Internet, Apps and Online Safety

Helen Browning
Chief of Staff
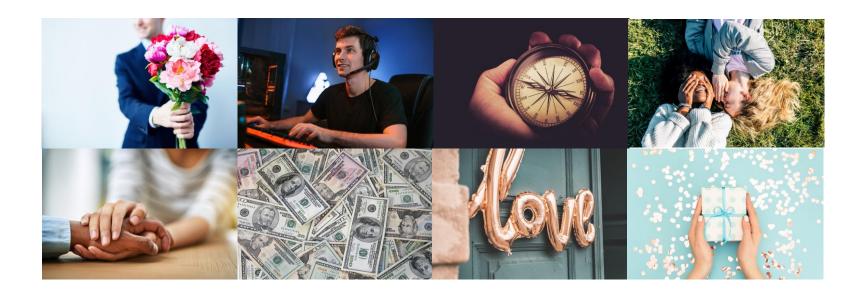
Objectives

Myths in Trafficking

Online Exploitation

Applications

Safety

Grooming

Grooming is a tactic where someone methodically builds a trusting relationship with a child or young adult, their family, and community to manipulate, coerce, or force the child or young adult to engage in sexual activities.

Grooming

SB 1527-

The law created a criminal offense for an adult who intentionally acts or attempts to coerce, entice, induce, or persuade a child younger than 18 years of age to engage in illegal sexual activity or conduct that constitutes a criminal sexual act on the part of the adult, or who makes a child a party to a sex crime.

This change allows law enforcement to prevent harm to child victims by giving authority for arrests of sexual predator's **pre-harm activity in order to minimize victimization** where there is evidence of enticement and/or coercion.

Child grooming is already a federal offense, known officially as coercion and enticement, with a penalty of 10 years to life in prison. Penal Code Section 15.032. CHILD GROOMING

Online Exploitation

The use of social medial or internet related sites to pursue, groom and exploit others for sexually explicated material.

• Predators playground to use anonymity and ability to disguise as someone else.

• Predators may not even be in the same city, state or country as the victim.

• In 82% of online sex crimes the offender used the victim's Social media to gain information

"People who do not believe that their children could ever become victimized online are living in an unrealistic world. Regardless of if your child makes 'As' [in school] or not, that child has the potential to become victimized through online technologies. I think it is very important for parents of all socioeconomic status and with all different roles in society to take this problem very seriously."

—Melissa Morrow, Supervisory Special Agent, Child Exploitation Squad, FBI

Accessibility

Online exploitation is easy to do because predators have accessibility to our children!

– From a young age children are given devices such as tablets, phones, computer for entertainment

– Parents believe that content restrictions fully protect their children

– Lack of monitoring or knowing how apps works

– Believing that you are interfering with your child's privacy

Why Now?

School Closures

- Social and physical isolation/lack of normal peer socialization
- Disruption of routines
- Child abuse in the home
- Domestic violence in the home

Increased Burdens

- Economic hardship
- Caretaking of siblings or other family members
- Fewer available services and supports
- Alcohol or drug misuse

Increased Internet Use

- Education
- Entertainment
- Connection

Declines

- Social Skills
- Coping Skills
- Resiliency

New Losses

- Quarantines and hospitalizations
- Death

Common Tactics

Engaging in sexual conversation/role-playing as a grooming method, rather than a goal.

Asking the child for sexually explicit images of themselves or mutually sharing images.

Developing a rapport through compliments, discussing shared interests or "liking" their online post, also known as grooming.

Finding Youth Online

The Number 1 Question

User Handles: (@yourchild'saccountname)

Hashtags (#12years)

Online Gaming

Why do Youth Engage?

-Prays on the desire for romance, adventure and sexual information

-Affirms feelings and choices by child

-Exploits natural sexual curiosities of children

-Make promises of an exciting, stress-free life, tailored to the youth's desires

What Should I look for?

Certain online behaviors may increase the risk for online enticement and becoming a victim of sextortion. These behaviors include:

Lying about being older to access certain platforms which would allow communication with older individuals.

Initiating online communication and/or offering an exchange with offenders, such as requesting financial compensation, alcohol/drugs, gifts, etc. for sexually explicit content of oneself.

Sending explicit photos or videos (known as "sexts") of oneself to another user.

Red Flags

and we are LIVE!!!

Hiding phones

Ending chats or conversations when you are in the room

Being on a device at late hours- always tired from being "online"

Gifts being delivered or having items they cannot afford

Creating "Wishlist's" and posting them

Having anxiety or depression

Changes in normal responses

Sextortion

Sextortion is defined as the act of coercing people into sending explicit images of themselves and subsequently blackmailing victims with the public release of said images.

Artificial Intelligence

Now with artificial intelligence or AI and the ability to easily create "deep fakes," they can turn any innocent picture online into pornography.

