



What Parents Need to Know Right Now

Apps change. The risky behaviors do not.

Social media can help kids connect, create, learn, and belong. It can also give predators, scammers, bullies, and violent online groups direct access to children. This guide focuses on the app functions and warning signs parents should understand - especially on platforms that appear repeatedly in current federal child-exploitation investigations.

IMPORTANT: THIS IS NOT A 'BAD APP' RANKING

ICAC specifically cautions parents not to focus only on which apps are 'bad.' Any platform that allows messaging, sharing, live interaction, or contact with strangers can be abused. The apps in this guide are highlighted because their features - and recent federal cases - illustrate risks parents are seeing right now.

THE SCALE OF THE PROBLEM

1.4M

CyberTipline reports concerning online enticement in 2025.

NCMEC, 2025 data

80,000+

2025 online enticement reports concerning sextortion.

NCMEC, 2025 data

3,000+

reports of sadistic online exploitation in 2025.

NCMEC, 2025 data

WHAT MATTERS MOST

Know who can contact your child, what strangers can see, whether location is shared, whether messages disappear, what groups or servers they join, and whether conversations are moving to a more private platform.



THE FEATURES THAT CREATE THE MOST RISK

FOCUS ON FUNCTIONS, NOT LOGOS

The same danger can move from one app to another in minutes.

DIRECT MESSAGES FROM STRANGERS

Private messaging gives an offender a one-to-one channel to flatter, groom, threaten, manipulate, or move a child into sexual conversation.

DISAPPEARING OR SELF-DELETING CONTENT

Temporary messages can create a false sense of safety. The FBI warns that nothing online should be assumed to truly disappear; content can be copied, screen-recorded, or captured with another device.

PUBLIC PROFILES & FOLLOWER LISTS

A public profile may reveal school, sports, family, friends, location clues, and the exact people an extortionist can threaten to contact.

LIVE VIDEO, VOICE & VIDEO CALLS

Live communication can escalate grooming quickly and may be used to pressure a child into sexual conduct, self-harm, or humiliating acts.

GROUPS, SERVERS, CHANNELS & COMMUNITIES

Large communities can expose children to unknown adults, extremist or violent content, sexual material, and private invitations outside the public group.

LOCATION SHARING

Location tools, geotagged posts, school/team references, and photos can help someone identify where a child lives, studies, practices, or spends time.

GIFTS, GAME CURRENCY & PAYMENTS

NCMEC and FBI materials describe offenders using money, gift cards, game credits, devices, or other incentives to lower a child's guard or obtain sexual content.

MOVING TO A DIFFERENT APP

The FBI specifically warns about strangers who meet a child on one platform and quickly ask to continue on a different, more private app.



SNAPCHAT & INSTAGRAM

TWO PLATFORMS PARENTS SHOULD UNDERSTAND

Recent federal prosecutions have involved offenders using Snapchat and Instagram to impersonate teens, groom minors, solicit explicit material, and threaten victims.

SNAPCHAT

Snapchat's private chats, disappearing-style communication, friend discovery, group chats, Stories, public profiles, and Snap Map can make it easy for teens to communicate quickly and privately. Recent DOJ cases describe offenders using Snapchat to groom and exploit minors, sometimes alongside Instagram or TikTok.

PARENT CHECK:

Turn on Family Center. Review recent contacts and new friends, location-sharing and Snap Map settings, public profile status, sensitive-content controls, and whether your child is communicating with anyone they do not know in real life.

INSTAGRAM

Instagram combines public or private profiles, follower lists, Stories, DMs, message requests, Reels, and easy cross-contact with strangers. For sextortion, a visible followers list can also give an offender leverage by showing exactly who to threaten with exposure. Federal cases continue to document Instagram being used in grooming and exploitation.

PARENT CHECK:

Keep the account private. Review followers/following, unknown message requests, linked accounts, public bio details, school/team/location clues, Story audience, and any person who quickly asks to move the conversation elsewhere.

RECENT FEDERAL CASE EXAMPLES

In May 2026, DOJ described a defendant who impersonated a teenage girl on Snapchat and Instagram and coerced at least seven minor girls into producing sexual content. Other 2026 federal cases describe Snapchat, Instagram, and TikTok being used in long-running sextortion and child-exploitation schemes.



TIKTOK & DISCORD

DIFFERENT PLATFORMS - DIFFERENT RISKS

TikTok is built around discovery and public content; Discord is built around communities, servers, direct messages, voice and video.

TIKTOK

TikTok's recommendation feed can expose teens to strangers and public audiences quickly. Depending on age and settings, features can include public posting, comments, downloads, search, DMs, Lives, Duet/Stitch, and follower visibility. Federal cases have documented offenders using TikTok with other apps to groom and coerce minors.

