THE DIGITAL HUNTING GROUND

SEBASTIAN T.

An Informative Report on Online Predatory Tactics, Grooming Methodologies, and the Exploitation of Children Through Social Media and Gaming Platforms

This report contains difficult subject matter regarding child exploitation. It has been prepared with the goal of educating parents, educators, and community stakeholders about theevolving threat landscape targeting children online.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the first six months of 2025 alone, the National Center for Missing & Exploited Children received over 518,000 reports of online enticement, a 77% increase from the same period in 2024. Reports involving generative artificial intelligence exploded from approximately 6,800 to over 440,000 in that same timeframe, representing one of the most alarming technological shifts in the history of child exploitation. These are not merely statistics. Behind each report is a child whose trust was exploited, whose life trajectory was fundamentally altered by an adult predator who saw them as a target rather than a human being.

This report, prepared by Sebastian T., synthesizes open-source intelligence from law enforcement agencies, child advocacy organizations, academic research, and investigative journalism to provide a comprehensive analysis of how predators target, groom, and exploit children in 2026's digital ecosystem. The threat landscape has evolved with unprecedented rapidity. The COVID-19 pandemic accelerated children's digital adoption, creating populations of young people who spend an average of 7-8 hours daily online...often in spaces parents neither understand nor monitor. Predators have adapted faster than protective measures, exploiting platform vulnerabilities and the psychological vulnerabilities of adolescent development.

What emerges from this research is a portrait of sophisticated, organized exploitation that transcends the stereotypical image of the "stranger danger" predator. Modern online predators demonstrate advanced understanding of youth culture, platform mechanics, and psychological manipulation. They operate within gaming communities, social media platforms, and messaging applications, often hiding in plain sight among legitimate users. Many spend weeks or months cultivating relationships before introducing sexual content. Others leverage artificial intelligence to create convincing fake identities or to generate explicit imagery without requiring direct victim cooperation. Some work in coordinated groups, creating artificial peer networks that normalize exploitative behavior.

The data reveals several critical findings that demand immediate attention. First, the age of first contact continues to decrease, with documented cases of predatory contact with children as young as 7 years old on platforms ostensibly designed for gaming or education. Second, boys now comprise a significant portion of reported victims, representing a dramatic shift from historical patterns and reflecting predators' adaptation to male-dominated gaming spaces. Third, the timeline from initial contact to exploitation has compressed dramatically, with some cases progressing from first message to explicit image request in under 30 minutes. Fourth, platform hopping…moving targets from moderated platforms to encrypted messaging apps (Signal, Telegram, Kik, Session, and others)—has become nearly universal in documented grooming cases.

Perhaps most concerning is the ecosystem that enables this exploitation. While platforms have implemented safety features, these measures often prove inadequate against determined predators. In 2024, Roblox submitted 24,522 reports to NCMEC's CyberTipline, a number experts believe dramatically understates the true prevalence of exploitation on the platform. The platform now faces over 100 federal lawsuits alleging it facilitated child sexual exploitation. Discord and other messaging platforms remain under intense scrutiny, with 80 Roblox and Discord-related sexual abuse lawsuits centralized in California federal court in December 2025. The gap between platform popularity among children and effective safety implementation creates what investigators describe as a "target-rich environment" for predators.

This report examines these threats through multiple analytical lenses. We document the grooming process as it unfolds across digital platforms, identifying the specific tactics, language patterns, and psychological manipulation techniques predators employ. We provide platform-specific analysis of how exploitation manifests differently across Roblox, Fortnite, Discord, Instagram, Snapchat, TikTok, and emerging platforms. We examine the technical evasion methods predators use to avoid detection, from VPN usage to coded language. We analyze emerging threats including AI-generated child sexual abuse material, virtual reality exploitation, and the intersection of online grooming with child sex trafficking.

Critically, this report translates intelligence into action. We provide detailed guidance on warning signs parents can observe, technological controls that actually work, and most importantly, the communication strategies that research shows are most effective at protecting children. The evidence is clear: technological solutions alone cannot solve this problem. The most powerful protective factor against exploitation is a trusting relationship between parent and child where disclosure is met with support rather than punishment, where mistakes are treated as learning opportunities rather than evidence of failure, and where children believe their parents are allies rather than adversaries in navigating online spaces.

The concluding section of this report addresses parents directly, acknowledging the fear and overwhelm that this information naturally produces while providing practical, actionable guidance grounded in what actually protects children. Perfect vigilance is impossible. Perfect knowledge of every platform and threat is unrealistic. But presence, engagement, open communication, and willingness to understand children's digital lives—these are achievable, and these are what make the difference between children who disclose concerning situations and children who suffer in silence.

The statistics in this report are drawn from NCMEC's 2025 CyberTipline data and early 2026 reporting, FBI assessments, Department of Homeland Security evaluations, state and federal law enforcement case files, academic research from institutions studying online grooming behavior, civil litigation records, and investigative journalism from 2025-2026. Every factual claim is sourced in the references section. The threat is real, the scale is massive, and the trajectory is deeply concerning. But knowledge is power, and informed parents represent the most significant barrier predators face.

THE THREAT LANDSCAPE

To understand the current crisis, we must first grapple with its true magnitude. The numbers coming from authoritative sources paint a picture of exponential growth that outpaces our collective ability to respond. In 2024, NCMEC's CyberTipline received 20.5 million reports of suspected child sexual exploitation, a 43% decrease from 2023's 36.2 million reports. This decrease, however, does not signal improvement. Rather, it reflects a troubling reality**: *certain platforms have reduced reporting even as exploitation has increased, and the widespread implementation of end-to-end encryption has created blind spots where abuse thrives undetected.***

When NCMEC analyzed these 20.5 million reports and adjusted for the new 'bundling' feature that consolidates duplicate reports from viral incidents, they found that these reports actually represented 29.2 million separate incidents of exploitation. This means platforms reported approximately 7 million fewer incidents in 2024 compared to 2023, despite the REPORT Act mandating reporting of additional categories of abuse. The decline is not evidence of success; it is evidence of failure at scale.

The mid-year 2025 data release, the first time NCMEC has ever published statistics mid-year rather than waiting for year-end, reveals why they broke protocol. The trends are so alarming that waiting another six months to warn the public was deemed irresponsible. John Shehan, NCMEC's Senior Vice President overseeing the Exploited Children Division, called the increases a 'wake-up call' and stated plainly: ***"These statistics are not just numbers, they represent children experiencing unthinkable harm."***

The Numbers Behind the Crisis

Online enticement reports jumped from 292,951 in the first half of 2024 to 518,720 in the first half of 2025, a 77% increase in six months. For the full year of 2024, NCMEC received more than 546,000 reports concerning online enticement, a 192% increase compared to reports in 2023. We have moved from tens of thousands to over half a million reports annually in just a few years. This represents not gradual growth but explosive acceleration driven by technological change, increased screen time, and predator adaptation.

Financial sextortion reports increased from 13,842 to 23,593 in the first half of 2025 compared to the same period in 2024, a 70% increase. This particular form of exploitation targets predominantly teenage boys, often through Instagram or Snapchat, where predators pose as attractive peers, quickly escalate to explicit image exchange, then threaten to expose the victim unless paid. Since 2021, NCMEC is aware of at least 36 teenage boys who have taken their lives because they were victimized by sextortion. By 2025, at least 46 teen boys have died by suicide after falling victim to online sextortion scams since 2021. Cases in 2025 and early 2026 demonstrate the devastating speed of these attacks, some victims dying by suicide within hours of the initial contact.

