A Parent Guide to Online Sexual Exploitation and Human Trafficking During COVID-19

For parents, managing a household during this pandemic also means managing uncertainty and fear, often combined with financial insecurity, illness or grief. Parents are trying to protect our children, and keeping one’s family safe also means making sure kids are practicing safe habits online. Whether it’s attending virtual classes or keeping in touch with friends, most youth are spending significantly more time on their computers, cell phones and gaming devices, which also means an increased risk of online exploitation. While the internet has been a positive catalyst for innovation, never before has it been easier for traffickers to hide their identities, make contact with children, photograph them and profit from these images of sexual abuse. This guide is meant to inform and empower parents with tools to ensure that our children are staying safe online.

What is Online Sexual Exploitation?

Online sexual exploitation includes recruiting, live-streaming, consuming child sexual abuse material (formerly known as “child pornography”), and coercing and blackmailing children for sexual purposes.

Grooming

Grooming is the process that traffickers use to win over their victims’ trust, even love, in order to control and sexually exploit them. Traffickers troll the internet looking for children who express a desire for family and connection. When they identify a target, a trafficker starts the grooming process by building trust and a friendship that, in the child’s mind, can turn into something deeper. For the groomer, however, information about the child’s family and home life, addictions, desires and fears is ammunition to exploit that child. Sex trafficking survivors have described being drawn to their traffickers because they seemed to be the only ones to truly love and understand them. This is no accident -- traffickers actually trade tips with one another on how to win over and trap their victims.

Grooming is a central technique in the pimp playbook, but the traditional “in-person” method of winning a young person’s trust could take weeks, months, even years. With the rise of social media and online gaming, new virtual “friendships” have slashed dramatically the amount of time required to connect with and control a young person. Children are now being groomed for sexual exploitation online in a matter of minutes.

Catfishing

Catfishing is when an exploiter creates a false online identity to deceive a victim into developing a relationship, often romantic. A “catfish” watches what a child posts on social media sites such as Facebook, Instagram or SnapChat, in order to plan the best way to manipulate the child. Perpetrators may offer opportunities for modeling, traveling, performing in music videos, gaining fame and wealth. To the victim, this newfound friend can appear like a dream come true, until the catfish begins making demands, sometimes subtle, sometimes threatening.
Sexting
Sexting is the transmission of a sexually explicit image via any digital device. Sexting can happen between a child and a stranger, but it also happens with people known to the child, including other children. ECPAT-USA's youth instructors have observed that sexting has become normalized by tweens and teens, who view it as a form of flirtation. However, once an image is posted online, it is difficult, if not impossible, to remove. In a disturbing trend, some youth have created social media accounts featuring nude photographs of their classmates, while others have sold the images to fellow students, causing the victims to suffer devastating shame. Sexting also has serious legal consequences. It is a crime for an individual to create, distribute, or view child sexual abuse material, even if that person is a minor.

Sextortion
Sextortion is a form of online blackmail. It occurs when a catfish or other predator threatens to spread sexual images of a victim, unless that victim agrees to send additional and more explicit content. A child who had been persuaded to send one image can be coerced to send many more, including films of engaging in sex acts, for fear of discovery by their friends, schoolmates and, especially, family members.

Revenge Porn
Revenge porn, more accurately known as image-based sexual abuse, occurs when someone publicly shares private pictures that had been meant only for them — often after a breakup. In ECPAT-USA's school outreach and training, students have reported being subjected to this form of abuse by a controlling ex-boyfriend or girlfriend. Unlike sextortion, revenge porn might not demand that the victim do anything further - the abuser wants to “punish” the victim. Perpetrators are looking to inflict maximum harm through humiliation.