PARENT CHECK:

Use Family Pairing. Confirm the account is private when appropriate, review DMs and comment permissions, downloads, followers, search/discoverability, Lives, who can interact with posts, and whether your teen is moving conversations off TikTok.

DISCORD

Discord can include private DMs, group DMs, public or private servers, voice channels, video calls, invite links, and communities centered on games or interests. FBI and NCMEC warnings about violent online networks describe offenders finding and grooming children through messaging, social media, Discord, Roblox and gaming spaces.

PARENT CHECK:

Use Discord Family Center. Review new friends, users messaged or called, servers joined, server names and member counts, DM permissions, friend-request settings, sensitive-content filters, and any server that pressures secrecy or off-platform contact.

WHY DISCORD DESERVES EXTRA ATTENTION

The FBI is investigating violent online networks commonly referred to as '764' and related groups. These networks target children on publicly available social media, messaging, and gaming platforms, then use manipulation, blackmail, sexual exploitation, self-harm demands, doxxing, or swatting to control victims. NCMEC specifically identifies Discord, Roblox and gaming sites in this threat pattern.



ROBLOX, GAMING & TELEGRAM

GAMING IS SOCIAL MEDIA TOO

If a platform lets users talk, friend one another, trade, gift, voice chat, or move off-platform, it deserves the same supervision as a social app.

ROBLOX & ONLINE GAMING

Roblox and other online games can include text chat, voice chat, friends, private/direct chat, parties, game communities, gifts, virtual currency, and links to outside platforms. NCMEC warns that online enticement occurs in gaming environments and can involve sexual conversation, requests for images, gifts, or attempts to meet.

PARENT CHECK:

Link a parent account and review communication controls, friends/connections, chat permissions, voice access, content maturity, spending, screen time, and whether anyone is asking your child to leave Roblox for Discord, Snapchat, Telegram, or another app.

TELEGRAM & PRIVATE MESSAGING

Telegram supports private messaging, groups, channels, file sharing, usernames, and optional Secret Chats with end-to-end encryption and self-destruct timers. Federal child-exploitation investigations have included Telegram alongside Discord, Snapchat, Instagram and Roblox.

PARENT CHECK:

Review contacts, groups, channels, usernames, privacy settings, unfamiliar invite links, downloaded files, and whether Secret Chats are being used. Do not assume a missing chat history means no conversation occurred.

THE 'MOVE OFF-PLATFORM' RULE

If someone your child only knows through a game, server, or social app asks them to switch to a more private chat, treat that as a reason to slow down and verify who the person is. The FBI specifically identifies this platform-switching behavior as a warning sign.



STRANGER-DISCOVERY & LESSER-KNOWN APPS

DO NOT IGNORE APPS YOU HAVE NEVER HEARD OF

Some platforms are built primarily around meeting new people, quick chats, anonymous discovery, or private messaging. These functions can create higher exposure to strangers.

YUBO, PURP & SIMILAR 'MEET NEW PEOPLE' APPS

A 2025 federal child-exploitation case described an offender using Instagram, Snapchat, Discord, Yubo, Purp and other apps to coerce and threaten at least 68 minors. The key risk is not the brand name - it is the app's ability to introduce a child to unknown people quickly.

WIZZ & FAST-MATCHING SOCIAL APPS

NCMEC's 2025 CyberTipline data specifically identified Wizz App among companies whose reports often lacked enough jurisdictional information for referral. For parents, any app centered on discovering or chatting with strangers deserves heightened scrutiny.

KIK & PRIVATE MESSAGING

Recent DOJ cases continue to involve Kik and other private-messaging services in child sexual abuse material investigations. Private chat, usernames, groups, and file sharing can be used by both legitimate users and offenders.

THE APP YOU DO NOT RECOGNIZE

Do not assume an unfamiliar app is harmless because it looks like a utility, game, calculator, photo tool, or chat app. Search the app name, review its age rating, read what communication features it has, and ask your child to show you how they use it.

A SIMPLE DECISION RULE

- ☐ Can strangers find or message my child?
- ☐ Can messages, photos, or video disappear?
- ☐ Can users join large groups, servers, channels, or live rooms?
- ☐ Can the app show location or reveal school/team/friend information?
- ☐ Can users send money, gifts, game currency, files, or links?
- ☐ Can my child easily move the conversation to a different platform?



WARNING SIGNS & WHAT PARENTS SHOULD REVIEW

CHANGES IN BEHAVIOR OFTEN MATTER MORE THAN THE APP ICON

One sign alone may mean nothing. A cluster of secrecy, panic, money requests, new contacts, or account changes deserves a calm conversation.

SUDDEN PANIC AFTER A MESSAGE

Your child becomes terrified, ashamed, or desperate after receiving a DM, photo, video, or threat.

