KNOW2PROTECT®

KNOW THE RISKS ASSOCIATED WITH PEER-ON-PEER CRIMINAL ACTIVITIES

A GUIDE FOR TWEENS

When you go online, things can seem safe and private. However, some situations can quickly turn into something you never expected. Some kids your age, even people you know or some kids you don't know, might use the internet to bother, trick or hurt others. These online activities can turn into more serious actions that could include possible crimes like cyberbullying, sextortion, catfishing or deepfakes.

This guide explains the types of activities happening online today between peers — which could turn into criminal activities — and helps you understand the possible consequences.

Living inside a fishbowl, anyone can look in and see what you're doing — and that's how it is when you're active online. Your actions, messages and behaviors are visible to anyone. Once you post or share something online, it's permanent and anyone could find it, even if you think it's private.

Common tactics associated with Peer-on-Peer criminal activities that DO NOT ALWAYS INCLUDE child sexual abuse material (CSAM):

- **Grooming** is a way that one person tricks another person into building trust and a connection with them either in person or online. For example, someone from school or a stranger on your favorite gaming site befriends a kid and makes them feel special online to earn their trust.
- **Cyberbullying** is when someone uses phones, computers, gaming platforms or other technology to hurt, threaten or embarrass others online.
- **Catfishing** is when someone intentionally creates a fake profile or identity to trick another person into thinking they are someone else.
- **Deepfakes** are a type of Artificial Intelligence used to generate videos, reels or GIFs of people doing or saying things they did not do or say by using a person's face or body and then digitally altering it to spread fake information to be mean and hurtful to that person.
- **Sexting and non-consensual sharing** is when private "nudes" are shared without consent. This can be seen alongside cyberbullying or peers spreading images around the school.
- **Doxing** is when someone finds a person's private information and shares it online to try to embarrass, scare or hurt them. This could include their full name, home address, phone number or where they go to school.

KNOW THE RISKS ASSOCIATED WITH PEER-ON-PEER CRIMINAL ACTIVITIES

- **Swatting** is when someone makes a fake emergency call to the police or other emergency team to trick them into going to a certain place. The person usually says something serious is happening, like a shooting or bomb threat, even though it's not true. People do this to cause chaos and panic or get someone in trouble, and it can be very dangerous, potentially resulting in violence.
- **Manipulation tactics to engage in violence** is when one kid pressures another kid and makes them feel like they have no choice but to participate in violent activities that they would not normally do. This is common on apps with group chats, online scams, gaming and other platforms.
- **Threats or violence used to intimidate** is when one kid uses violence or the threat of violence to harm or scare another kid into doing something they wouldn't normally do. For example, one person makes another person cut themselves or cause harm to themselves or gets them to engage in doxing or swatting.

Common actions associated with Peer-on-Peer criminal activities that INCLUDE CSAM:

- **Self-generated CSAM** is sexually explicit images or videos taken of themselves. These images can then be shared consensually, with someone they are involved with, to remember an act of romance or sexual exploration.
- **Generative Artificial Intelligence CSAM (GAI CSAM)** stands for Generative Artificial Intelligence Child Sexual Abuse Material of a real or GAI-created child. GAI CSAM is sexually explicit images or videos created using generative AI, including deepfakes, of kids. Private nudes often become GAI CSAM.

RISKS ASSOCIATED WITH PEER-ON-PEER CSAM

No matter where CSAM images or videos come from, having them or sharing them is illegal. If these images or videos get into the wrong hands, they can be used to exploit and sextort victims.

- **Traditional Sextortion** is when a predator demands more photos of a person to keep the "nudes" they already have private. They will blackmail them by using the photo they already have, and tell them that if they do not give them more photos, they will share the photos or videos they already have with other people, including friends, family and other students at school. This is affecting both boys and girls.
- **Financial sextortion** is like traditional sextortion but instead of being blackmailed and extorted for more photos, kids are forced to send the predators money,gift cards, or something of monetary value. Once they send any amount of money, the person facilitating this action will typically continue to ask for more money. This happens to both boys and girls but happens more often to boys.
- **Sadistic sextortion** is like traditional and financial sextortion, but the demands being made include making the victim suffer or submit to the offender through violence or self-harm, such as being made to carve or brand themselves leaving permanent scars on the victim's body. This type of sextortion is often organized through online groups[1].

[1] *thorn.org/research/library/sexual-extortion-young-people*

KNOW THE RISKS ASSOCIATED WITH PEER-ON-PEER CRIMINAL ACTIVITIES

Any sexually explicit photo or video of a kid is considered illegal, whether it's self-generated or AI-generated, and there can be **legal consequences**. Creating, sharing or even having this on your device can be illegal. There may be legal consequences for sharing Peer-on-Peer CSAM ranging from a simple verbal warning to appearance before a juvenile or family court judge where consequences are imposed which may include various levels of deterrence such as court ordered community service or counseling, to more serious consequences including arrest and detention. Both adults and minors can be held accountable when they commit crimes online. In addition to possible federal criminal violations, many states have specific criminal statutes regarding sextortion and online harassment. Check state and local government resources in your area for more information.

If you or someone you know has experienced online child sexual exploitation and abuse:

- Contact law enforcement. Law enforcement helps keep you safe from online dangers, assists and supports you if you are victimized online and works to make sure those who break the rules are held responsible.
- If you've become a victim, don't feel embarrassed or ashamed, it's not your fault.
- Immediately save everything — images, screen shots of messages, audio and video recordings. Consider placing the phone in airplane mode and make sure Bluetooth and Wi-Fi are off to prevent anyone from remotely accessing, changing or deleting the information. This also helps preserve data on the device.
- Stop responding to the online predator.
- Do not send money and if you have already sent some, do not send more. Many kids comply with the demands to send money thinking it will stop the threats, but in most cases, the threats become more frequent once money is sent.
- Tell a trusted adult and visit dhs.gov/know2protect/how-to-report together.