Southwest Missouri Cyber Crimes Task Force
303 E 3rd Street, Joplin, Missouri 64801-2274
Tel: (417) 623-3131 x1459
Fax: (417) 624-2820

Current Trends in Online Child Exploitation & Offender Tactics

Prepared for Southwest Missouri Regional Sex Offender Officer Meeting – October 15, 2025

Purpose

To provide law enforcement and probation officers with up-to-date insights on how offenders are exploiting technology to target minors. Includes current trends, behavioral indicators, and practical takeaways for investigations and field contacts.

Recent Trends

- Sextortion Surge: Offenders posing as teens on Snapchat, Instagram, or Discord. Rapid threats to expose images for payment — primarily targeting boys aged 13–17.
- AI-Generated Nudes & Deepfakes: Use of diffusion models and free bots to fabricate explicit content of real victims, often classmates or peers.
- Grooming Through Gaming & Livestreams: Offenders exploiting interactive spaces (Roblox, Fortnite, TikTok Live) to build trust via gifts, in-game items, or compliments.
- Encrypted Platforms & File-Sharing: Kik, Telegram, and decentralized storage (Mega.nz, IPFS) used to exchange or store CSAM collections.

How Offenders Reach Victims

- Social engineering tactics: flattery, sympathy, fear, or curiosity.
- Creating multiple fake profiles and migrating conversations off-platform.
- Late-night or secretive communication patterns.
- Language cues: 'Don’t tell anyone,' 'Trust me,' 'You’re mature for your age.'

Officer Awareness Indicators

- Repeated phone/SIM changes or multiple devices in use.
- Hidden or renamed apps ('Calculator+', 'Vault').
- Dual accounts on platforms; unfamiliar online contacts.
- Anxiety or secrecy surrounding phone checks.

Forensic & Investigative Takeaways

- Preserve volatile evidence (chats, cache, cloud data) early. Contact SMCCTF
- Common artifact sources: Discord logs, Mega sync folders, hidden album storage.
- Increased need for AI-image detection and metadata correlation.
- Close collaboration between line officers and forensics accelerates case timelines.

Key Resources

- CyberTipline – streamlined reporting and triage workflow.
- FBI & ICAC training and resource portals.
- Search.org ISP/ESP contact database for subpoenas.

Quick Takeaways

- Offender tactics evolve monthly — don't assume old patterns.
- Every internet-connected device is a potential contact point.
- Ask victims how contact started, not just what was said.
- Swift referrals and evidence preservation save lives.

Top 10 Questions to Ask During Field Contacts

When speaking with registered offenders, suspects, or persons of concern:

1. **What social media or messaging apps do you use most often?**

   → Look for evasive answers or new/unfamiliar app names (Discord, Kik, Telegram, Whisper, etc.).

2. **Do you communicate with anyone you met online?**

   → Gauge whether they distinguish between online and real-world relationships.

3. **Do you ever chat with minors or people you only know from gaming or social media?**

   → Watch for rationalizations ('They messaged me first,' 'It's just a game').

4. **Do you use any alternate or backup accounts?**

   → Many offenders maintain multiple identities to evade supervision.

5. **Do you have any hidden or encrypted apps on your phone or tablet?**

   → Note use of vault apps or renamed icons ('Calculator+', 'KeepSafe').

6. **What devices do you currently have access to?**

   → Include game consoles, smart TVs, or secondary phones.

7. **Where do you store your photos and videos?**

   → Cloud services (Google Drive, Dropbox, Mega) are common hiding spots.

8. **Do you use a VPN, Tor, or privacy browser?**

   → May indicate deliberate effort to conceal activity.

9. **Who else uses your devices or shares your Wi-Fi?**

   → Helps identify shared environments and potential secondary users.

10. **Have you ever been contacted by someone asking for or sending sexual content online?**

    → Opens the door to disclosures from either suspects or victims.

