

IDENTITY THEFT TODAY

Cyber and Scam Threats for Kids and Teens

August 19, 2026
12pm - 1pm EST



SESSION NOTES

Below is a summary of the topics and items discussed on the August 19, 2026 session of **Identity Theft Today: Cyber & Scam Threats for Kids and Teens**, featuring guest speaker Jennifer Weinstein of the National Cybersecurity Alliance.

These notes were compiled following a virtual webinar presentation and are provided for general informational purposes only. The session was presented by an attorney licensed in a specific state. Attorneys are not licensed in every state, and laws, regulations, terminology, and requirements vary by jurisdiction. This content is not legal advice and should not be relied upon as such. While best efforts were made to accurately capture the discussion, this document is a transcription summary and may contain errors, omissions, or inaccuracies in wording, facts, or interpretation. Legal Resources and the presenter are not responsible or liable for any consequences that may arise from reading, using, or interpreting this material. For legal advice specific to your situation, please consult with a qualified attorney licensed in your state.

SESSION TOPICS

Cyberbullying | Sextortion | Online predators | AI/deepfakes | Gaming scams
School tech privacy | Digital regulations | Account security | Family safeguards

[Click Here to Access Recorded Session](#) →

DIGITAL REALITY

- 95% of U.S. teens use smartphones, and nearly half say they are online almost constantly.
- Kids spend most time on YouTube, followed by TikTok, Instagram, Snapchat, and Facebook. Gaming is almost universal—an estimated 45.7 million U.S. kids play online.
- School-issued devices and learning apps add another daily layer, so each environment (social, gaming, school) carries its own risks.

ATTRACTIVE TARGETS

- Kids often lack the experience to recognize bad actors — the same "stranger danger" lesson applies online, because people aren't always who they say they are.
- They frequently have access to a parent's payment methods for in-app/game purchases.
- Scammers exploit social pressures — the desire for followers and public profiles over private ones.

CYBERBULLYING SIGNS

- Roughly a quarter of students report being cyberbullied in the past month, and more than half at some point; girls report it at higher rates.
- Unlike in-person bullying, it follows kids home, can be anonymous, is often permanent, and spreads fast — yet only about 44% of bullied students tell an adult.
- Watch for reduced online activity, deleting apps, and going silent about online life.

PREDATORS & SEXTORTION

- Predators commonly pose as a peer, build trust over time, and groom a child into staying silent; online enticement reports have risen sharply.
- Financial sextortion — one of the fastest-growing threats — involves coercing a minor into sharing an explicit image, then demanding money (gift cards, payment apps, crypto).
- Paying rarely stops it; offenders escalate. Victims are most often boys ages 14–17, with offenders frequently overseas.



PLATFORM SCAMS

- **Gaming:** In-game currencies like V-Bucks, Robux, and Minecoins have real value, drawing account theft, "free currency" scams, and fake giveaway links impersonating popular games or creators.
- **Social media:** Fake giveaways, AI-impersonated influencers, "fun quizzes" that harvest personal details, and fake friends who build trust before asking for info, money, etc.

AI THREATS

- Reports to NCMEC's CyberTipline involving generative AI have risen dramatically.
- Deepfake apps can turn an ordinary photo into a fake explicit image, and consumer-grade voice cloning can impersonate trusted adults.
- The federal Take It Down Act criminalizes non-consensual intimate images (real or AI-generated) and requires platforms to remove reported content within 48 hours.

SCHOOL TECHNOLOGY

- School-issued devices and ed-tech apps collect student data, and parents are often unaware of what's being used. Ask the school which sites are blocked and which apps collect data, and compare notes with other parents.
- COPPA requires parental consent before many services collect info from children under 13; keep school and personal accounts separate.

GLOBAL REGULATIONS

- **Australia:** A world-first law (in effect December 2025) bars kids under 16 from major platforms — with fines falling on platforms, not parents or kids.
- **Europe:** The Digital Services Act restricts under-13s, while France, Denmark, Greece, and Spain move toward under-15/16 limits.
- **U.S.:** No national ban; the baseline remains COPPA. None of these laws replace hands-on guidance at home.

ACCOUNT BASICS

- Use strong, completely unique passwords of at least 16 characters, stored in a password manager (which also flags credentials found on the dark web).
- Turn on multi-factor authentication everywhere it's offered.
- Keep software updated (enable automatic updates) and scrutinize every message, pausing before acting on urgency or pressure.

WARNING SIGNS

- After a scam, kids may show sudden withdrawal, mood or sleep changes, reluctance to attend school, unexplained charges, or screen-hiding.
- If a child is targeted: stop all contact, preserve evidence with screenshots, reassure them they're the victim of a crime, and report to the platform or law enforcement.
- If a child is in crisis or talking about self-harm, treat it as an emergency and call or text 988, the Suicide & Crisis Lifeline.

REPORTING RESOURCES

- **NCMEC CyberTipline and Take It Down** (free removal of minors' intimate images).
- **FBI** and **FTC** for online scams — reporting helps build the database even when you don't get a direct reply.
- **Common Sense Media** for app reviews and privacy settings; **staysafeonline.org**, **StopBullying.gov**, and FBI sextortion resources for deeper guidance.

Q&A HIGHLIGHTS

Q1: With kids on a parent's iPad as young as one or two, at what point do you start having safety conversations?

A: Many families begin around kindergarten, when kids first get school devices and start grasping "stranger danger." For younger children, use dedicated, locked-down kids' tablets so they can play or watch without reaching every corner of the internet.

Q2: Do some device lockdown features work better than others? The YouTube algorithm can still surface strange content.

A: No parental setting is foolproof. Tablets made specifically for kids help, but many parents find the controls aren't enough on their own — so it's important to check in regularly and review what your kids are actually accessing.

Q3. Are PayPal accounts easily hacked?

A: Not necessarily more than other platforms, but PayPal connects to many accounts (stores, gaming platforms), and every connection adds vulnerability. This is why you shouldn't save payment details across accounts — a breach on one exposes your PayPal info.

Q4. How do I approach my son and daughter-in-law about better safeguards for my grandkids (ages 11, 8, and 2), who each have their own iPad?

A: Start by making sure they're aware of the threats, so they understand why it matters. Then keep it simple — enabling parental settings on each device goes a long way. When there are multiple devices, beginning with a few basics is far more manageable than trying to lock down everything at once.

Q5. With age-verification tools like face scanning, is the U.S. just figuring this out, and will it improve?

A: Right now we're still figuring it out, and AI has thrown a wrench into verification. The most important thing is having conversations with kids early — teaching online safety the same way we teach looking both ways before crossing the street — so they can eventually protect themselves without a parent watching over every action.

ABOUT THE SPEAKER:



JENNIFER WEINSTEIN | NATIONAL CYBERSECURITY ALLIANCE

Ian has spent roughly six years at Iris® Powered by Generali, a provider of identity monitoring solutions that help users detect data exposure, protect their personal information, and recover in the event of identity theft or fraud. IRIS is Legal Resources' service and technology partner for its identity theft protection benefit. Attendees with questions may contact Legal Resources for more information or a referral.

DISCLAIMER: This summary highlights key webinar points and questions. For comprehensive details, view the full seminar at [LRSeminars.com](https://www.LRSeminars.com).

Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768

Email: info@legalresources.com

www.legalresources.com