

What parents can teach before the first dangerous contact

If you take away nothing else: tell your child, out loud and often, “You will not be in trouble for telling me.” That single sentence — practiced before anything goes wrong — is the difference between a child who hides a problem and a child who brings it to you. These few words, repeated when you have a break, is enough to start.

The rest of this article is about building the conditions that make that sentence true:

Critical thinking + Guardrails + Safe disclosure = Resilience

When Belonging Becomes a Trap

Most parents have heard the warning by now: artificial intelligence is making online deception better.

The warning is true, but incomplete.

Here’s the part that gets skipped: children don’t go online because they’re targeted. They go online for the same reasons they always have — because they’re bored, because they want to be seen and accepted, because somewhere in a group chat or a game or a comment section, someone notices them, and they keep coming back to the places where that happens. Those are healthy, ordinary reasons. This pull has a chemical engine: unpredictable social reward is what drives dopamine hardest — the same mechanism behind a slot machine or screen addiction. [15] Many families fall into a version of this pattern early, and it isn’t limited to any one age: a phone handed over to quiet a fussy toddler, calm a bored eight-year-old, or settle a frustrated teenager is an ordinary, common habit in checkout lines, waiting rooms, restaurants. [16] It works in the moment, so it repeats — and in some children, repeated enough, that pattern can tip from habit toward something closer to dopamine addiction, a reward system that comes to need a screen to regulate a hard feeling at all. AI has not invented them. What it has done is get radically better and cheaper at counterfeiting them — manufacturing the exact feeling of being noticed, understood, and included, on demand, at scale, for whoever is worth targeting. The vulnerability was never the technology. It’s the very ordinary human pull that puts a child in front of it.

AI can make a fake profile more convincing, a romantic overture more fluent, a fraudulent message more personalized, an impersonated voice more believable, and a

manipulative conversation easier to sustain across hundreds of targets. It improves the quality of deception—its realism, speed, adaptability, and scale.

The FBI has warned of increased activity by “764” and similar violent online networks that target and exploit vulnerable young people. These networks are not simply conventional scams; they may use manipulation, sexual exploitation, extortion, coercion, and threats to pull victims into escalating harm. [1]

The extreme cases matter because they make the mechanism visible. But parents should not assume the risk is limited to highly publicized networks, or that it can’t happen in their own home. Everyone can be a target — the same scam or approach goes out to thousands of kids at once, whether or not any one of them seems special. These scams include sextortion, bullying, impersonation, romance fraud, gaming-community manipulation, and predatory “friendships.”

But technology alone does not explain why a child, teenager, or vulnerable young adult stays in a harmful conversation after the first suspicious message. The deeper answer is human and social: people return to places where they feel noticed, accepted, understood, useful, admired, desired, or included.

That is the part parents need to understand.

Online risk isn’t only about grabbing a child’s attention. It’s about belonging. A platform might first get a child’s attention through boredom, novelty, outrage, humor, or curiosity. But belonging — real, partial, or faked — is often what keeps a child coming back.

This isn’t the whole story — family context, peer relationships, mental health, platform design, and individual differences all matter too. But it’s the part most safety advice skips.

And that is where prevention must begin.

The first opening is often ordinary

We have all seen what boredom can look like in a cat: the sudden, apparently purposeless sprint down the hallway; the ambush of a shoelace; the demand for attention at the exact moment a human tries to work. This is not an argument that children are cats, or that human online behavior can be reduced to animal instinct. It is a simpler observation: attention seeks something meaningful to do.

But the observation is still useful. Attention is not spent evenly. We conserve it, direct it, and respond to what appears meaningful.

For a child or teenager, social media, games, group chats, livestreams, and messaging platforms provide a nearly continuous stream of things that might matter: a notification, a comment, a new follower, an invitation, a private message, a friend request, a rumor, a trend, a reward, a challenge, or a person who seems unusually interested.

Boredom can make that stream attractive. It creates availability for attention capture.

But boredom is rarely the whole story. A young person may open a platform because there is nothing else happening, then stay because someone replies. Someone laughs at a joke. Someone shares a problem. Someone offers a role in a group. Someone says, “I understand you.” Someone asks for help. Someone appears to choose them.