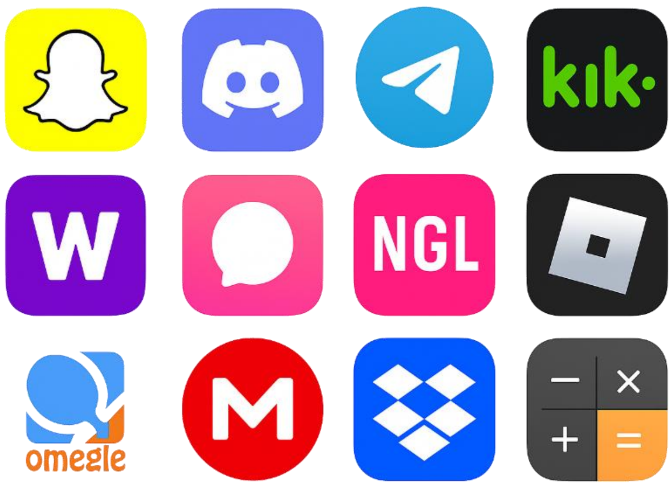
Tips for Officers

- Ask conversationally — not as a checklist.
- Document exact app names, usernames, or handles.
- Note inconsistencies between verbal answers and device contents.
- Trust your instincts when tech explanations sound rehearsed or vague.

Apps Commonly Associated with Exploitation or Concealment

- Snapchat – primary contact tool for sextortion and hidden communications.
- Kik – persistent offender platform; allows anonymous accounts.
- Telegram – encrypted messaging and group file sharing.
- Discord – heavy offender presence; used for grooming, file sharing, and community access.
- Whisper / Yubo / Wink – 'meet new friends' apps popular among minors and offenders.
- Omegle alternatives – random video chat sites used for exposure and coercion.
- Tellonym / NGL / Ask.fm – anonymous Q&A apps used to initiate contact.
- Grindr / Tinder / MeetMe – used by offenders posing as teens or seeking minors.
- Calculator+ / Keepsafe / Vault – hidden photo/video storage disguised as utilities.
- Mega.nz / Dropbox / Google Drive – common for CSAM or extortion content storage.
- Badoo / Wizz / Hoop – lesser-known social discovery apps linked to grooming behavior.
- Anywhere kids are!

⚠️ Officers should document app names, note icons on devices, and preserve screenshots or manifests before deletion.



Appendix: Investigative Tools & Resources

Open Source Intelligence (OSINT)

- WhatsMyName – Search for usernames across hundreds of platforms. (https://whatsmyname.app/)
- HaveIBeenPwned – Check if email addresses or usernames appear in known data breaches. (https://haveibeenpwned.com/)
- IntelTechniques Tools – OSINT utilities for usernames, phones, and domains. (https://inteltechniques.com/tools/)
- Social Searcher – Monitor public social mentions and profiles. (https://www.social-searcher.com/)
- Username Search – Alternate username lookup and social mapping tool. (https://usersearch.org/)
- ExifTool / Jeffrey's Image Metadata Viewer – Examine photo metadata to identify device or location data. (https://exiftool.org/)

Network & IP Investigation

- Whois.domaintools.com – Domain registration and IP ownership lookups. (https://whois.domaintools.com/)
- ViewDNS.info – Multi-tool for IP geolocation, reverse lookups, and DNS history. (https://viewdns.info/)
- Censys / Shodan – Identify exposed devices or infrastructure linked to offenders. (https://search.censys.io/ / https://www.shodan.io/)
- WiGLE.net – Wireless access point mapping for correlating Wi-Fi networks to physical locations. (https://wigle.net/)

Image & Video Intelligence

- Google Reverse Image Search / TinEye – Detect reuse of victim or suspect imagery. (https://images.google.com/ / https://tineye.com/)
- FotoForensics – Analyze image manipulation or compression artifacts. (https://fotoforensics.com/)
- InVID Verification Plugin – Browser add-on for verifying online videos. (https://www.invid-project.eu/tools-and-services/invid-verification-plugin/)

Dark Web / Encryption Awareness

- Ahmia – Search engine for Tor hidden services (for investigators). (https://ahmia.fi/)
- Tor Metrics – Monitor Tor usage and patterns. (https://metrics.torproject.org/)
- PGP Tools – Decrypt or verify PGP-signed communications when lawful authority is granted.

Law Enforcement / Specialized

- ICAC Task Force Portal – Training, deconfliction, and resource sharing.
- NCMEC CyberTipline – Centralized reporting for CSAM and sextortion.
- Search.org ESP/ISP Contact List – Subpoena and data request reference for providers.
- Legal Reference – 18 U.S.C. § 2703, RSMo 542.271, and Stored Communications Act summaries.