Child sex trafficking reports surged from 5,976 in early 2024 to 62,891 in the first half of 2025, a staggering 952% increase. While some of this increase reflects the REPORT Act's expansion of mandatory reporting categories, investigators believe it also reflects traffickers' increasing use of online platforms for recruitment. In the first 11 months of 2025 (the first full year the REPORT Act was in effect), online platforms submitted 98,489 child sex trafficking reports, compared to 8,480 voluntary reports in 2023 before the Act's

passage. Children are groomed through gaming platforms and social media, then manipulated into meeting in person, where exploitation transitions from digital to physical.

NCMEC saw more than 1,300 reports tied to violent online groups in 2024, representing a 200% increase from 2023. These cases involve organized groups, often operating through Discord, that coerce children into performing acts of self-harm, recording these acts, and sharing them within the group. In one reported case, a young girl was coerced into cutting the perpetrator's online username into her arm at the direction of a violent group. ***"Just the power they have over my daughter is mind blowing,"*** her mother told NCMEC. The child responded to her abuser: ***"I love you, too."*** The psychological control these groups exert represents some of the most disturbing exploitation patterns investigators have encountered.

The AI Amplification Effect

Perhaps most alarming is the role of artificial intelligence in this crisis. Reports involving generative AI surged by 1,325%, climbing from 4,700 in 2023 to 67,000 in 2024. But that explosive growth was just the beginning. In the first six months of 2025, generative AI reports exploded to 440,419, representing a 6,345% increase over the first half of 2024. We have gone from thousands of reports to hundreds of thousands in barely 18 months.

What's driving this explosion? AI tools have democratized the creation of child sexual abuse material. Where previously a predator needed to coerce a child into creating explicit content, they can now generate highly realistic images using publicly available photographs like, school websites, social media profiles, and sports team photos. The technical barrier has evaporated. A predator with no coding skills can generate explicit imagery in seconds by typing prompts into consumer AI image generators.

With the rise of generative AI, offenders no longer always need to coerce content directly. Many are now creating fake sexualized images, so-called "deepfakes", using photos from children's public social media or school websites. These AI-generated images are then used for multiple purposes: blackmail (threatening to share the “evidence” unless the child complies with demands for real images or in-person meetings), normalization (showing children AI-generated images of themselves or peers to desensitize them to sexual content), and commercial distribution (selling synthetic child sexual abuse material in dark web marketplaces). The psychological impact on victims who discover AI-generated explicit images of themselves is profound, experiencing violation without having participated in any way, yet seeing their own face in abusive imagery.

Who is Being Targeted

The demographic profile of victims has shifted significantly. While girls aged 13-17 remain the largest victimized population, boys now comprise a substantial portion of reported victims, representing a dramatic shift from historical patterns. This reflects predators' adaptation to male-dominated gaming spaces and the exploitation of boys' relative lack of awareness about their vulnerability. Many boys and their parents believe online sexual exploitation “happens to girls,” creating a dangerous gap in awareness and vigilance.

Research from child protection organizations identifies elevated risk among several populations. LGBTQ+ youth are 1.5 to 2 times more likely to indicate prior experience of unwanted or potentially risky interactions online. LGBTQ+ teens were more than twice as likely as non-LGBTQ+ teens to have received a request for nudes from someone they don't know online, twice as likely to have been blackmailed or received

threats, and 3 times more likely to have had an adult attempt to befriend and manipulate them online. In a nationwide survey of over 600 homeless youth aged 17-25, 24% of LGBTQ youth had engaged in some form of commercial sex, with transgender youth at even greater risk due to experiences of rejection, marginalization, and employment discrimination. Children experiencing mental health challenges, family instability, academic struggles, or social rejection show increased susceptibility to grooming tactics that offer validation and attention.

Importantly, these vulnerabilities are not random, predators actively screen for them. They scan public profiles for indicators of emotional distress, search for posts suggesting family conflict or loneliness, identify children who post frequently about feeling misunderstood or isolated, and target children who share personal information suggesting lower parental supervision. The targeting is deliberate, systematic, and increasingly sophisticated.

The Global Nature of the Threat

NCMEC's data shows that 84% of CyberTipline reports resolve to locations outside the United States, underscoring the international nature of online exploitation. Predators operate across borders with impunity, exploiting jurisdictional complexities that complicate investigation and prosecution. A child in Florida may be groomed by a predator in Romania, using a platform headquartered in California, with communications routed through servers in Ireland.

Research from Childlight reveals that over 300 million children per year globally are victims of technology-facilitated sexual exploitation and abuse, approximately 10 cases per second worldwide. Regional variations exist, with different patterns emerging across North America, Eastern and Southern Africa, Southeast Asia, and other regions. Many financial sextortion cases are emanating from organized criminal groups in Nigeria and Côte d'Ivoire (Ivory Coast) in West Africa, with reports linking to those countries. Nigerian **"BM Boys**" use TikTok to show off wealth accumulated from blackmailing and sextorting youth, and use the platform to recruit and train others, providing scripts, stolen photos, and tips to avoid detection.

The scale is genuinely difficult to comprehend. We are not discussing isolated incidents or rare occurrences. We are describing a global epidemic of child exploitation that has found an ideal environment in the connected, largely unregulated, minimally supervised online spaces where children increasingly spend their time. Understanding this scale is not meant to paralyze parents with fear, it is meant to convey that addressing this threat requires serious, sustained attention commensurate with its severity.

HOW PREDATORS BUILD TRUST AND CONTROL

To effectively protect children, we must understand how grooming actually works, not as a theoretical construct, but as a practiced methodology refined through experience and shared among predator communities. Online grooming follows predictable patterns that research has documented across thousands of cases. While individual tactics vary, the underlying psychological manipulation remains remarkably consistent. Predators are not improvising; they are following established playbooks that exploit fundamental aspects of adolescent psychology and development.

Recent research using machine learning to analyze grooming conversations has identified specific language patterns, emotional tones, and progression sequences that distinguish grooming from legitimate interaction. Studies published in 2025 demonstrate that predators use measurably more positive language in early stages flattery, compliments, affirmations to establish themselves as sources of validation and support. They systematically mirror the target's interests, vocabulary, and communication style to create the perception of shared identity. They demonstrate detailed knowledge of youth culture, current music, gaming trends, social media personalities that makes them appear age-appropriate even when they are decades older than their targets.

Stage One: Target Selection and Reconnaissance

Grooming begins before first contact. Predators conduct reconnaissance to identify vulnerable targets and gather intelligence for initial approach. They scan public profiles for specific indicators: recent posts expressing loneliness, sadness, or frustration with family; profile information revealing single-parent households or family conflict; public sharing of school names, sports teams, or locations; evidence of minimal parental supervision through posting patterns and times; interests in mature content or discussions beyond typical age-appropriate topics; large friend lists suggesting the child accepts contact from unknown users.

This reconnaissance phase is often extensive. Predators may observe a potential target for days or weeks, learning their schedule, interests, friendship networks, and vulnerabilities before making contact. They research the games the child plays, the influencers they follow, the music they like. When contact occurs, it appears remarkably well-informed and coincidental, ***"I can't believe you like that band too!"*** or ***"I just started playing that game, do you have any tips?"*** when in reality, it is carefully engineered based on gathered intelligence.

FBI analysis has identified that predators increasingly use automated tools to scan social media for potential targets. They search hashtags associated with mental health struggles, family issues, or isolation. They identify children participating in communities where sharing personal information is normalized. They maintain spreadsheets or databases tracking potential targets, noting optimal times for contact and specific vulnerabilities to exploit.