NEW ONLINE FRIENDS YOU CANNOT IDENTIFY

Especially when the person seems older, highly flattering, romantic, secretive, or unusually generous.

MOVING BETWEEN APPS

A new contact quickly asks to switch from a game or public platform to a private chat.

MONEY OR GIFT-CARD REQUESTS

Your child suddenly needs Cash App, Apple Pay, gift cards, crypto, game currency, or money they cannot explain.

MULTIPLE OR SECRET ACCOUNTS

New usernames, alternate profiles, extra email addresses, accounts with false ages, or profiles parents were never told about.

DELETING & REINSTALLING APPS

The child removes an app before a phone check or bedtime and redownloads it later.

LATE-NIGHT USE & EXTREME SECRECY

Sleeping with the phone, moving devices into bathrooms/bedrooms, hiding screens, or becoming distressed when access is limited.

SELF-HARM, VIOLENCE OR EXTREME CONTENT

FBI warnings about violent online networks include coercion into self-harm, animal cruelty, sexual acts, doxxing, swatting, and suicide-related content.



THE PARENT ACTION PLAN

REVIEW THESE SETTINGS TOGETHER

The FBI recommends open, ongoing conversations and knowing the platforms, usernames, passwords, privacy settings, and people your child interacts with online.

1

Set accounts to private whenever possible and remove unknown followers/friends.

Review profile photos, bios, school/team names, birthdate, location clues, and public follower/following lists.

2

Turn off unnecessary location sharing.

Review Snap Map, app-level location permissions, photo geotags, check-ins, and live-location features.

3

Review who can message, call, comment, add, or invite your child.

Pay special attention to message requests, server DMs, group invites, friend discovery, and stranger contact.

4

Use the platform's parent tools.

Snapchat Family Center, TikTok Family Pairing, Discord Family Center, Roblox parental controls, and device-level Screen Time/Family Link can improve visibility - but none replaces conversation.

5

Do not allow children to lie about their age to unlock features.

The FBI advises children not to cheat age verification. Age-based protections only work when the account has the correct birthdate.

6

Create a 'come to me first' rule.

Tell your child clearly: If someone threatens you, asks for sexual content, pressures you to move apps, demands money, or tells you to keep a secret, come to me. I will help first.

IF SOMETHING HAS ALREADY HAPPENED

Preserve evidence. Do not pay, bargain, or send more content. Do not forward explicit images of a minor. Block the offender after evidence is saved, report the account to the platform, and contact local law enforcement, the FBI, or NCMEC's CyberTipline. For nude or sexually explicit images taken when the person was under 18, NCMEC's Take It Down service may help limit online spread.

REPORTING & HELP

NCMEC CyberTipline: report.cybertip.org | FBI: tips.fbi.gov / 1-800-CALL-FBI

Take It Down: takeitdown.ncmec.org | Immediate danger: 911 | Crisis support: call/text 988

**MORE FREE PARENT
SAFETY RESOURCES**

OfficerNaeNae.com





OFFICIAL SOURCES & CURRENT CASE EXAMPLES

PRIMARY SAFETY GUIDANCE

This guide relies primarily on NCMEC, FBI, ICAC/OJJDP and U.S. Department of Justice materials.

NCMEC CyberTipline Data

[Open official source](#)

FBI - Violent Online Networks Warning

[Open official source](#)

NCMEC Online Enticement

[Open official source](#)

ICAC Task Force Program

[Open official source](#)

NCMEC Gaming Safety

[Open official source](#)

ICAC - Apps: Focus on Functions

[Open official source](#)

NCMEC - Violent Online Groups / 764

[Open official source](#)

ICAC OCEPI Prevention Resources

[Open official source](#)

FBI - Keeping Kids Safe Online

[Open official source](#)

DOJ Project Safe Childhood

[Open official source](#)

FBI - Sextortion

[Open official source](#)

NCMEC Take It Down

[Open official source](#)

RECENT FEDERAL CASE EXAMPLES USED TO ILLUSTRATE PLATFORM RISK

These cases show how offenders have used specific platforms; they do not mean a platform itself is inherently criminal or unsafe.

DOJ - Snapchat & Instagram impersonation/exploitation (May 21, 2026)

[Open official source](#)

DOJ - Instagram, Snapchat, Discord, Yubo & Purp; 68 minor victims (Sept. 4, 2025)

[Open official source](#)

FBI victim notice - Roblox, Discord, Telegram, Snapchat & Instagram (2026)

[Open official source](#)

DOJ - Snapchat, Instagram & TikTok sextortion case (Jan. 23, 2026)

[Open official source](#)

Updated September 2026. Platform settings and safety tools can change after publication.