Child Sex Trafficking
Child sex trafficking occurs when someone under 18 years old is bought or sold for sexual purposes. Children are also victims of sex trafficking when they engage in sex in return for basic needs such as food, shelter, safety, or pocket money to purchase consumer goods. Child trafficking is a crime under both federal and state law. A child can never, under any circumstances, consent to be sold for sex. Traffickers are often adults, but they can manipulate other children to assist in recruiting victims. Both victims and traffickers can be male or female. In all instances, abusers are exploiting the vulnerabilities of the child.
Signs of Online Sexual Exploitation or Trafficking

This period of social distancing offers an opportunity to monitor for common indicators of trafficking and online exploitation. Below are some behaviors to consider if your child:

1. frequently exits and enters the home despite prohibitions on travel;
2. works excessively long hours for a new “job” (virtually or outside of the home);
3. displays signs of depression, anxiety or unusual fears, or a sudden loss of self-confidence;
4. exhibits injuries or other signs of abuse;
5. fears authority figures;
6. receives sums of money transferred into accounts such as Venmo, CashApp, and PayPal;
7. experiences a disturbance from usual sleep patterns;
8. spends an increased amount of time online or on the phone, checking in with an unidentified “friend;”
9. suddenly changes their appearance or style of dress;
10. has an increase in package deliveries, money, clothing or jewelry;
11. provides inconsistent explanations for any of the above.

It is important to note that there is no one red flag to spot trafficking, and professionals in the anti-trafficking field typically look for multiple indicators when working with victims.

It’s Your Responsibility To Understand E-Technology

If you are the parent of a teen or tween, chances are that your child has a much more comfortable relationship with internet technology than you do. That’s normal, but to help protect them, it’s essential to be aware of some important information.

Privacy Settings
Parents should understand how to adjust privacy settings. Default settings for many platforms are “public,” which means that any stranger can see what your child is posting. Settings should be restricted to known friends. At the end of this guide, we have placed some instructions for adjusting privacy settings for some popular sites amongst children and teens.

Limit Identifying Information
In addition to explicit photos, check that your child is not posting sensitive information like his or her cell phone number, address, email address or birth year on social media. For younger children who insist on posting photos, provide them other alternatives such as setting their profile picture to a favorite cartoon character. Below, we have provided information on ways to monitor social media usage.
Set Rules about Where and How Your Child Uses Social Media
Require that children use their phones or laptops in common areas of the house, such as the living room, especially at night. Ask them about who they chat with, along with names or phone numbers that you do not recognize. Some parents have required that their children add them as “friends” in their social media groups but be advised: kids have created accounts for their parents to view and a separate one for their peer group (these accounts are often called a “Finsta” - “fake Instagram”).

Set Rules about Where and How Your Child Uses Online Gaming Sites
Require that your child play in a room where you can keep an eye on them and hear their headset conversations. If your child receives a message from someone they don’t know, ask them to not respond or click on any links contained within the message. Report these users directly to the site.

Take time to explore games with your children. Ask them to show you what they like about the game and take interest. Speak with them about making their profile private if possible and to only speak with gamers that are their real life friends.

Talk to your child about their gut feelings they may have when something doesn’t feel right. Some examples of predator solicitations include:
1. Gradually steers the conversations toward sexual themes;
2. Sends many messages to your child over a short period of time;
3. Asks your child to keep their relationship a secret.

Beware of New “Friend” Requests
The internet has revolutionized the ability of our children to connect with their peers across the globe, an innovation that can be educational and deeply meaningful. At the same time, any time your child connects with a “new friend,” there is a real danger that a predator is entering their life and your home. Teach them that a friend is not someone they just met and that a “friend” online is not the same thing as a friendship developed over time and in person. Make sure that children are not sending friend requests to (or accepting requests from) people they’ve never met.

Block and Monitor Certain Sites
If you feel that your child needs protections beyond what can be accomplished through conversation or house rules, consider using programs to prevent him or her from visiting certain sites, especially those with sexually explicit content. You can put a filter on any devices your child uses through different programs and apps. To prevent accidental exposure, consider configuring your search engine for “safe search.”
Speak With Your Kids

ECPAT-USA has spent hundreds of hours in classrooms with students, and while we have been sharing information with them about healthy relationships, online safety and the dangers of sex trafficking, they also have taught us a great deal. Here’s what we have learned from them:

Knowledge is Power
Candid conversations with our children about healthy and unhealthy sexual behavior is essential to protecting them. Some child trafficking victims reported being tricked by an exploiter because they never had discussed sex with their families. Additionally, traffickers target children who have suffered prior sexual abuse and who do not have a clear understanding of sexual boundaries.

