Understanding Online Exploitation of Minors

(Disclosure: I created this document with the help of Google Gemini. To verify the data, I tracked down authentic sources for each reference or citation mentioned by Gemini. I have inserted those authentic sources as links so that you can read more about the specifics mentioned throughout the document.)

Will Daddario, PhD, LCAS, LCMHC | Will Daddario Counseling and Consulting PLLC | 704-800-4325

"Long-form grooming" and **"social engineering"** are documented exploitation tactics used by sophisticated online predators whose goal is to create a deep, immersive sense of reality and safety for the kids they prey upon. In the spirit of "knowledge = power," I present the following information.

The Current Scope of the Problem

The FBI, the Department of Homeland Security (DHS), and child safety organizations all study tactics used by exploitative groups who target children and adolescents online. As you read about the tactics, note the way that advanced technology can weaponize the malicious intent of the predator. Bottom line: vast networks of criminals seek to exploit minors online, and they have developed techniques for doing this.

1. The "Peer Proxy" (Teenagers used as Fronts)

There are numerous cases where a predator recruits a real teenager (often a previous victim) to act as the "face" of the operation. (For example)

- In these scenarios, the person on FaceTime or TikTok or Instagram is a real teen, which bypasses all "stranger danger" alarms. However, the adult predator is the one managing the group chat, reading the messages, and directing the teen on what to say.
- **Source:** The FBI and Child Rescue Coalition have published accounts (such as "Amelia's Story") where victims were certain they were talking to a child because they saw them on screen, only to find an adult was orchestrating the entire interaction from behind the scenes.
    - From "Amelia's Story": "Amelia [9 years old] looked at me and said, 'No, no mummy, it was another child I was talking to. She said we'd both go to jail if I said anything to anyone, and every weekend, I've been scared that the police would find out and arrest me and take me away from you. I was so worried because you always told us not to play with people we didn't know.'"

2. Live Deepfake Grooming

It is a common misconception that video calls are un-fakeable. Technology now allows for real-time digital "masks."

- The Digital Resistance organization and Ampyx Cyber have documented "Live Deepfake" scams where predators use two phones and an app to overlay a teenager's face onto their own during a live call.
- **Proof Point:** There are videos where technology buffs show off how somebody could pose as young woman or teen in live video chats, with the digital face matching their mouth movements and expressions perfectly.
  - Video showing how deep-fake masks work
  - Open-Source: The technology is available for anyone to use

3. The "Social Proof" Group Tactic

Predators often create "artificial social circles" to make a lie seem like a lifestyle.

- By creating multiple fake accounts (or using multiple "mules"), a predator builds a group that chats, jokes, and hangs out together for months or years. This makes the victim feel that if they leave or doubt the primary contact, they are losing an entire community.
- **Source:** DHS (Know2Protect) reports that predators often "nest" within fake online communities or gaming groups to normalize sexual or manipulative conversations over long periods. Such gaming groups can be found on Roblox, Discord Channels, or really any system that utilizes simultaneous online interaction.

4. The "International Distance" Bluff

Living "overseas" is a specific tactic used to avoid the parent meeting without looking suspicious. If someone tells your child that they live in Europe, for example, they could be anywhere in the world, even close to your home location.

- International distance can be a safety net for predators. It allows them to make grand promises (like meeting the mom) because they know the logistical hurdles make it unlikely to actually happen. If the meeting ever gets close to reality, they often use a strategic crisis to cancel.

Where to Find Official Reports

- **FBI News:** Search for "The Financially Motivated Sextortion Threat" (covers long-term social engineering).
- **DHS Know2Protect:** Info sheet about Online Grooming Tactics.
- **National Center for Missing & Exploited Children (NCMEC):** They have extensive PDFs (like this one) that detail how predators use "peer" identities and long-term trust-building.

Motive: Why Do People Do This?

The goal of long-term grooming is rarely a single, simple objective. Instead, it is usually a gradual erosion of boundaries designed to achieve one or more of the following outcomes.

1. Sexual Exploitation (The "Slow Play")

This is the most common goal. By spending a year building a "friendship" or "romance," the predator moves from the stranger"category to the trusted inner circle category.

- **The Goal:** Once the victim feels completely safe and indebted to this friend who has been there for a year, the predator begins asking for increasingly explicit photos, videos, or live webcam performances.
- **The Leverage:** They often use the group chat dynamic to normalize this behavior (e.g., "we all show each other stuff, it's just what friends do").

2. Extortion and "Sextortion"

In many cases, the goal is financial or psychological control.

- **The Goal:** Once the victim has shared private information, secrets, or compromising photos, the predator flips the script. They threaten to send the material to the victim's parents, school, or the "group" unless the victim pays money or does more "favors."
- It takes a long time to gather enough "collateral" to make the threat feel inescapable. For this reason, predators are willing to invest a year or more in building a relationship.

3. Radicalization or "Cult-Like" Recruitment

Sometimes the goal isn't sexual or financial, but ideological.

