minds by their victimisers. At best, this victim-perpetrator cycle muddies the waters and can lead to confusion. At worst, failing to understand this cycle could lead to revictimisation and the inability to identify the original extortionists.

This consideration is particularly important given that when a victim is first encountered or identified (whether by parents, bystanders or law enforcement), it is possible that they will be in the role of the perpetrator. It is important to consider their potential status as a victim, particularly when dealing with minors or those that are otherwise vulnerable. This does not legally invalidate the crimes they may have committed nor lessen the damage they may have inflicted on their victims, but it should inform the approach taken.

If a parent, coach, educator or even law enforcement suspects that someone (especially a minor) is involved with the 764 network, regardless of their role, it is important to approach the conversation with an understanding of the victim–perpetrator cycle. While law enforcement officers may be obligated to act on information about criminal activity and many jurisdictions designate professions such as teachers and therapists as mandatory reporters—a person who is required to report certain types of suspected abuse or neglect to authorities—victims should be encouraged to share all aspects of their interactions with the network whenever possible. They should be assured that their original status as victims is not compromised even if they were coerced to participate in further sextortion.

Similarly, those interviewing or otherwise engaging with suspected perpetrators of 764 sextortion should remain aware of this cycle, especially if operating with limited information. It is possible that a suspected perpetrator is themselves a victim.

Wherever possible, best practices such as trauma-informed victim interviewing should be leveraged even if the interviewer believes the individual to be a

perpetrator rather than a victim.[1] Open-ended questions and reassuring, nonjudgmental language can help interviewees share their experiences in their own words. This approach is more likely to elicit honest disclosures–including possible admissions of criminal or anti-social behaviour.

CSAM Considerations

Note: The content in this section should not be considered legal advice in the US or any other jurisdiction. The information may not reflect the latest case law or legislation and is written only for readers' awareness.

In the US, as in most jurisdictions, the possession or distribution of child pornography is a criminal offence. Virtually every situation involving CSAM uploaded to or transmitted via the internet is a federal offence. As the law is written, there is no carveout or exception made if the CSAM is produced by the minor depicted in it. Historically, the creation and first-person distribution of self-produced child pornography (SPCP) has not been charged at the state or federal level. However, despite efforts to address the question, it remains a legal grey area.

If an individual is involved with the 764 network, whether as a perpetrator or a victim, there is a near certainty that they have engaged in or been exposed to the creation and/or distribution of child pornography. It is very likely that they have CSAM stored on their electronic devices (whether intentionally or unintentionally). Care must be taken to ensure that this material is treated appropriately. Researchers recommend that the following steps be taken:

- Do not attempt to preserve or save the CSAM by transferring it to another device or taking screenshots.
- The devices in question should be disconnected from the internet and switched off. Where possible, remove the battery and/or use a Faraday bag to prevent the device from connecting to any networks.
- When possible, automatic syncing or downloading to platforms such as Google Drive or iCloud should be disabled to prevent the spread of CSAM to other devices or servers.
- Contact law enforcement or a known mandatory reporter.

Vigilante actors

In recent years, there has been a surge in self-styled vigilantes targeting alleged online child predators and documenting their actions. These include viral videos where individuals lure suspected offenders to in-person encounters, sometimes resulting in harassment or assault. In other cases, vigilantes engage in digital campaigns which identify and expose individuals linked to sextortion networks, including those associated with the 764 ecosystem.

Across multiple platforms, individuals and groups are engaged in tracking alleged perpetrators. Some operate quietly but others create videos and content out of their exploits that they then share with their audience. While often framed as a form of grassroots justice, these efforts frequently backfire.

Vigilante actions can interfere with active investigations and push offenders further underground. This can make it more difficult for law enforcement to locate and prosecute them. In some cases, members of these anti-extortion groups attempt to reverse-extort their targets, forcing them to perform degrading acts on camera as a form of retribution. These vigilantes can also become targets themselves, ultimately joining the ranks of victims they sought to defend.

Worryingly, some groups share images of victims as evidence of harm caused by perpetrators. These materials may include graphic self-harm photos or even blurred sexual abuse content, raising serious legal concerns. Possession or distribution of such content may constitute criminal activity, regardless of intent. It also raises ethical concerns: when shared without consent, this content can retraumatise and revictimise those already harmed.

While the impulse to support and engage with these actors is understandable–particularly given the slow pace of legal systems–their actions often cause more harm than good.

1 It should be noted that the recommendations in this section seek to elicit information necessary to gain a holistic understanding of a victim's participation in the network and are primarily intended for non-law enforcement audiences. The authors recognise that these techniques have the potential to allow perpetrators (including non-victim perpetrators) to obscure their culpability and participation in illegal activity and may not be appropriate for law enforcement interviews in which there is no indication that the perpetrator is also a victim.

Resources

US Resources

- National Center for Missing and Exploited Children (NCMEC): NCMEC is a non-profit organisation which works to prevent the exploitation and victimisation of children through providing a variety of services.
- TakeItDown: TakeItDown is a free service provided by NCMEC which facilitates the removal of non-consensual intimate imagery from participating online platforms. Victims submit images to be added to TakeItDown's hash-sharing database, preventing further victimisation.
- CyberTipline: The CyberTipline is NCMEC's central hub for reporting both on- and offline child exploitation. NCMEC can provide direct support to victims who report through the CyberTipline, as well as connecting them with law enforcement resources.
- FBI Internet Crime Complaint Center (IC3): Formerly known as the Internet Fraud Complaint Center, the IC3 is the FBI's central hub for reporting any "cyber-enabled crime", including hacking and online extortion. IC3 provides an online portal for victims and associated individuals to report online crimes to the bureau.
- National Association for Eating Disorders (NEDA): NEDA is a non-profit organisation that supports individuals and families affected by eating disorders through education, resources, interventions and research.
- 988 Lifeline: The 988 Lifeline is a national network of crisis centres who provide free and confidential emotional support to individuals struggling with suicidal thoughts, behaviours or crises.
- Crisis Text Line: Crisis Text Line is an organisation that provides free, text-based mental health support and crisis intervention.

UK Resources

- Child Exploitation and Online Protection Command (CEOP): Part of the UK's National Crime Agency (NCA), CEOP provides a reporting centre for child sexual exploitation and abuse, as well as educational resources for children, parents and professionals.
- NSPCC (National Society for the Prevention of Cruelty to Children): A leading UK child protection charity offering helplines, counselling and advocacy.
- Childline: A free, confidential helpline and online service provided by the NSPCC for children and young people up to the age of 19.
- Internet Watch Foundation (IWF): A UK charity working to remove CSAM and criminal content online. The IWF provides a public reporting hotline where illegal imagery can be flagged for rapid removal.
- Revenge Porn Helpline: A confidential support service for adults (18+) who have experienced non-consensual sharing of intimate images offering legal advice, emotional support and help in removing content online.
- Papyrus UK: A national charity dedicated to the prevention of youth suicide.
- Beat: The UK's leading charity supporting people with eating disorders.

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org