That is not a trivial exchange. Being recognized is one of the basic experiences through which people form identity and belonging.

The concern is not that children seek belonging. They should. Healthy belonging—to family, friends, teams, classrooms, faith communities, clubs, neighborhoods, and interests—is protective. The problem is that online systems and bad actors can imitate its signals — exploiting that innocence — without offering its safety.

Belonging has become an attack surface

Cybersecurity professionals use the phrase “attack surface” to describe the points at which a system can be entered, manipulated, or compromised.

For young people online, one of the most important attack surfaces is not a password or a device. It is the need to be seen.

That need can be exploited in many forms:

Human need or condition	Healthy function	How it can be exploited
Boredom or unoccupied attention	Rest, exploration, curiosity	Clickbait, bait content, predatory outreach
Belonging	Friendship, community, shared identity	Fake groups, grooming, “us against them” loyalty

Trust	Cooperation and reduced social friction	Impersonation, compromised accounts, false authority
Urgency	Fast action in real problems	“Act now,” account threats, family-emergency scams
Identity	Exploration of interests, values, and competence	Status games, extremist recruitment, false expertise
Care and empathy	Mutual aid and moral action	Charity fraud, rescue scams, emotional manipulation
Romance or attraction	Intimacy and development	Catfishing, sextortion, coerced images or content

These mechanisms are not new. Fraud, coercion, romance scams, recruitment, and blackmail existed long before smartphones.

What has changed is the delivery infrastructure.

Technology now lets an offender find potential targets, collect public clues about them, send test messages, move conversations across platforms, use false identities, maintain contact at all hours, and pressure a person without ever entering the family home. AI increases the efficiency of every early stage: identifying a likely target, generating plausible messages, matching language and interests, and creating fake images, voices, or social proof.

The basic structure is old. The reach and realism are new.

Six ways AI has changed the landscape

This article focuses on one specific pattern — AI-enhanced grooming through simulated belonging — because it's built on the deepest, most ordinary human need, and it's the hardest to see coming. But it isn't the only way AI has changed the risk to families.

AI-enhanced grooming. Chatbots and AI-assisted conversation can now mimic a peer's tone convincingly enough to build trust without a human predator typing every message. This is what the rest of this article is about.

AI-generated sextortion. An identifiable photo of your child, posted publicly or just sent by them in an ordinary conversation, can be turned into fake explicit content and used to threaten exposure to people who know them. No grooming required — which is

exactly why the disclosure promise matters even when nothing felt wrong. The FBI's Internet Crime Complaint Center has warned of this pattern since 2023. [2]

Deepfake cyberbullying. A 2023 CDC survey found that 16% of high school students had been bullied online in the past year — that's the baseline, before AI even enters the picture. [3] What AI changes is who's capable of doing real damage: increasingly, the person weaponizing it against a child isn't a stranger — it's a classmate. Widely available tools can turn an ordinary photo into a fake explicit image in minutes. NCMEC has reported a sharp rise in these cases, including one involving more than 40 girls at a single Iowa high school whose classmates used AI to create non-consensual deepfake images from their social media photos. [4]

AI voice-cloning scams. A short audio clip of a child's voice — pulled from a public video — is enough to convincingly fake an emergency call to a parent. Guardrail #7 below covers how to verify before you believe it.

Unregulated AI companionship. Nearly three in four teens have used an AI companion app for conversation, role-play, or emotional support. [5] That's not automatically dangerous — but a companion that's always available, never disagrees, and never gets tired can make a lonely child less likely to do the harder work of real relationships.

Data exposure through sharenting. Photos parents post publicly — birthdays, first days of school, everyday milestones — can be scraped and repurposed by anyone, including for the kind of extortion described above. Your child doesn't have to make an online mistake to be at risk; your own posting habits are part of the exposure.

Each of these deserves its own article. This one goes deep on the first, because belonging is the hardest attack surface to patch — you can't just turn it off.

The path from contact to control

Most dangerous online interactions do not begin with an obvious threat. If they did, they would fail quickly.