- **The Goal:** To isolate the victim from their "real world" support systems (parents, local friends) and replace them with the online family.
- **The Outcome:** The predator can then influence the victim's political beliefs, encourage self-harm, or recruit them into fringe groups. A year of group hangouts, for example, is the perfect amount of time to perform the necessary brainwashing to make the victim trust the group more than their own family.

4. Identity Theft and "Mule" Recruitment

If the predator is part of an organized crime ring, the goal might be more functional.

- **The Goal:** To turn the victim into a "mule" for illegal activities. This could mean using the victim's bank account to move money, using their address to receive packages, or using their social media profile to lure other victims.
- **Why the Child or Teen Proxy?** Using a real teen on FaceTime makes the operation feel legitimate, which is essential if they want the victim to perform real-world tasks.

5. Psychological Dominance (The "God Complex")

For some predators, the goal is purely the thrill of the lie.

- **The Goal:** Some individuals derive a sense of power from successfully manipulating a target and their family for a long period. They enjoy knowing they have fooled a parent and successfully integrated into a stranger's life.
- **The Outcome:** They may never even ask for money or photos; they just want to see how far they can push the deception before it breaks.

Predators view long cons as research and development. Every FaceTime, every group chat, and every "offer to meet the mom" could be a data point they use to map out the victim's psychological weaknesses. By the time they make their move, they want the victim to feel that the predator is the only person who truly understands them.

Deep Dive Into Long-Cons

While it may seem like an exhausting amount of effort for one person to commit to building a nearly 24/7 relationship with a minor for a year or more, there are several reasons why this occurs and techniques that

predators deploy:

1. The Use of "Decoys" or Accomplices

In many cases, the predator is not acting alone, or they have manipulated other victims into participating in these calls. By having multiple people on a video chat, the predator creates social proof. If you see five people chatting and laughing, your brain naturally lowers its defenses because it assumes they can't all be in on it. But this possibility means that whenever you suspect your own child is caught in a trap, there is likely one or more other minors being exploited elsewhere through the same scam.

2. Technical Manipulation

More and more tech tools maintain the illusion during video hangouts:

- **Looping Video/Deepfakes:** They may use pre-recorded footage of someone else and feed it into the video chat software.
- **Voice Changers:** Real-time AI voice modulation has become highly effective at altering pitch and tone. Adults sound convincingly like kids.

3. The "Slow Play" Strategy

What time investment accomplishes:

- **Isolation:** By becoming the victim's primary social group, the predator slowly cuts their target off from real-world friends and family.
- **Information Gathering:** Over a year, they can learn every detail of a person's life—their fears, their location, and their schedule.
- **Normalization:** After a year, the victim no longer questions the predator's presence; they become a "best friend" or "found family," making future requests for money, explicit content, or physical meetings much harder to refuse.

Once a parent or an adult helper has a suspicion, here's what to look for:

Even with technology and time to invest in exploitation projects, certain inconsistencies usually remain:

- **The "No-Show" at Scale:** No one in the group ever meets in person, despite living relatively near each other or having the means to travel.
- **Deflection:** Whenever you ask to verify an identity or do a specific task on camera (like "hold up three fingers"), they experience "lag" or get offended that you don't trust them.
- **Shared Drama:** The group frequently experiences high-intensity crises that require your emotional (or financial) support, bonded by a "us against the world" mentality.

Calling The Bluff

The "Mechanical Verification" Method.

A real person can respond to questions and commands instantly; a deepfake or a person using a pre-recorded loop cannot. It is NEVER recommended to try these techniques yourself. Instead, as soon as you suspect something inappropriate is happening, call the authorities and cut-off all contact right away. In the interest of showing shortcomings of predators' schemes, however, I present the following information about how to prove somebody you see online is real or a fake.

1. **The "Random Physical Action" Test:** During a live FaceTime, ask them to do something random and specific that isn't part of a normal conversation. *"Hey, can you grab a fork from your kitchen and hold it up to your left eye?"* or *"Can you turn around in a full circle while waving?"* Deepfakes often "break" or glitch when the person moves rapidly or introduces objects near their face.
2. **The "Specific Background" Request:** Ask them to walk to a window and show you the street or a specific room in their house that you haven't seen.
3. **The Mom's Meeting (The Actual Test):** Tell them, *"My mom is actually going to be in your area for work next month and would love to take you and your parents to lunch."* Watch their reaction. A real person would be excited or ask for details; a predator will immediately begin "de-escalating" or creating reasons why that specific time won't work.

Related Tactics (if you're interested)

1. More Mechanical Stress Tests

- **The "Face-Block" Test:** Ask them to wave their hand slowly directly in front of their face, or to "pinch" their nose. A digital filter will often "glitch," flickered, or momentarily reveal the real face behind the mask when an object passes between the camera and the face.
- **The "Sideways" Test:** Ask them to turn their head 90 degrees to the side so you see their profile. Deepfakes often struggle to maintain the 3D map of a face at sharp angles, leading to "floating" features or blurred ears.
- **The "Lighting" Test:** Ask them to turn off their main light or move to a different room. Deepfakes often have "baked-in" lighting that won't match a sudden change in the physical environment.

2. The "Real-Time Interaction" Test (Anti-Loop/Recording)

If they are using pre-recorded footage of a real person (a "loop"), they cannot react to spontaneous, unscripted requests.