Take An Interest In Their Friends
Encourage friendships that have been long-lasting and beneficial for your child as they grow. At the same time, stay aware of new friendships. How does your child know this person and how is that information confirmed? Are they older or isolating your child from their normal friend group? Are they offering opportunities that seem unrealistic? Let them know that traffickers specifically try to woo young girls and boys with promises of a better life, attention, and love.

Create A Safe Space
Fear of “getting in trouble” is a major factor in a child’s decision to avoid seeking help. Catfish, traffickers and other exploiters know this, and a child will often be subjected to prolonged sexual abuse rather than risk discovery by a parent. If your child has engaged in sending explicit posts, remain calm and supportive. Your child is likely a crime victim, and needs your support and protection, not criticism or punishment.

Helpful Resources For Parents
If you see warning signs and think a child may be a victim of human trafficking, call the National Human Trafficking Hotline at 888-373-7888.

NCMEC (National Center for Missing and Exploited Children) - 1-800-THE-LOST
NCMEC’s CyberTipline is the nation’s centralized reporting system for the online exploitation of children.

National Human Trafficking Hotline - (888) 373-7888 or text 233733
Also offers an online chat. All are available 24/7 in English and Spanish, or in 200 additional languages through an on-call interpreter.

For more tools and information, check out the resources page on our site. To learn more about how to empower youth to become advocates against trafficking in their communities, visit ECPAT-USA’s Youth Against Child Trafficking (Y-ACT) program page on our site.
How To Adjust Privacy Settings

Facebook (Desktop)
Step 1: Log into the Facebook account with the phone number/email and password.

Step 2: Click the pull-down menu arrow in the top right corner. Select “Settings.”

Step 3: Select “Privacy” on the left sidebar and you will be directed to the account privacy settings where they can be adjusted as preferred.

Facebook Messenger
Step 1: After logging into the account with the phone number/email and password on the Messenger app, tap the profile icon in the top, left corner and select “Messaging Settings.”

Step 2: Toggle the bar so that only designated people can chat with you and all other messages go to spam.
**Instagram (App)**
Step 1: Log in to the Instagram account with the username/email and password.

Step 2: Select Menu on top right corner of app and select “Settings” > “Privacy.”

Step 3: You will be directed to the account privacy settings where they can be adjusted as preferred.

**SnapChat (App)**
Step 1: Log in to the SnapChat account with the username/email and password.

Step 2: Select the Settings gear icon on the top right corner.

Step 3: Scroll down to the “WHO CAN...” Menu to adjust who can view the images and location.
TikTok (App)
Step 1: Log in to the TikTok account with the username/email and password.

Step 2: Select the Settings icon on the top right corner.

Step 3: Select “Privacy and Safety.”

Step 4: You will be directed to the account privacy settings where they can be adjusted as preferred.

TikTok Family Pairing Mode-New Feature
1. Open TikTok on the parent’s and child’s phones.
2. Go to profile, then head to settings (it’s the “...” button in the top-right corner).
3. Scroll down to Digital Wellbeing.
4. Tap Family Pairing and select whether the phone belongs to the adult or the teen.
5. You’ll have to scan a QR code on one phone with the other to link the accounts.
6. Now, the adult can access the parent password-protect security features.

Links for Privacy Settings and Parental Controls on Gaming Platforms
Step-by-step instructions for some of the most popular gaming platforms can be found on the following websites:

Gaming Consoles and Systems
PlayStation 3 and PlayStation 4
Xbox One
Steam

Popular Games with Chat Function
Minecraft
Fortnite

Chatrooms for Gaming Sites
Discord
Twitch