Stage Two: Establishing Connection and Building Trust

Initial contact appears innocent and age-appropriate. The predator presents as a peer or slightly older teen facing similar challenges. They offer compliments that feel genuine: ***"You seem really mature for your age"*** or ***"You're really good at this game, I wish my friends were this skilled."*** They share (often fabricated) personal information about their own lives: struggles with school, conflict with parents, feeling misunderstood by peers. This sharing creates the impression of reciprocity and intimacy.

The predator invests heavily in this stage, sometimes communicating multiple times daily for weeks or months. They become a reliable presence: always available, always supportive, and always interested. For children experiencing genuine loneliness or family conflict, this attention feels profoundly validating. The predator positions themselves as uniquely understanding: ***"Nobody else gets me like you do"*** or ***"I can talk to you about things I can't discuss with anyone else."***

Research on grooming behavior shows predators deliberately create emotional dependency during this stage. They provide support during difficult moments, celebrate successes, remember details about the child's life that even close friends might forget. They become integrated into the child's emotional landscape as a primary source of validation and support. This investment creates the foundation for later exploitation, the child now has significant emotional investment in the relationship and fears losing it.

Stage Three: Isolation and Risk Assessment

With trust established, the predator begins isolating the victim and assessing detection risk. This occurs gradually through seemingly innocent questions***: "Do your parents check your phone?" "Does anyone else know we're friends?" "What do your parents think about you gaming/using social media?"*** The predator is mapping the surveillance environment and identifying opportunities for undetected communication.

The predator introduces the concept of secrecy, often framed as protecting a 'special' relationship: ***"This ____ is just between us, right?"*** or ***"I don't think your parents would understand our friendship."*** They may disparage parents or other authority figures: ***"Parents never understand"*** or ***"Adults always assume the worst."*** They create an 'us versus them' dynamic that positions the child's relationship with the predator as something precious that must be protected from interfering adults.

During this stage, predators often suggest moving communication to less monitored platforms. A relationship that began in a moderated game chat moves to Discord. Discord conversations migrate to Snapchat, WhatsApp, Signal, Telegram, where messages disappear. Each platform hop reduces visibility and accountability while normalizing the idea that this relationship needs privacy. By the time sexual content is introduced, the relationship exists in spaces parents don't know about, on platforms they don't understand.

FBI reports indicate this platform hopping has become nearly universal in documented grooming cases. Roblox to Discord to Snapchat represents one common progression. Investigators describe this as the predator ***"walking***

the child away from the playground", each step increasing isolation and reducing the likelihood of detection or intervention.

Stage Four: Desensitization and Sexualization

With the relationship isolated and trust firmly established, the predator begins introducing sexual content. This progression is carefully calibrated to avoid alarming the victim. It typically starts with humor: sexual jokes or memes that test the child's comfort level. If the child responds positively or doesn't object, the predator escalates. Questions become progressively more personal: ***"Do you have a boyfriend/girlfriend?" "Have you ever kissed anyone?" "What do you think about sex?"***

The predator frames these conversations as normal peer interaction: ***"Everyone our age talks about this stuff"*** or ***"I thought you were mature enough to have this conversation."*** They may share (fabricated or real) sexual experiences to establish expectation of reciprocity. They introduce sexual content as education or exploration: ***"I want to make sure you're informed"*** or ***"It's natural to be curious about these things."***

Research on grooming discourse shows predators use specific linguistic strategies during this phase. They employ progressive compliments focused on physical appearance, introduce sexual vocabulary gradually while gauging comfort, use hypothetical questions ***("What would you do if..."***) to discuss sexual scenarios without direct requests, and position sexual content as evidence of trust or intimacy between them.

For children with limited sexual education or experience, this information may seem genuinely educational. For those experiencing normal adolescent curiosity, the predator appears to be a safe person to explore questions they're uncomfortable asking adults. The predator exploits natural developmental curiosity while positioning themselves as the appropriate source for this information.

Stage Five: Exploitation and Control

With the groundwork laid, the predator makes explicit requests***: "I want to see what you look like"*** or ***"Can you send me a picture?"*** These requests start relatively innocuous, maybe a picture in a swimsuit or sleepwear, before escalating to fully explicit content. The predator frames these requests through the lens of the established relationship***: "If you really care about me, you'd do this"*** or ***"This is what people who love each other do."***

Once the predator obtains any explicit image, the power dynamic shifts decisively. The predator now possesses material that can be used for coercion. Some immediately reveal their intention to exploit: ***"If you don't send more/meet me in person/do what I say, I'll send these to your parents/school/friends."*** Others continue the facade of relationship while using implicit threat, the child understands the predator could release the images at any time.

This is where many cases transition to what investigators term **'sextortion'**, the continued extraction of images, videos, or in-person meetings through explicit blackmail. The predator may demand increasingly extreme

content, monetize the child's images by selling them, or force the child to recruit other victims. At this point, the child often feels completely trapped…believing they will face legal consequences (predators often claim the child committed a crime by creating the images), social destruction (if images are shared with peers or family), and unbearable shame.

Group Grooming and Coordinated Targeting

FBI analysis has identified an emerging and deeply concerning trend: coordinated grooming by multiple predators working together. In these schemes, groups of adults pose as children, join gaming clans or social media groups targeting children, and use each other to normalize the exchange of sexual material. A child joining what appears to be a group of peers finds an environment where sharing explicit images seems to be normal peer behavior, when in reality, all or most of the 'peers' are adult predators.

This group dynamic creates immense pressure to conform. Children, who are developmentally oriented toward peer acceptance, find it extremely difficult to resist behavior that appears normative within their peer group, even when that behavior is objectively harmful. The child may believe they are the only one uncomfortable with the requests, when in reality they are the only actual child in the group.

The sadistic online exploitation groups documented by NCMEC represent an extreme evolution of this coordinated approach. These groups, often operating through Discord, create cult-like environments where children are coerced into performing acts of self-harm, recording these acts, and sharing them within the group; ***(Ex. District of Columbia | Leaders of 764 Arrested and Charged for Operating Global Child Exploitation Enterprise | United States Department of Justice.).*** The psychological manipulation is profound, children describe feeling they 'belong' to these groups, expressing love for the predators coercing them into harming themselves. The combination of isolation, manipulation, and manufactured peer pressure creates a psychological trap that children, with their developing brains and limited life experience, have minimal capacity to recognize or escape.

WHERE AND HOW EXPLOITATION OCCURS

Understanding the threat landscape requires examining where exploitation actually occurs. Different platforms create different opportunity structures for predators. The features that make platforms engaging for children are: social connection, real-time communication, and content sharing…are the same features predators exploit. In 2024, certain platforms emerged as particularly high-risk environments based on CyberTipline reporting data, civil litigation, criminal prosecutions, and investigative journalism.

Gaming Platforms: The New Hunting Ground

Roblox has become the subject of intense scrutiny and multiple lawsuits alleging systemic failures in child protection. With approximately 85 million daily active users, 40% of whom are under age 13, the platform presents an enormous target population for predators. In 2024, Roblox submitted 24,522 reports to NCMEC's CyberTipline, a number that cybersecurity analysts believe represents a fraction of actual exploitation occurring on the platform.

The platform's user-generated content model creates thousands of game environments with varying levels of moderation. Predators create games specifically designed to attract children, 'adoption' games, 'hangout' spaces, 'dating' simulators, then use these environments to initiate contact. Once initial rapport is established within the game, predators push communication to Discord or Snapchat, where moderation is weaker and parents are less likely to monitor activity.

