CURRENT TRENDS IN ONLINE CHILD EXPLOITATION & OFFENDER TACTICS

Prepared for Southwest Region P&P Meeting

October 15, 2025

DET. CHRIS CORBETT

- 14 years of law enforcement experience
- 20+ years of information technology experience
- Internet Crimes Against Children (ICAC) TFO
- Southwest Missouri Cyber Crimes TFO
- Homeland Security Investigations (HSI) TFO

PURPOSE

Provide law enforcement and probation officers with the latest information on how offenders exploit technology.

Highlight current trends, behavioral indicators, and field-level investigative takeaways.

RECENT TRENDS

- Sextortion Surge – Offenders posing as teens, demanding money or images from victims.
- AI-Generated Nudes & Deepfakes – Synthetic CSAM using real faces from social media.
- Grooming Through Gaming & Livestreams – Building trust via games, chats, and gifts.
- Encrypted File-Sharing – Kik, Telegram, and decentralized platforms like Mega.nz or IPFS.

HOW OFFENDERS REACH VICTIMS

- Social engineering: flattery, sympathy, curiosity, or fear.
- Multiple fake profiles and migration off mainstream platforms.
- Late-night chat patterns and secretive communications.
- Language cues: 'Don’t tell anyone,' 'You’re mature,' 'Trust me.'

OFFICER AWARENESS INDICATORS

- Repeated phone/SIM swaps or multiple active devices.
- Hidden or renamed apps ('Calculator+', 'Vault').
- Dual accounts or secret social media profiles.
- Anxiety or secrecy during device inspections.

FORENSIC & INVESTIGATIVE TAKEAWAYS

- Preserve volatile evidence (chat logs, caches, cloud content) early. Contact SMCCTF
- Artifacts often found in Discord logs, Mega folders, or hidden albums.
- Growing need for AI-image and metadata analysis.
- Close collaboration between patrol, detectives, and forensics shortens case timelines.

KEY RESOURCES

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

QUICK TAKEAWAYS

- Offender tactics evolve monthly — stay updated.
- Every connected device is a potential contact point.
- Ask offenders how contact started, not just what was said.
- Early referrals and evidence preservation save lives.

1. What social media or messaging apps do you use most often?
2. Do you communicate with anyone you met online?
3. Do you chat with minors or people you only know from gaming or social media?
4. Do you use any alternate or backup accounts?
5. Do you have any hidden or encrypted apps?
6. What devices do you have access to?
7. Where do you store your photos and videos?
8. Do you use a VPN, Tor, or privacy browser?
9. Who else uses your devices or Wi-Fi?
10. Have you ever been contacted about sexual content online?

TOP 10 QUESTIONS TO ASK DURING FIELD CONTACTS

VERIFY INFO AGAINST SO REGISTRATION

TIPS FOR PO'S

1. Ask conversationally — not like an interrogation checklist.
2. Document app names, usernames, or handles verbatim.
3. Compare statements to actual device contents.
4. Trust your instincts when tech explanations sound rehearsed or evasive.

APPS COMMONLY ASSOCIATED WITH EXPLOITATION OR CONCEALMENT

Snapchat – frequent use in sextortion and hidden chats.

Kik, Telegram, Discord – encrypted and anonymous communication hubs.

Whisper, Yubo, Wink – social discovery apps for teens and predators alike.

Omegle-style random video chats – now mirrored by clone sites.

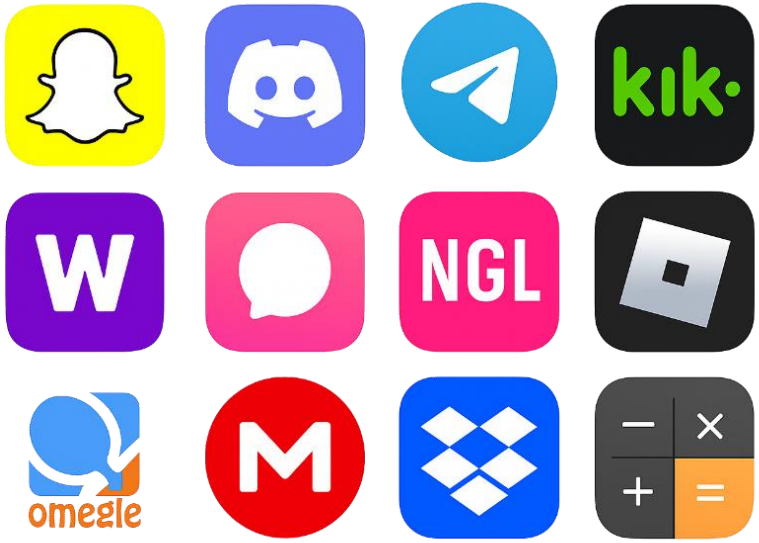
Tellonym, NGL, Ask.fm – anonymous messaging portals.

Calculator+, Vault, Keepsafe – disguised storage apps.

Mega.nz, Dropbox, Google Drive – remote storage for illicit files.

Grindr, Tinder, MeetMe – used for misrepresentation and grooming.

APPS COMMONLY ASSOCIATED WITH EXPLOITATION OR CONCEALMENT



STAY VIGILANT, STAY INFORMED

- Technology evolves — so do offenders.
- Field awareness and prompt evidence handling remain our best defense.

CONTACT AND RESOURCES

Contact Det. Corbett

P&P Resources