They may begin with friendliness, humor, concern, flattery, shared interests, a gaming connection, a fandom, a group chat, a claim of similar experience, or an offer of help. The message may come from a real peer, a stranger pretending to be a peer, or a manipulated account belonging to someone the child already knows. Today, that might

be an AI deepfake of a friend, inviting them into harm without the friend ever knowing their likeness was used.

Picture an ordinary Tuesday. A twelve-year-old is bored, scrolling a game's chat after homework, and someone new joins the conversation — friendly, funny, oddly interested in a hard week at school. Over a few days the messages get more frequent, more personal. "You're actually easy to talk to." "Nobody else gets it like you do." Then: "Let's move to a different app, it's easier to just talk here." A week later: "Don't tell your parents about this — they wouldn't get it, and it's kind of our thing." By the time an uncomfortable request shows up — a photo, a secret, a "test" of trust — the child isn't weighing it against a stranger's demand. They're weighing it against losing the one place they felt fully seen.

This is a composite, not one child's story. But the shape of it — ordinary boredom, real recognition, a quiet request for secrecy, a small compromise, then leverage — is the same shape investigators describe case after case. It rarely announces itself as danger. It arrives as attention.

A useful model that summarizes the process is:

Not every harmful interaction follows every stage, and no formula replaces careful judgment. But the sequence helps explain why "just block them" is often too late or too simple.

Reachability

The target is reachable: through a public profile, open direct messages, game chat, a group invitation, a private server, a comment thread, a livestream, a shared group, or a friend-of-a-friend connection.

The young person may not be "looking for trouble." They may be lonely, bored, curious, stressed, socially uncertain, or simply present where billions of ordinary people are present.

Recognition

Someone makes the person feel noticed by responding with:

“You’re actually funny.”

“You seem different from everyone else.”

“You can tell me what is really going on.”

“You’re safe with us.”

“You’re better than the people around you.”

A child who feels unseen in ordinary life may thrive on this kind of attention, even when the source isn’t safe. That’s one of many reasons a purely technical response isn’t enough — a safe environment at home is essential.

Secrecy

Then comes the test: “Don’t tell your parents.” “They would not understand.” “This is just between us.” “Prove you trust me.” “You’ll get us both in trouble.” “Move to this other app.”

Secrecy is the pivot point. Healthy relationships may include privacy, surprise, discretion, and personal boundaries. But a relationship that requires a child to hide something frightening, sexualized, cruel, illegal, or isolating from a protective adult is not asking for healthy privacy. It is attempting to cut off rescue.

Compromise

The offender may seek an image, a personal fact, a recording, an embarrassing disclosure, an act of rule-breaking, money, access to an account, or evidence of compliance.

The compromise need not be dramatic at first. Often it is incremental: a small secret, a private photo, a joke that becomes a test, a request that becomes more explicit, a “challenge” that becomes proof of loyalty.

Threat

Once the target is compromised, the tone can change: exposure, humiliation, abandonment, threats to family, threats to distribute images, claims that authorities or friends will find out, or assertions that there is no safe way back. A trauma bond can form here — a strong emotional attachment to the person controlling them, built through

repeated cycles of abuse, tension, and intermittent kindness or reconciliation. [6] That cycle isn't only emotional. Unpredictable kindness after fear or tension delivers a dopamine hit sharper than steady kindness ever could — the same mechanism behind the checkout-line phone, now with much higher stakes — and the nervous system learns to crave the relief of reconciliation with the person controlling them the way it craves any other reward it can't predict. A victim caught in this cycle may display the fawn trauma response — trying to appease or please the person holding the threat, simply to stay safe. [7]

This is why children and teens may hide an online problem even from loving parents. Shame is not just an unfortunate byproduct. It is part of the control mechanism. It is essential to prevent the interaction from reaching this point.

What parents can do - the message that changes the outcome

The most protective online-safety message is not “never talk to strangers.”

That advice is too blunt for the world children actually inhabit. Some strangers become teachers, coaches, counselors, friends' parents, teammates, mentors, or future friends. More importantly, a harmful person may not feel like a stranger. They may appear to be a peer, a romantic interest, a trusted gaming friend, a fellow fan, or a person who seems to understand something nobody else understands.