Multiple state attorneys general have initiated investigations or filed lawsuits against Roblox. Kentucky Attorney General Russell Coleman's October 2025 lawsuit alleges that ***"Roblox is a platform, a playground for predators"*** with insufficient guardrails exposing children to predators, violence and sexually explicit material. Tennessee Attorney General Jonathan Skrmetti filed suit in December 2025, alleging Roblox ***"lures children into an environment it knows is dangerous but promises is safe."*** Louisiana, Florida, Oklahoma, Iowa, and Texas have launched similar investigations or lawsuits.

By December 2025, more than 100 federal lawsuits had been filed against Roblox, which were consolidated into MDL 3166, In re: Roblox Corporation Child Sexual Exploitation and Assault Litigation, with 85 pending claims as of January 5, 2026. A Hindenburg Research report referenced in civil litigation accused Roblox of prioritizing ***"profit and attractiveness to investors above online safety"*** and exposing children to an ***"x-rated hellscape, grooming, pornography, violent content and abusive speech."***

Case documentation reveals a pattern: children as young as 9 years old meet predators through Roblox gameplay, communication moves to external platforms, and exploitation progresses rapidly once outside Roblox's moderation systems. In documented cases, predators have offered Robux (in-game currency) to incentivize children to move conversations off-platform or to coerce participation in exploitation. The platform's economy

thus becomes a tool for grooming, predators leverage children's desire for in-game advancement to facilitate abuse.

For context on the platform's reach: a December 2017 study found children ages 5-9 primarily spend time playing Roblox over all other activities. By 2020, monthly player base included half of all American children under 16. The platform is not a niche product, it is where American children spend their time, and predators have followed them there.

Discord: The Migration Destination

Discord appears repeatedly in exploitation cases not as the initial contact point but as the platform where grooming intensifies after initial contact on gaming platforms. In 2024, Discord submitted 241,354 reports to NCMEC, a 28% decrease from the 339,412 reports it submitted in 2023, despite the REPORT Act's passage mandating increased reporting. This decline raised concerns from federal legislators about platform compliance. The platform has been named in numerous civil lawsuits and appears on the National Center for Sexual Exploitation's 'Dirty Dozen' list for the fourth consecutive year.

Discord's design creates ideal conditions for exploitation. The platform allows self-reported ages with minimal verification, enabling predators to easily create accounts claiming to be minors. Users under 13 can access the platform by falsifying their birthdate, a barrier so trivial as to be effectively nonexistent. The platform's server structure creates thousands of private spaces where predators operate communities, some explicitly designed for grooming. Voice and video chat capabilities provide richer interaction than text-only platforms, accelerating relationship development.

New Jersey's Attorney General sued Discord in April 2025 under the Consumer Fraud Act, alleging deceptive practices and insufficient safety features. The lawsuit criticizes default messaging settings that enable stranger contact, weak age verification systems, and misleading marketing positioning Discord as a 'safe space' for teens. Florida has issued subpoenas investigating Discord's child safety protocols alongside similar inquiries into Roblox.

Criminal cases demonstrate Discord's role in exploitation escalation. In January 2025, Jacob Lozano received a 32-year sentence for allegedly luring three boys through Discord after initial contact on Fortnite. In April 2025, Lonnie Youmans was charged with sexual exploitation of children through Discord, allegedly grooming victims as young as 12 and threatening to leak explicit images if demands weren't met. These cases follow a pattern**: initial contact through gaming → migration to Discord → intensified grooming → coercion for explicit content → blackmail to prevent disclosure**.

The sadistic online exploitation groups that NCMEC has identified operate primarily through Discord. These violent groups, including the notorious 764 network, target children through public Discord servers, gaming platforms, and social media, then coerce them into recording acts of self-harm. The platform's relative anonymity, combined with community features that create artificial peer environments, makes it particularly suited to these coordinated manipulation campaigns.

.

Social Media Platforms: Scale Meets Vulnerability

Facebook (Meta) submitted 8,590,357 reports to NCMEC in 2024, representing 42% of all CyberTipline reports despite the 43% overall decline in reporting. This massive volume reflects both Meta's user base and its detection capabilities, but also the scale of exploitation occurring across its platforms (Facebook, Instagram, Messenger). Instagram in particular presents significant risk for adolescents due to its visual focus and strong presence among teen users.

Predators use Instagram's discovery features to identify targets through hashtag searches, explore pages showing similar users, location tags revealing schools or hangout spots, and suggested user features based on algorithmic connections. Public accounts, which many teens maintain to grow follower counts, provide predators with extensive personal information before any direct contact. Research shows predators conduct reconnaissance through post history to identify emotional vulnerabilities, family situations, and optimal approach strategies.

Instagram's Direct Message system provides private communication with features including disappearing messages that reduce evidence, voice and video calling without leaving text transcripts, story replies that create the impression of organic conversation initiation, and the ability to unsend messages, complicating forensic investigation. Predators create fake profiles using stolen images, often maintaining multiple personas to create the appearance of a social network validating their fake identity.

Financial sextortion cases disproportionately occur through Instagram and Snapchat. The typical pattern: an attractive profile messages a teenage boy, conversation quickly becomes sexual, explicit image exchange occurs, followed immediately by blackmail demanding payment to prevent distribution to the victim's contacts. NCMEC receives nearly 100 financial sextortion reports daily. By 2025, at least 46 teen boys have died by suicide after falling victim to online sextortion scams since 2021, including the February 2025 case where AI-generated imagery was used as blackmail material.

TikTok submitted 1,359,806 reports in 2024, a substantial volume reflecting both its popularity among young users and exploitation occurring within it. The platform's algorithm rapidly connects users with similar interests, including predators and potential victims. The comment system allows predators to identify vulnerable users through their public comments and content. Live streaming provides real-time interaction with thousands of viewers, creating opportunities for both targeted grooming and opportunistic contact.

Predators exploit TikTok trends to appear relatable and current. They participate in viral challenges, use popular sounds and effects, and demonstrate knowledge of TikTok culture that makes them appear age-appropriate. The duet and stitch features justify communication as content collaboration. For teens seeking validation through social media success, predators offering to 'boost' their content or 'collaborate' with larger creators present an appealing but dangerous opportunity.

Snapchat's Unique Risk Profile

Snapchat's disappearing message feature creates a false sense of privacy that encourages risk-taking behavior. The platform appears in over 60% of sextortion cases according to law enforcement reports. Its design philosophy: messages that vanish, and reducing permanent record of communication, makes it attractive for both legitimate privacy-conscious users and predators seeking to avoid evidence creation.

The Snap Map feature, when enabled, reveals real-time location, information predators can use to determine when targets are home alone, identify movement patterns, or locate targets for in-person contact. Quick Add surfaces friend suggestions based on minimal connection, mutual friends, phone contacts, or proximity, expanding networks in ways that introduce strangers. The streak feature, which rewards consecutive daily communication, normalizes constant contact and creates social pressure to maintain communication even when uncomfortable.

The psychological impact of disappearing messages is significant. Children perceive requests made via Snapchat as less serious or permanent than requests via text or email. This perception makes them more likely to comply with progressively inappropriate requests, the evidence will disappear, so it feels less real, less permanent, less dangerous. This is precisely why predators prefer the platform.

RECOGNIZING EXPLOITATION IN PROGRESS

Early intervention depends on recognizing warning signs before exploitation fully develops. While no single indicator proves exploitation, clusters of concerning behaviors warrant careful attention and open conversation. The research literature and investigator experience have identified reliable indicators that children may be experiencing grooming or exploitation.

