KNOW2PROTECT®

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

A GUIDE FOR TEENS

There are many things you do online that can feel safe at first but then quickly spiral out of control. Most online crimes of exploitation start with grooming and can shift into other actions that could include crimes like cyberbullying, sextortion, catfishing or deepfakes. This can happen to anyone. Online perpetrators can even be your friends, people you know or other kids you don't know.

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.

When you communicate online, it's helpful to imagine yourself in a fishbowl. No matter where someone on the outside of the bowl stands, they can see inside. The same is true when you communicate online. Once something is shared online, it is permanent and anyone could see it.

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

- **Grooming** is a way in which one person manipulates another person into building trust and a connection with them either in person or online. For example, have you ever had someone slide into your DM and start complimenting you and trying to earn your trust? That can sometimes be innocent and sometimes lead to grooming.
- **Cyberbullying** is when someone uses phones, computers, gaming platforms or other types of technology to hurt, threaten or embarrass others online. Sometimes it can go so far that it breaks the law.
- **Catfishing** is when someone intentionally creates a fake profile or identity to trick another person into thinking they are someone else.
- **Coercion tactics to engage in harmful activities** can happen when a person pressures another person and makes them feel obligated to participate in an activity they otherwise would not do. This is common in online scams and groups. For example, dangerous online challenges that spread on social media that can lead to serious harm to oneself and others, such as death by suicide and even accidental death.
- **Deepfake** is 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.

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

- **Sexting and Non-Consensual Sharing** is when private "nudes" are shared without consent. This can be seen alongside cyberbullying or when peers spread images around school.
- **Doxing** is when someone finds a person's private information and shares it online to try to hurt them, publicly humiliate them, stalk them or harass them.
- **Swatting** is when someone calls 911 or another emergency number and makes a false claim of severe crisis or threatening situation to trick the police or other emergency personnel into going to a certain place. People do this to create a significant law enforcement response and cause chaos and panic that can potentially result in violence.
- **Intimidation tactics that involve threats or violence** can happen when someone harms or instills fear and coerces someone into doing something they wouldn't otherwise do to themselves. For example, one person makes another person cut themselves or cause harm to themselves and their bodies 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 by an individual and commonly shared amongst peers and people they meet online. These images can be taken and shared intentionally by minors, such as "sharing nudes" with someone they are involved with, memorializing an act of romance or sexual exploration.
- **Generative Artificial Intelligence CSAM (GAI CSAM)** stands for sexually explicit images or videos created using GAI by manipulating existing imagery.

RISKS ASSOCIATED WITH PEER-ON-PEER CSAM

Regardless of where the images or videos come from, having CSAM in your possession or sharing it can be illegal. If these images or videos get into the wrong hands, they can be used to exploit and sextort victims.

- **Traditional Sextortion** occurs when an online predator demands more explicit photos of a victim to keep the "nudes" they already have private. They will blackmail or extort a victim by telling them that if they do not give them more photos that they will share the photos or videos they already have of them with other people, including friends, family and other students at school.
- **Financial sextortion** is like traditional sextortion but instead of being blackmailed and extorted for additional imagery, they insist that the victims send them money, gift cards, or something of monetary value. Once a victim sends any amount of money, the predator will consistently ask for more. Since 2021, there has been an increase in the targeting of teenage boys. This has even led to devastating results, like death by suicide.
- **Sadistic sextortion** is like traditional and financial sextortion but the demands include making the victim suffer or submit 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 used by online groups such as Violent Extortion and Gore Groups[1].

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

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

- **Lifelong Consequences:** While it's not your fault if you are victimized by a peer online, you still need to be mindful of what you share online as it can have negative consequences. What you share online is out there forever. Many coaches, schools, colleges and employers check social media and other online platforms before sending offers to join their teams, offering admission to college, or sending a job offer.
- **Legal Consequences:** Any sexually explicit content of a minor is considered illegal, whether self-generated or AI-generated. Creating, sharing or even possessing this type of content on a device can be illegal. There may be legal ramifications 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 incarceration. 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 people safe from online dangers, assists and supports those who are victimized online and works to hold offenders accountable.
- If you've become a victim, don't feel embarrassed or ashamed, it's never the victim's 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 or if you have already sent some, do not send more. Many teens 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.