A more useful message is:

No person who cares about you will require secrecy, sexual content, self-harm, cruelty, money, proof of loyalty, or isolation from people who protect you. If someone asks for those things, bring it to me. You will not be in trouble for telling me.

The final sentence is the load-bearing one.

A child who believes, “My parents will panic, punish me, take away my phone, blame me, or be disgusted,” is more vulnerable to coercion. The offender's threat lands on an existing fear: *If anyone finds out, I lose everything.*

A child who believes, “I can tell an adult and we will solve this together,” has an exit route.

Household rules still matter, but safety comes first, particularly before things escalate — left unchecked, it's a downward spiral. The immediate response to disclosure must be protection, calm, evidence preservation, and help—not interrogation or moral judgment.

Federal guidance on sextortion makes this explicit: the predator is responsible, not the child or the family; paying or complying rarely ends the blackmail; the account and messages should be preserved; and the incident should be reported. [8]

Beyond a safe environment - The core countermeasure

Recognizing the pattern is necessary, but recognition alone is not protection.

No one safeguard can prevent every harmful online interaction. A young person can be thoughtful and still be manipulated. Parental controls can reduce exposure but cannot eliminate it. A child may understand a rule yet feel too ashamed or frightened to ask for help.

The strongest protection is layered:

Critical thinking + Guardrails + Safe disclosure = Resilience

Critical thinking gives a young person a pause. They learn to ask:

Who is asking? What do they want? What is missing?
How can I verify this outside the message itself?

Within a safe environment they should be encouraged to ask the parent when in doubt.

Guardrails reduce isolation and exposure. They include age-appropriate privacy settings, shared-space norms, device routines, restricted direct messages, adult awareness, and clear boundaries around secrecy and contact.

Safe disclosure provides an exit. A child needs to know: *I can tell a safe adult without shame, immediate punishment, or abandonment.* That belief turns a frightening private problem into one that can be handled with support.

Together, these layers make manipulation harder to start, harder to sustain, and easier to interrupt.

What parents can do early

Parents do not need to become digital-forensics specialists. They need to establish a family culture in which critical thinking, practical guardrails, and safe disclosure are practiced before a crisis.

1. Build safe disclosure

Say the words out loud, repeatedly:

- “If something online scares you, confuses you, embarrasses you, or makes you feel trapped, tell me.”
- “You will not be in trouble for coming to me.”
- “We will deal with the problem together.”
- “Even if you broke a rule, sent something, or kept it secret, I would rather know.”

Do not wait until a problem appears. A child needs to hear this when nothing is wrong, in a calm setting, enough times that it becomes believable.

Then test whether the family’s behavior matches the promise. If a child confesses a small mistake and is met with ridicule or explosive anger, the larger promise will not hold when it matters.

2. Teach relationship red flags, not merely stranger danger

Children need clear words for what manipulation looks like. Teach them to notice when someone:

- Wants immediate private contact.
- Pressures them to move to a less visible app.
- Uses flattery to create a rapid bond.
- Says adults, parents, or friends “would not understand.”
- Demands secrecy.
- Asks for sexual images, personal images, money, passwords, location, or “proof.”
- Makes them feel responsible for someone else’s feelings or safety.
- Uses threats, guilt, urgency, or fear of embarrassment.
- Wants them to cut off people who care about them.

NCMEC's NetSmartz program offers age-appropriate materials, activities, and discussion guides for parents, teachers, and youth. [9]

3. Build critical thinking through structured second thoughts.

The goal is not to teach suspicion of everyone. It is to teach structured second thoughts.

When a message, video, image, claim, invitation, or urgent request appears, ask together:

- Who is making this claim?
- How do we know they are who they say they are?
- What do they want us to feel or do?
- What information is missing?
- What would make this story less likely?
- Can we verify it outside the message itself?
- Who benefits if we act before checking?

This is a child-scaled form of critical thinking. It is not an interrogation. It can happen at the dinner table, in the car, while watching a video, or when a family member receives a suspicious text.