Behavioral Changes

Excessive screen time, particularly at unusual hours, like late night or early morning use suggests communication the child wants to keep private from parents. Emotional volatility correlated with device use: becoming upset, anxious, or defensive when devices are unavailable or when parents ask about online activity. Withdrawal from previously enjoyed activities, family time, or face-to-face friendships in favor of online interaction. Secretive behavior around device use, quickly minimizing screens, taking devices to private spaces, using devices under covers at night.

Children experiencing grooming may receive unexpected packages or gifts whose source they cannot or will not clearly explain. They may demonstrate knowledge of relationships or sexual topics beyond age-appropriate understanding. They may express that parents ***"wouldn't understand"*** their online friendships or become defensive when parents show interest in their digital lives. Academic performance may decline as exploitation consumes emotional and cognitive resources.

Digital Evidence

Direct observation of digital activity may reveal concerning patterns. Multiple accounts or profiles parents were unaware of, particularly accounts with different ages or personal information than the child's real identity. Communication with people parents haven't met, especially if the child resists introducing these 'friends' or providing information about them. Platform hopping, starting on a game, moving to Discord, then to Snapchat or WhatsApp, is a nearly universal pattern in grooming cases.

Message content visible through notification previews may show age-inappropriate conversations, requests for privacy or secrecy, discussion of meeting in person with someone met online, requests for images or videos, offers of money or gifts from unknown sources, or pressure to keep the relationship secret from parents. Children may receive messages at school hours from people claiming to be students, or at times suggesting the sender is in a different time zone than they claim.

Installation of apps designed to hide content, 'vault' apps that appear as calculators or other innocent tools but actually hide photos and messages, VPN apps that mask location and activity, or messaging apps parents don't recognize, all warrant investigation. While teens may seek privacy for legitimate reasons, extreme measures to hide digital activity often indicate concerning situations.

Psychological Indicators

Children experiencing exploitation often display sleep disturbances, changes in appetite, increased anxiety or depression, or physical signs of stress like nail-biting, hair-pulling, or skin-picking. They may become emotionally dependent on online relationships, expressing that an online friend is the ***"only person who understands them"*** or that they ***"can't live without"*** specific online relationships.

Crucially, children being groomed may not appear distressed, the predator has positioned themselves as a source of positive validation and emotional support. The child may seem happier with increased online activity initially, only showing distress once exploitation escalates to coercion or blackmail. This makes early identification challenging, the warning signs may be subtle behavioral changes rather than obvious distress.

DEEPFAKES, SEXTORTION, AND SYNTHETIC ABUSE

The integration of generative AI into exploitation represents perhaps the most significant threat evolution in decades. The 6,345% increase in AI-related exploitation reports between the first half of 2024 and first half of 2025, from 6,835 to 440,419 report, signals a fundamental shift in how exploitation occurs. AI has eliminated technical barriers that previously limited who could create child sexual abuse material, how quickly it could be created, and how realistic it could appear.

Deepfake Technology and Non-Consensual Imagery

Current generative AI tools can create highly realistic explicit images using innocent source photos like, school pictures, social media posts, sports team photos. A predator no longer needs to coerce a child into creating explicit content; they can generate it synthetically using publicly available images. These AI-generated images serve multiple exploitative purposes in documented cases.

First, blackmail without prior victim cooperation, predators create fake explicit images, then threaten to share them unless the victim provides real explicit content or complies with other demands. The victim has done nothing wrong, participated in no way, yet sees their own face in abusive imagery and faces the same social destruction threat as if the images were real. The February 2025 suicide of a teenage boy who was threatened with an AI-generated nude demonstrates the psychological impact is equivalent to actual imagery.

Second, normalization and desensitization, predators show children AI-generated explicit images of themselves or peers to normalize sexual content, reduce inhibitions about creating real content, or demonstrate ***"what everyone is doing."*** Seeing themselves or classmates in explicit imagery, even synthetic imagery profoundly affects adolescent perception of sexual norms and boundaries.

Third, commercial distribution. AI-generated child sexual abuse material is bought and sold in dark web marketplaces. While no actual child was exploited in the image's creation, the material normalizes and perpetuates demand for child exploitation. Some predators use AI tools to 'age progress' existing abuse material or to create synthetic material featuring specific children on demand.

The 'deepfake' phenomenon has also emerged as a serious problem in schools. Teen boys use AI tools to generate nude images of female classmates, distributing these images as pranks or revenge. While often dismissed as adolescent misbehavior, the psychological impact on victims is profound, experiencing violation without consent, seeing explicit imagery of themselves they never created, facing peer ridicule and social destruction. Some victims have transferred schools or required mental health intervention for trauma resulting from synthetic imagery.

AI-Enhanced Social Engineering

Large language models enable qualitatively new forms of manipulation. Predators can now use AI to maintain dozens of simultaneous grooming conversations with contextually appropriate responses, analyze target social media to identify psychological vulnerabilities and craft personalized grooming approaches, generate convincing personas complete with coherent backstories and communication styles, and deploy chatbots to conduct initial contact and victim screening before human predators take over promising interactions.

Research published in 2025 demonstrates that AI language models can be prompted to generate grooming conversations, simulate explicit chats with fictional minors, or provide tactical guidance on manipulation techniques. While major AI companies implement safeguards against such uses, determined actors bypass these protections through jailbreaking techniques or use open-source models without built-in restrictions.

The efficiency gains are profound. Where a human predator might effectively groom 3-5 targets simultaneously, AI assistance allows scaling to dozens or hundreds. Where developing a convincing fake persona required research and consistency maintenance, AI generates complete identities instantly. Where maintaining appropriate emotional tone across multiple conversations challenged predators, AI ensures contextually appropriate responses. The technology industrializes grooming in ways previously impossible.

Voice and Video Synthesis

Emerging voice cloning technology allows predators to create convincing audio of specific individuals using minimal source material, as little as a few seconds of audio. This enables phone-based scams where predators impersonate parents calling schools to authorize student release, or impersonate children calling parents to explain why they're with a 'friend' or 'need to be picked up' at unexpected locations. Video synthesis technology, while currently requiring more technical skill, is advancing rapidly and will soon enable real-time video manipulation.

Voice synthesis also enables predators to create more convincing online identities. Where previously text chat might reveal inconsistencies in a fake identity, synthetic voice communication sounds appropriately age-appropriate, gendered, and emotionally responsive. The predator claims to be a 15-year-old girl, and AI generates a voice that sounds exactly like one.

Detection Challenges and Future Trajectory

Current detection methods struggle with high-quality synthetic content. Law enforcement and platform moderators cannot reliably distinguish AI-generated imagery from photographs without forensic analysis. Parents certainly cannot. This means by the time synthetic material is identified as AI-generated, damage may already be done…the child has been blackmailed, distributed the material thinking its real, or experienced psychological trauma from seeing it.

The trajectory is deeply concerning. As models improve, synthetic content becomes more convincing. As tools become more accessible, technical barriers disappear entirely. As awareness spreads among predator communities, adoption accelerates. NCMEC's data showing 6,345% increase in just one year suggests we are in the early stages of AI-enabled exploitation, with the worst impacts potentially still ahead.

REAL-WORLD EXPLOITATION PATTERNS

Abstract statistics require concrete examples to fully comprehend. The following cases, drawn from law enforcement records, civil litigation, and investigative journalism, illustrate how the tactics, platforms, and technologies described in this report manifest in actual exploitation. Identifying details have been altered where necessary to protect victims' privacy.

Case 1: The Roblox-to-Discord Pipeline

A 9-year-old girl joined Roblox in 2021 with parental permission after her father researched the platform and believed it safe for children. Over months of gameplay, she befriended a user who presented as a fellow child. This 'friend' offered Robux, helped with difficult game levels, and communicated regularly through Roblox chat. After trust was established, the predator suggested moving to Discord 'to chat better while playing other games.'