- **The Finger Count:** Tell them, "Hold up four fingers, then tuck one away." This requires immediate cognitive and physical coordination that a recording cannot replicate.
- **The "Read This" Test:** Send a random, nonsensical word in the chat (e.g., "Banano-Graph") and ask them to read it out loud immediately.
- **The Mirror Test:** Ask them to hold a mirror up to the camera or walk to a mirror in their house. Seeing the "behind-the-scenes" of their room usually breaks a digital set or a pre-recorded loop.

3. The "Overseas Reality" Check

If a predator claims to be in England, for example, they should have immediate, effortless knowledge of their surroundings that a VPN or Google search can't easily fake.

- **The "Window" Verification:** If it is 8:30 PM in North Carolina, it is 1:30 AM in London. Ask them to walk to the window and show you the dark street. If it’s broad daylight or the weather doesn't match the current UK forecast, the lie is revealed.
- **The "Coin" Test:** Ask them to show you the change in their pocket. A real person in England will have Pounds and Pence. Ask them to show a specific coin (like a 50p piece) close to the camera.
- **The "Mundane" Detail:** Ask them what they had for lunch from a specific UK grocery store (like "Tesco" or "Sainsbury’s"). Follow up with a question about a store-brand item. Liars usually have a script for big things, but they fail on the mundane details of daily life.

4. Calling the "Parent" Bluff

If the predator has offered to meet the mom, force the escalation. BUT: DO NOT INTRODUCE ANOTHER PERSON INTO THE CHAT. You don't want to give more data to whoever may be operating the scam.

- **The "Three-Way" Video Call:** Tell them your mom wants to talk *right now* for 5 minutes. If they suddenly have a "bad connection," "need to ask their parents first," or get angry, the offer was a bluff.
- **The "Official" Meeting:** Propose a specific, public video meeting with *their* parents. Say, "My mom wants to talk to your mom to coordinate the visit." A predator will almost always use "strict parents" or "busy schedules" to block adult-to-adult contact.

5. Digital Footprint Audit

- **The "Liveness" of Social Media:** Does the suspect have a long history of tagged photos from other people (friends, schoolmates, family) at identifiable UK locations? A predator's profile is usually a "walled garden" where they are the only ones posting content.
- **Reverse Image Search:** Take a screenshot during a FaceTime and use Google Lens or something similar. You might find that the "teen" is actually a minor social media influencer from a different country whose content has been stolen.

What Parents and Adult Helpers Can Do

1. **Acknowledge the problem:** these are not random occurrences anymore. The FBI and other International organizations track extensive rings of human traffickers who use online deception to prey on potential victims.
2. **Trust your intuition:** If you suspect something is wrong based on, for example, the excessive amount of time your child spends online, do not avoid confronting the child. Have the difficult conversation. Introduce the notion of therapy if the child doesn't want to talk about emotions to you. Most importantly, trust your gut.
3. **Learn from your child:** How much do you know about how online gaming works? Ask your child to show you what their online world is all about. Ask questions about how it's possible to communication with other people online. Ask your child how they met certain friends and whether or not they know they are real.
4. **Talk to your kids about authenticity vs. virtual reality:** The online webscape is a part of your kid's identity and reality. It has existed as long as they have been alive. Help them learn how that reality works, what benefits it provides but also what dangers it introduces. Talk about trust, honesty, and emotions. If you yourself feel unequipped to confront these issues, ask for help. School counselors and local therapists can provide advice or workshops to equip you with the skills you need to keep your kids safe online.

What School Counselors Can Do

1. **Add online deception to your discussions of "stranger danger."** If you born before 1990, threats to kids came from windowless vans, strangers offering candy, and other in-person dangers. Those threats still exist, but now they are accompanied by online predators.
2. **Look for signs:** Some of the typical signs of emotional distress point to problems that the minor is experiencing online. If you see kids with flat affects who are avoidant or shut down, check in on them. If a kid has a lot of absences, enlist community partners to provide therapeutic support in addition to the punitive measures taken by truancy officers.
3. **Explain to parents the challenge with location trackers:** A lot of people use Live360 and other apps to keep track of their kids' whereabouts. Unfortunately, this same technology can forge a sense of intimacy between your child and other people. If you track your kids' location, know that your kids might be tracked by other people, too.
4. **Curriculum enhancement:** We all know the benefits of social-emotional learning. Consider adding a unit on this topic to Grade 4 and 5 curricula. Show kids the live deepfake technology and "mask" apps, admit that technology is amazing, and then show them how the same technology can be used for harmful ends. Knowing how to "call the bluff" with a masked online person may be the current version of knowing how to dial 911.

Who To Call

Know2Protect Tipline: 833-591-KNOW (5669)

Submit a report with the National Center for Missing and Exploited Children at report.cybertip.org

To report a crime to the FBI Charlotte Field Office, call (704) 672-6100, submit a tip online at tips.fbi.gov, or visit the office at 7915 Microsoft Way, Charlotte, NC 28273. The office operates 24/7, and you can submit tips anonymously. For internet-related crimes, file a complaint at www.ic3.gov.