The household lesson is simple: an appealing story is not automatically a true story, and urgency is not automatically an emergency. That's true online, and it's true everywhere else, too — a dramatic headline isn't automatically an accurate one.

Create practical guardrails

Guardrails are not a substitute for relationship or judgment. They reduce exposure, interrupt isolation, and make it easier for a young person to bring a concern forward.

4. Know the actual online environment

"Screen time" matters, but it is a crude measure. Two hours of drawing with a friend, watching tutorials, messaging cousins, and playing a game are not identical to two hours alone in rapidly changing private chats.

Parents should know:

- Which platforms, games, chat systems, and servers their child uses.
- Whether strangers can direct-message them.
- Whether the child has alternate accounts.
- Which groups or communities matter to them.
- Who their closest online contacts are.
- Which apps are used to move conversations away from parents, moderators, or public visibility.

This does not require reading every private word or turning the home into a surveillance state. It does require real involvement. The strongest version is collaborative: “Show me what you like about this space. Who is here? What are the rules? What would happen if someone made you uncomfortable?”

5. Use controls as scaffolding

Privacy settings, age-appropriate accounts, restricted direct messages, device limits, parental controls, and account reviews are useful. They lower exposure and make certain forms of contact harder.

But they are not a substitute for relationship.

A determined child can evade controls. A bad actor can enter through a friend’s account, a game, a school device, an email, a text, or a new app. Think of controls as guardrails, not the driver. The durable protection is the child’s practiced ability to pause, recognize pressure, and seek help.

6. Use shared space as a safeguard, not a spy system

For younger children, make shared family spaces the default place for computers, tablets, gaming, and new online activities. A desktop or laptop in an open room does not prevent every problem, but it creates ordinary visibility. A parent can see the digital world the child is entering, ask a casual question, and notice a shift in tone — making conversation part of online life rather than an emergency intervention after something goes wrong.

For phones and tablets, an especially useful family rule is simple: **devices charge outside bedrooms overnight.** Late-night, isolated access is a different risk environment. Fatigue lowers judgment, intense feelings can become amplified, and

private conversations can continue without the ordinary interruptions of household life. A shared charging place also protects sleep without treating the child as a suspect.

Older children need growing privacy, and parents should not confuse privacy with danger. The principle is not “I must read every message.” It is: *you are entitled to privacy, but you are never required to manage coercion, sexual pressure, threats, or fear alone.*

The limits should be acknowledged honestly. Children can borrow devices, make alternate accounts, use mobile data, or move between platforms. That is why shared spaces, privacy settings, and parental controls are scaffolding—not the whole structure. They reduce opportunity and make help more reachable; the durable protection remains a child’s practiced capacity to pause, recognize manipulation, and bring a problem to a safe adult. Shared expectations about where and how devices are used, together with co-viewing or co-playing, remain part of current pediatric media-use guidance. [10][11]

7. Verify before you believe a voice

AI can clone a voice convincingly from just a short audio clip — often pulled from a public video a child has already posted. If you get a call, voicemail, or video that sounds like your child in distress, the response is the same as for any unverified claim: hang up and call them back on a number you already have, not one the caller gives you. [12] A family code word is a reasonable backup layer, but it depends on everyone remembering it under pressure — the callback is what actually works.

Practice the safe-disclosure response

8. Stop, Save, Tell

If a child receives coercive, sexualized, threatening, or manipulative content:

1. **Stop.** Do not send more images, money, passwords, or personal information. Do not send anything further, pay, or try to appease the person. With an adult’s help, preserve the account and messages, report the account, and then block the suspect.
2. **Save.** Preserve usernames, profile links, messages, dates, threats, payment requests, and screenshots. Do not delete the account or conversation before saving what may help reporting.

3. **Tell.** Bring in a trusted adult immediately.

Then report through the platform. For suspected child sexual exploitation, NCMEC's CyberTipline is the national reporting system; the FBI also directs victims and families to report sextortion and related crimes. [13][8]

If there is immediate danger, call 911.

9. Give the child more than one trusted adult

Some children will not tell a parent first. That is painful but normal. They may fear disappointing a parent, worry about losing access to friends, feel ashamed, or believe the adult will not understand.