On Discord, communication intensified. The predator introduced sexual topics gradually; first jokes, then questions, then explicit content. By the time the child was 12, she had been coerced into creating and sending explicit images. When she tried to stop, the predator threatened to send the images to her family and school. The abuse continued for months before the child disclosed to her mother after the predator discovered her physical location through information shared during their communication.

Investigation revealed the predator was a 27-year-old man operating multiple Roblox accounts targeting prepubescent girls. He had victimized at least 15 children using identical tactics: initial contact on Roblox, migration to Discord, gradual sexualization, exploitation, then blackmail. His Roblox accounts appeared legitimate with years of gameplay history. His Discord server appeared to be a gaming community but was actually a grooming operation.

Case 2: Financial Sextortion Through Instagram

A 16-year-old boy received an Instagram direct message from a profile appearing to be an attractive girl his age. The profile had hundreds of followers and regular posts suggesting a real person. Conversation began casually, moved quickly to flirtation, then to explicit image exchange. Within 30 minutes of initial contact, the 'girl' requested explicit images and the boy complied.

Immediately after receiving the images, the tone shifted. The predator revealed they had the boy's contact list, would send the images to everyone he knew unless he paid $500 within an hour. The payment demand increased when initial compliance occurred. Over 48 hours, the boy paid $1,200 before disclosing to parents. The stress of blackmail and shame led to suicidal ideation requiring hospitalization.

Investigation determined the profile was operated from Nigeria as part of a financial sextortion ring targeting American teenage boys. The attractive profile pictures were stolen from a European Instagram user

unaware her images were being weaponized. The operation contacted hundreds of potential victims daily, used scripted conversation templates, and moved only successful extortions to human operators for payment collection.

Case 3: AI-Generated Imagery and Tragic Outcome

In February 2025, a teenage boy discovered explicit images of himself circulating among classmates. The images appeared realistic but had been generated using AI from his social media photos. The images were accompanied by threats: pay $3,000 or the images would be sent to his family, school, and college admissions offices. Unable to pay and terrified of disclosure, the teen died by suicide days later.

Investigation found the images were created using freely available AI tools, required no technical sophistication, and took minutes to generate. The perpetrator had targeted dozens of students from the victim's school, generating explicit imagery of each, then blackmailing those who appeared most susceptible to coercion. The psychological impact of synthetic imagery proved equivalent to actual images, the victim experienced the same shame, fear, and desperation despite never participating in any inappropriate behavior.

Case 4: Sadistic Online Group Exploitation

A 13-year-old girl joined a Discord server advertised in a Roblox game as a 'hangout' for teens interested in anime. The server appeared to have dozens of members her age discussing shared interests. Over weeks, she developed friendships within the group. Gradually, conversations introduced darker themes such as, self-harm as artistic expression, cutting as demonstrating commitment to the group, proof of belonging through increasingly extreme acts.

The girl was eventually coerced into cutting a group symbol into her arm and recording the act. When completed, group members praised her: ***"You're so strong," "We love you," "You're one of us now."*** Her mother discovered the injury and reported to NCMEC. Investigation revealed nearly all 'members' were adult men running fake profiles. The single-digit number of actual children in the server were all being groomed toward increasingly serious acts of self-harm and sexual exploitation.

The mother later reported to investigators: ***"Just the power they have over my daughter is mind blowing. She truly believed these people loved her. She would do anything they asked. Please help."*** The psychological manipulation had created bonds of affection between victim and abusers, a trauma bond exploiting fundamental human needs for belonging and acceptance.

PROTECTIVE STRATEGIES: WHAT ACTUALLY WORKS

Understanding threats requires equal attention to protection. Research evidence and investigator experience have identified strategies that meaningfully reduce exploitation risk. No approach eliminates risk entirely, that is an impossible standard. The goal is reducing risk to acceptable levels while maintaining healthy parent-child relationships and age-appropriate digital independence.

The Primary Protective Factor: Relationship

Research consistently identifies the parent-child relationship as the most powerful protective factor against exploitation. Children who believe they can approach parents with concerns, questions, or mistakes without facing disproportionate punishment are significantly more likely to disclose concerning situations before they escalate. Predators rely on isolation and secrecy. A child who believes ***"my parents will help me"*** rather than ***"my parents will take away my devices/ground me/be angry"*** is substantially more protected.

This requires conscious cultivation. When children make digital mistakes, clicking suspicious links, sharing more information than they should have, accepting friend requests from people they don't know, responding with support and education rather than anger creates foundation for disclosure when stakes are higher. When children come to parents saying, ***"someone online is making me uncomfortable,"*** being met with problem-solving rather than 'I told you so' or immediate device confiscation determines whether they'll disclose future incidents.

This does not mean no boundaries or consequences, children need structure and guidance. It means proportionate responses that maintain trust. Temporary restriction of privileges while addressing a safety issue is reasonable. Permanent device confiscation that eliminates all digital social connection is often counterproductive, children learn to hide activity rather than seek guidance.

Age-Appropriate Digital Literacy Education

Children need explicit education about online threats appropriate to their developmental stage. For younger children (ages 7-10): ***"Not everyone online is who they say they are. Some adults pretend to be kids to trick children. If anyone online asks you to keep secrets from me, tell me immediately. If anyone makes you feel uncomfortable, come to me and I'll help you, you won't be in trouble."***

For pre-teens (ages 11-13): More detailed discussion of grooming tactics, how predators build trust before making inappropriate requests, why they ask to move conversations to different platforms, and how initial friendliness can progress to exploitation. Explain that predators study youth culture to appear relatable, that feeling a special connection with someone online can be engineered, and that adults who truly care about children respect boundaries rather than pressing for increasing intimacy.

For teenagers (ages 14+): Frank discussion of sextortion, financial exploitation schemes, how explicit images shared privately can become public, legal consequences of creating explicit imagery even of themselves, and the psychology of manipulation. Teens should understand that once explicit images are shared digitally, control is permanently lost; deletion, promises to keep secret, and trust are all ineffective once images are in another person's possession.

Technological Controls and Monitoring

Technology-based protections work best when paired with relationship-based protections, not as substitutes for them. Effective approaches include: parental control software providing activity oversight and content filtering (with transparency about what's monitored), device-free zones and times (bedrooms at night, family meals, etc.), privacy settings maximized on all platforms, location services disabled for social media, and periodic device checks that are announced as family policy rather than secretive snooping.

Platform-specific configurations include…Instagram: private account, message requests limited to followers, story sharing restricted; Snapchat: Ghost Mode enabled, contact limited to confirmed friends, Quick Add disabled; TikTok: private account, duets/stitches restricted to followers, commenting limited; Discord: DMs restricted to friends, server discovery disabled, careful review of server membership; Roblox: contact restricted to approved friends, trading disabled, chat settings appropriate to child's age.

Important caveat: determined children often find workarounds to technological controls. They use friends' devices, create secret accounts, use VPNs to bypass restrictions. This is why relationship-based protection is primary, a child motivated to hide activity from parents will usually succeed. A child who trusts parents and believes in their guidance is protected by internal compass rather than external barriers.

Recognizing and Responding to Concerns

If concerns arise, behavioral changes, evidence of concerning relationships, discovery of inappropriate content, response protocol matters. Remain calm to encourage continued openness. Express concern for the child's wellbeing rather than anger about rule violations. Document evidence (screenshots) before anything is deleted. Report to platform using safety reporting features. Contact law enforcement if exploitation has occurred or is imminent. Contact NCMEC CyberTipline (www.cybertipline.org) for serious incidents. Consider professional mental health support for the child.