Name other people they can contact: a grandparent, aunt or uncle, coach, counselor, teacher, youth leader, family friend, or older sibling. Make clear that asking another safe adult for help is not disloyalty. It is good judgment.

A child with multiple routes to safety is harder to isolate.

The role of schools—and their limits

Schools matter, but they cannot carry the full weight of online safety. Teachers are already managing crowded classrooms, performance requirements, administrative demands, behavioral needs, and limited time. A one-time internet-safety assembly cannot create the trust required for a child to disclose coercion, and a school policy cannot replace the daily relational work of family life.

Still, schools can make a meaningful contribution. Teachers can normalize critical inquiry and teach digital citizenship and media literacy. They can also notice when a student seems suddenly frightened, unusually secretive, distressed by notifications, withdrawn from familiar friends, preoccupied with an online relationship, or worried that something may be shared. None of these signs proves online coercion; each may reflect bullying, grief, family conflict, mental-health distress, or ordinary adolescent change. But they are enough to justify a calm, private opening:

"You seem under a lot of pressure. Is there anything online or off that is making you feel unsafe, trapped, or afraid to tell someone?"

The responsibilities are different but complementary. Parents and caregivers are the primary relational safety layer: they create repeated conversations, disclosure safety, household norms, and real knowledge of a child's digital life. Teachers are early observers and trusted-adult access points. Counselors and safeguarding staff provide assessment and intervention. Platforms, law enforcement, and policymakers retain system-level responsibilities that cannot be shifted onto families.

No one adult can see everything. The goal is a connected safety net in which a child does not have to face something frightening alone.

Use AI as a practice partner

AI is part of the risk environment. It can imitate, persuade, flatter, mislead, and generate seemingly authentic material.

But it can also be used constructively—under adult guidance—as a simulator for practicing recognition.

As an exercise to promote critical thinking, a parent and child might ask AI to create three **fictional, nonsexual, age-appropriate** messages:

- One from a legitimate classmate inviting someone to a study group.
- One from an ordinary scam trying to create urgency.
- One from a manipulative online contact asking for secrecy.

Then ask:

- What makes each message seem believable?
- What clues suggest pressure or manipulation?
- What information would we need before responding?
- What would be the safest next step?
- What might the AI itself have missed?

This use of AI teaches two lessons at once: how manipulation works, and why AI should never be treated as unquestionable authority.

This is a proposed family practice, not a proven prevention program. Try and adapt. Keep in mind that every incident is unique, and families should adapt the conversation

framework to its specific circumstances. It should supplement—not replace—adult involvement, platform safeguards, and professional help when a child is at risk.

Keep firm boundaries:

- Do not paste real private messages, names, images, school information, addresses, or account details into an AI system.
- Do not ask AI to diagnose whether a real person is dangerous.
- Do not use AI to continue a conversation with a suspected exploiter.
- Do not let AI become the child’s primary confidant for fear, shame, sexuality, self-harm, or coercion.
- Use it to rehearse questions, not to replace a trusted adult.

UNESCO’s AI-education frameworks emphasize human agency, critical thinking, ethics, and responsible use—exactly the posture families need. [14]

The deeper lesson

The future of child online safety will not be secured by one better filter, one stricter rule, one annual school presentation, or one more frightening news story.

It will be shaped by whether your child learns early that:

- They are valuable as they are. They don’t need a stranger’s acceptance.
- Not every invitation is friendship.
- Privacy is healthy; secrecy imposed by someone with power is dangerous.
- Belonging should never cost them their safety or isolation from people who love them.
- An urgent message can wait long enough to be checked.
- Shame is a signal to seek help, not a reason to disappear.
- Asking for help is not failure. It is a form of strength.

AI will improve the quality of manipulation. That is real.

The answer is not to make children afraid of every online relationship, every new technology, or every stranger. It is to give them something stronger than fear:

Critical thinking + Guardrails + Safe disclosure = Resilience

Practiced judgment helps a child recognize pressure. Guardrails reduce isolation and exposure. Safe disclosure makes sure there is always a way back to a trusted adult when something goes wrong.