Critically: do not confront the predator directly. Do not delete evidence thinking this protects the child, evidence is essential for investigation. Do not blame the child regardless of their decisions or actions, children cannot consent to exploitation regardless of apparent participation. The sophistication of manipulation means children often believe they made free choices when in reality they were systematically coerced.

MOVING FORWARD WITH KNOWLEDGE AND HOPE

If you've read this far, you've absorbed information that is genuinely difficult to process. The scale of exploitation, the sophistication of tactics, the vulnerability of children in digital spaces, these realities are heavy. The natural response is fear, perhaps anger at platforms or predators, possibly guilt about past decisions or monitoring failures. These reactions are entirely human and understandable.

But fear without direction is paralyzing rather than protective. The purpose of this report is not to terrify but to educate, to provide knowledge that enables informed protection. You now understand threats most parents remain unaware of. That knowledge is power. That knowledge makes you better able to protect your child than you were before reading this report.

What You Need to Hear

First: You cannot protect your child from every risk. This is impossible. Accept this limitation not as failure but as reality of parenting in any era, amplified by digital connectivity. Perfect vigilance, comprehensive monitoring of every platform, awareness of every online interaction…these are unachievable standards that generate anxiety without corresponding protection. Effective protection is not perfect protection; it is sufficiently good protection that reduces risk to acceptable levels.

Second: Your child's digital life is not inherently dangerous. Online spaces enable learning, creativity, social connection, identity exploration, and genuine friendship. Millions of children interact online daily without exploitation. The goal is not eliminating online activity but enabling safer participation through education, monitoring, and open communication.

Third: If your child has been victimized, this is not their fault. Children cannot consent to exploitation regardless of apparent participation. Predators study manipulation as a practiced skill. They exploit normal adolescent psychology, desire for validation, curiosity about sex, need for independence, susceptibility to peer pressure. A child who was groomed did not fail; they were systemat ically manipulated by an adult who knew exactly what psychological levers to press.

Fourth: If you discover concerning activity, your response determines whether your child continues seeking your guidance or begins hiding everything. Disproportionate reactions, complete device removal, extreme punishment, expressions of betrayal or disappointment, teach children that bringing problems to parents results in worse outcomes than dealing with problems alone. Measured responses, temporary restrictions while addressing safety, problem-solving rather than blame, professional support if needed, maintain trust while addressing real concerns.

Practical Steps Forward

Start with conversation. If you haven't discussed online safety with your child, begin tonight. Adapt the discussion to your child's age. Acknowledge you're learning about online risks and want to understand their experiences. Ask what platforms they use, who they interact with, whether anyone has made them uncomfortable. Listen more than lecture. Believe what they tell you. Validate their feelings even when addressing concerning behavior.

Implement age-appropriate monitoring. For younger children (under 13), direct supervision of online activity is appropriate and expected. For teens, balance appropriate privacy with safety oversight. Consider family policies: devices charge in common areas overnight, periodic checks are announced family practice rather than secretive snooping, certain platforms or features restricted until maturity demonstrated.

Know what platforms your child uses. You don't need to master each platform, but understand their basic functions and risk profiles. Ask your child to show you what they do online. Many children enjoy teaching parents about platforms, this creates bonding opportunity while providing oversight.

Model healthy digital citizenship. Children learn more from observing parent behavior than from lectures. If you're constantly on devices during family time, ignoring them to check social media, or sharing personal information carelessly online, children internalize these patterns regardless of your stated rules for them.

If Exploitation Has Occurred

Discovering your child has been exploited is devastating. The violation feels personal, how did this happen to my child? Under my roof? While I believed they were safe? These feelings are valid and painful. They are also obstacles to helping your child if they prevent clear-headed response.

Your child needs three things from you: Unconditional love and support, they need to know your feelings toward them haven't changed, that you don't view them differently, that they didn't cause this. Professional help, trauma-informed therapist experienced with child exploitation can provide crucial support. Advocacy, navigating law enforcement, platform reporting, school notification if needed.

Things your child doesn't need: Shame or blame for their participation. Detailed questioning about exploitative interactions. Immediate removal of all technology without discussion. Broadcasting the situation to extended family or community. Treating them as damaged or changed. What they need is to still be seen as themselves, your child who experienced something terrible that wasn't their fault, who deserves support in healing, who remains the person they were before this happened.

The Long View

The statistics and cases in this report describe a genuine crisis. But they also describe something else: increased awareness, improved reporting, enhanced investigation, and growing legal accountability. Ten years ago, many of these cases would have gone unreported. Platforms had minimal safety features. Law enforcement lacked training and resources for digital investigations. Parents had no framework for understanding online risks.

Today, while threats have evolved, so have protections. NCMEC's CyberTipline receives and processes millions of reports. Law enforcement has specialized units investigating online exploitation. Platforms face legal and regulatory pressure to improve safety. Parents have access to information like this report. The problem has not been solved, far from it, but collective awareness and response have dramatically improved.

Your role in protecting your child is irreplaceable. No technological solution, platform safety feature, or law enforcement resource can substitute for an engaged parent who maintains open communication, provides age-appropriate education, implements reasonable monitoring, and offers unconditional support. These things are within your power. These things make profound difference.

The digital world is where your child's social life exists, where they learn and create, where they explore identity and form relationships. It's not going away. Your job is not preventing their participation but enabling safer participation. Armed with knowledge from this report, you're better equipped for that job than the vast majority of parents. Use that knowledge. Trust your judgment.

Maintain connection with your child. That's what actually protects them.

REFERENCES AND DATA SOURCES

This report synthesizes information from multiple authoritative sources including law enforcement agencies,child advocacy organizations, academic research, government reports, civil litigation records, and investigative journalism from 2024-2026. All factual claims are traceable to cited sources.

Primary Statistical Sources

NationalCenterforMissing&Exploited Children. 2024 CyberTipline Data Report. Published 2025. Retrieved from: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

National Center for Missing & Exploited Children. Mid-Year 2025 Report: Spike in online crimes against children a 'wake-up call.' Published September 2025. Retrieved from:

https://www.missingkids.org/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call

National Center for Missing & Exploited Children. *NCMEC Releases New Data: 2024 in Numbers.* Published 2025. Retrieved from: https://www.missingkids.org/blog/2025/ncmec-releases-new-data-2024-in-numbers

National Center for Missing & Exploited Children. *NCMEC on the Hill: "Online child exploitation escalating, more violent". December 2025. Retrieved from: https://www.missingkids.org/blog/2025/ncmec-on-the-hill-online-child-exploitation-escalating-more-violent*

U.S. Department of Homeland Security. Know2Protect: Online Child Sexual Exploitation & Abuse Informational Bulletin. Published November 2025. Available at: https://www.dhs.gov/sites/default/files/2025-11/25_1121_k2p_csea-onepager.pdf

Thorn. What the 2024 NCMEC CyberTipline Report says about child safety. Published May 2025. Retrieved from: https://www.thorn.org/blog/what-the-2024-ncmec-cybertipline-report-says-about-child-safety

Childlight: Global Child Safety Institute, University of Edinburgh. Technology-facilitated sexual exploitation and abuse research, 2024. Available at https://www.childlight.org

Law Enforcement and Government Sources

U.S. House ofRepresentatives Energy andCommerceCommittee. Testimony by Yiota Souras, NCMEC Chief Legal Counsel. March 26, 2025. Available at https://www.congress.gov

Federal Bureau of Investigation. Internet Safety 101: Grooming. Available at https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion

Federal Bureau of Investigation. *Sextortion: A Growing Threat Preying Upon Our Nation's Teens.* January 17, 2024. Available at: https://www.fbi.gov/contact-us/field-offices/sacramento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens

U.S. Department of Justice, Project Safe Childhood. Investigations and prosecutions data, 2024-2025. Available at: https://www.justice.gov

New Jersey Office of the Attorney General. State of New Jersey v. Discord Inc., filed April 17, 2025. Consumer Fraud Act litigation.