References and source notes

- [1] Federal Bureau of Investigation. (2025, March 6). Violent online networks target vulnerable and underage populations across the United States and around the globe. <https://www.fbi.gov/investigate/cyber/alerts/2025/violent-online-networks-target-vulnerable-and-underage-populations-across-the-united-states-and-around-the-globe>
- [2] Federal Bureau of Investigation, Internet Crime Complaint Center. (2023, June 5). Malicious actors manipulating photos and videos to create explicit content and sextortion schemes. <https://www.ic3.gov/PSA/2023/psa230605>
- [3] Centers for Disease Control and Prevention. (2024). Youth Risk Behavior Survey Data Summary & Trend Report, 2013–2023. <https://www.cdc.gov/yrbs/dstr/pdf/YRBS-2023-Data-Summary-Trend-Report.pdf>
- [4] National Center for Missing & Exploited Children. (2025). The deepfake dilemma: New challenges protecting students, confidentiality. <https://www.missingkids.org/blog/2025/the-deepfake-dilemma-new-challenges-protecting-students-confidentiality>
- [5] Common Sense Media. (2025, July). Nearly 3 in 4 teens have used AI companions, new national survey finds. <https://www.commonsensemedia.org/press-releases/nearly-3-in-4-teens-have-used-ai-companions-new-national-survey-finds>
- [6] Speck, P. M., & Patrician, P. A. (2019). A concept analysis of trauma coercive bonding in the commercial sexual exploitation of children. *Journal of Pediatric Nursing*, 46, 48–54. <https://doi.org/10.1016/j.pedn.2019.02.030>
- [7] Walker, P. (2003, January/February). Codependency, trauma and the fawn response. *The East Bay Therapist*. <https://www.pete-walker.com/codependencyFawnResponse.htm>
- [8] Federal Bureau of Investigation. (2024, January 12). The financially motivated sextortion threat. <https://www.fbi.gov/news/stories/the-financially-motivated-sextortion-threat>

- [9] National Center for Missing & Exploited Children. (n.d.). NetSmartz: Resources for parents, educators, and communities. <https://www.ncmec.org/netsmartz/resources>
- [10] Munzer, T., Parga-Belinkie, J., Milkovich, L. M., et al.; American Academy of Pediatrics Council on Communications and Media. (2026, January 20). Digital ecosystems, children, and adolescents: Policy statement. *Pediatrics*, 157(2), e2025075320. <https://publications.aap.org/pediatrics/article/157/2/e2025075320/206129/Digital-Ecosystems-Children-and-Adolescents-Policy>
- [11] American Academy of Pediatrics. (2026, January 20). How to make a Family Media Plan. <https://www.healthychildren.org/English/family-life/Media/Pages/How-to-Make-a-Family-Media-Use-Plan.aspx>
- [12] Federal Trade Commission. (2023, March). Scammers use AI to enhance their family emergency schemes. <https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes>
- [13] National Center for Missing & Exploited Children. (n.d.). CyberTipline. <https://www.ncmec.org/gethelpnow/cybertipline>
- [14] UNESCO. (2025, February 20). What you need to know about UNESCO's new AI competency frameworks for students and teachers. <https://www.unesco.org/en/articles/what-you-need-know-about-unescos-new-ai-competency-frameworks-students-and-teachers>
- [15] Özüçetin, B. (2026). Social approval, reward learning, and the neurobiological basis of social media use: A narrative review. *Journal of Consultation Liaison Psychiatry*, 2(1), 10-21. <https://doi.org/10.71350/jclp.27>
- [16] Radesky, J. S., Kaciroti, N., Weeks, H. M., Schaller, A., & Miller, A. L. (2023). Longitudinal association between use of mobile devices for calming and emotional reactivity and executive functioning in children aged 3 to 5 years. *JAMA Pediatrics*, 177(1), 62-70. <https://doi.org/10.1001/jamapediatrics.2022.4793>

Source note

The capture sequence, relationship-red-flag framing, and model Critical thinking + Guardrails + Safe disclosure = Resilience are analytical frameworks developed in this article. The cited sources provide factual context and practical reporting, safety, media-

use, and AI-literacy guidance; they do not independently validate every element of the framework.