Kentucky Office of the Attorney General. Commonwealth of Kentucky v. Roblox Corporation, filed October 6, 2025. Available at: https://www.ag.ky.gov/Press%20Release%20Attachments/2025.10.06%20-%20%5BFINAL%5D%20KY%20Roblox%20Complaint.pdf

Tennessee Office of the Attorney General. *State of Tennessee v. Roblox Corporation,* filed December 18, 2025.

U.S. Senate Judiciary Committee. *Protecting Our Children Online Against the Evolving Offender.* Hearing, December 9, 2025.

Academic and Research Sources

Lorenzo-Dus, N.,Micallef, N.,Daish,P.,Paiement, A., Sahoo, D. Co-design of an Interactive AI Platform for Tactics-Based Detection of Online Grooming. Proceedings INTERACT 2025, Lecture Notes in Computer Science, vol 16111. Springer.

Frontiers in Pediatrics. Comparing machine learning models with a focus on tone in grooming chat logs. Volume 13, Published May 30, 2025. doi: 10.3389/fped.2025.1591828

Elkhatib, R. An Exploration of Cyber Predator Patterns in Grooming Children Using Social Media Applications. Doctoral dissertation, January 2025.

Thorn. LGBTQ+ Youth Perspectives: How LGBTQ+ Youth are Navigating Exploration and Risks of Sexual Exploitation Online. Published April 2024. Available at: https://www.thorn.org/research/library/lgbtq-teens-are-at-a-greater-risk-for-exploitation-online

Thorn. New Research from Thorn: LGBTQ+ Minors are 3X More Likely to Experience Unwanted and Risky Online Interactions. February 28, 2025. Available at: https://www.thorn.org/blog/new-research-from-thorn-lgbtq-minors-are-3x-more-likely-to-experience-unwanted-and-risky-online-interactions

The Trevor Project. Sexual Violence and Suicide Risk among LGBTQ+ Young People. October 2, 2025. Available at: https://www.thetrevorproject.org/research-briefs/sexual-violence-and-suicide-risk-among-lgbtq-young-people

National Child Traumatic Stress Network. Child Sex Trafficking: What You Might Not Know. Available at: https://www.nctsn.org/sites/default/files/resources/fact-sheet/child_sex_trafficking_what_you_might_not_know.pdf

Saprea. Protecting LGBTQ+ Youth from Sexual Abuse. November 25, 2024. Available at**: https://saprea.org/blog/sexual-abuse-lgbtq-community**

International Protection Alliance. How Online Grooming Fuels Child Sex Tourism: Analysis of global trafficking patterns. Published September 2025. Available at https://protectall.org

Our Rescue. How Online Grooming Impacts Child Exploitation: Field Operations data and analysis. Published October 2025. Available at https://ourrescue.org

Civil Litigation and Investigative Journalism

Multiple civil lawsuits. *In re: Roblox Corporation Child Sexual Exploitation and Assault Litigation,* MDL No. 3166, U.S. District Court for the Northern District of California. Consolidated December 2025. Case documentation available through PACER.

Multiple civil lawsuits. Discord child exploitation litigation, filed 2024-2025 in California, Texas, Florida, and federal courts.

Hindenburg Research. Roblox investigation report, October 2024. Referenced in civil litigation.

NBC News. Two families sue Meta over teens' deaths by suicide, citing 'sextortion' scams. December 17, 2025. Available at: https://www.nbcnews.com/tech/social-media/two-families-sue-meta-teens-deaths-suicide-citing-sextortion-scams-rcna248136

NBC News. Child exploitation watchdog says Meta encryption led to sharp decrease in tips and reports. May 9, 2025. Available at: https://www.nbcnews.com/tech/security/child-exploitation-watchdog-says-meta-encryption-led-sharp-decrease-ti-rcna205548

NBC News. 2 Nigerians sentenced to over 17 years in 'sextortion' case that led to Michigan teen's suicide. September 5, 2024. Available at: https://www.nbcnews.com/news/us-news/two-nigerians-sentenced-years-sextortion-case-led-michigan-teens-rcna169730

WTOC News. Reports of AI-generated child sexual abuse material have skyrocketed in just two years. October 2, 2025. Available at: https://www.wtoc.com/2025/10/02/reports-ai-generated-child-sexual-abuse-material-have-skyrocketed-just-two-years

CBS News. Kentucky attorney general sues Roblox alleging a "playground for predators." October 8, 2025. Available at: https://www.cbsnews.com/news/kentucky-attorney-general-russell-coleman-sues-roblox

WHAS11. Kentucky Attorney General Russell Coleman reflects on 2025. Available at: https://www.whas11.com/article/news/local/kentucky-ag-russell-coleman-reflects-2025-indictments-roblox-lawsuit-2026/417-471b116e-a6b4-4e91-96f6-b01d234973e0

WJHL. Tennessee attorney general files lawsuit against Roblox, citing child safety concerns. December 19, 2025. Available at: https://www.wjhl.com/news/regional/tennessee/tennessee-attorney-general-files-lawsuit-again-roblox-citing-child-safety-concerns

Bloomberg News. Reporting on Roblox federal investigation, February 2025.

Philadelphia Inquirer. 'Parents sue Roblox, saying it's a haven for sexual predators.' Published September 30, 2025.

Homeland Security Today. Surge in Online Crimes Against Children Driven by AI and Evolving Exploitation Tactics, NCMEC Reports. Available at: https://www.hstoday.us/subject-matter-areas/cybersecurity/surge-in-online-crimes-against-children-driven-by-ai-and-evolving-exploitation-tactics-ncmec-reports

NBC News, NBC Miami, SFGATE, New York Post. Various reporting on Roblox, Discord, and gaming platform exploitation cases, 2024-2025.

Channel 9 Eyewitness News. Investigative report: Predators using AI to generate explicit images of children on gaming platforms. Published 2025.

Fight the New Drug. NCMEC's 2025 Report: A Digital Red Flag for Child Safety. November 18, 2025. Available at: https://fightthenewdrug.org/a-digital-red-flag-ncmecs-2025-report

Platform Safety Documentation

National Center for Sexual Exploitation. Dirty Dozen List 2024: Platform accountability report including Discord analysis. Available at https://endsexualexploitation.org

Common Sense Media, ConnectSafely, Internet Keep Safe Coalition, NetSmartz. Platform safety guides and parental resources, 2024-2025.

Global Platform for Child Exploitation Policy. International policy tracking and platform reporting analysis. Available at https://globalchildexploitationpolicy.org

NCMEC. *CyberTipline Reporting Portal. Available at: https://report.cybertip.org*

NCMEC. *Take It Down Service. Available at: https://www.missingkids.org*

Report Prepared By

Sebastian T.

Publication Date: February 15, 2026

Report Version: 1.0

Classification: For Parental Awareness & Education

This report is provided for educational purposes. While every effort has been made to ensure accuracy, the threat landscape evolves continuously. Parents should seek updated information regularly and consult with law enforcement or child safety professionals for specific situations. This report does not constitute legal advice or professional counseling services.