Current target:
- Open Social media accounts of youth with a focus on young boys
- Youth that have "a lot" to lose

"In nineteen and a half hours they sent over 200 texts," said Tamia Woods who's own 17-year-old son [James Woods](#) became a victim of sextortion in November 2022.

What to do!

The 3 R's

- Resist responding

- Retain the information, images and messages

- Report it to police, the platform where they contacted you and the FBI at the internet crimes complaint center

- Tightening security settings on all social media account

- Limit identifiable information posted online

- Only share or interact with people you actually know

APP's

SNAP CHAT

Content
Seemingly "private" sharing results in more revealing content
Discover feature is highly suggestive and explicit

Restrictions
Family Center is easily disabled by teen

Safety
App pushes location sharing with strangers
Many teens use platform for sexting (considered distributing child pornography, if under 18)

Privacy
User data used for ads and marketing across the web

- Easy less formal way to communicate

- Hard platform to monitor for content

- Discover feature has no controls and can not be disabled.

- App defaults to sharing user information to strangers

Tik Tok

Content
Educational value offset by explicit content
Algorithm known to promote extreme content

Restrictions
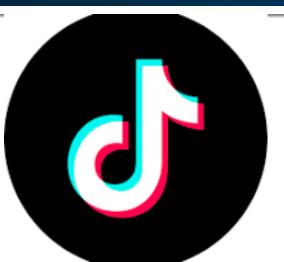Comprehensive parental restrictions available in Family Pairing

Safety
Teens able to quickly access more than they can handle

Privacy
Substantial data security concerns with ByteDance HQ in China

- 1 billion active users

- 63% of teens in America have it

- Dangerous trends, explicit material, content filtering is limited

- Highly addictive

Safety:
Family paring: Screen time, limit content, restrict notifications

Instagram

Content
Positive messaging is offset by explicit or overly edited content

Linked to many self image issues among teens

Restrictions
Supervision feature is limited and easily disabled by teen

Safety
Cyberbullying and unwanted outreach from strangers is common

Privacy
Shares aggregate data with third parties, data used for marketing

- Supervision can be removed by either party

- Privacy setting have no lock

- Highly addictive

- Sexually explicated content widespread

Safety:
Can hide like counts to help with self-esteem, set time limits, can not see messages, limited controls

WhatsApp

WhatsApp is a free, communication app owned by Meta (Facebook)
- Send Text and voice messages
- Make voice and video calls
- Share images, documents, user locations and other content

Over 2 billion users globally

Safety Concerns:
- Sharing location
- Ease of deleting activity history
- Privacy controls can be turned off on with out password

WhatsApp creates the ability for strangers to easily go from a social media platform to a voice/video/text messaging platform with live location sharing.

Facebook

Content

Content for all ages is available with minimal options to restrict certain types of content and creators

Restrictions

Supervision feature is limited and easily disabled by tee[n]

Safety

Users can limit public availability of profile information

Privacy

Settings can be toggled between friends and the public
Shares aggregate data with third parties for marketing

Safety Concern:
- Friend recommendation feature- recommends minors to adults

- Encrypted messages

- Limited parental controls

"The extra layer of security provided by end-to-end encryption means that the content of your messages and calls with friends and family are protected from the moment they leave your device to the moment they reach the receiver's device. This means that nobody, including Meta, can see what's sent or said, unless you choose to report a message to us."
~ Meta

Discord

Content
Explicit content widely available, platform frequently linked to cyberbullying

Restrictions
Family Center helpful but very limited, all other restrictions easily overridden/changed

Safety
Teens able to quickly access more than they can handle

Privacy
Extensive data collection with unclear uses

- Private invite only servers

- Highly sexual content with little to no monitors

- Multiple cases of predators using CSAM to groom children

- No real parental controls

Safety:
Family Center: can only see last 7 days of activity
 # of new users they added
# of friends they messaged

Roblox

Content
Content for all ages is available unless "allowed experiences" age-appropriate restrictions are enabled

Restrictions
Parent PIN must be enabled to lock restrictions

Safety
Chat is filtered by default
Limiting friends and chat in settings is essential

Privacy
Personally identifiable information should be protected by all gamers in usernames and chat

- Lots of parental control

- Roblox developers are updating content for safety and continues resources to support to report users

- Highly addictive and in app purchases

- Chat feature- can expose to offensive material

Safety:
- Parental controls
- Parent PIN- verified by email
- Robust chat filter

Minecraft

Content

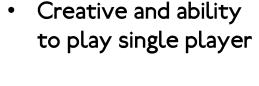Single player modes are largely safe, explicit content may be found with global players in multiplayer modes

Restrictions

Restrictions must be enabled within Microsoft Family Safety from a parent account

Safety

Private servers and realms are a safer alternative to multiplayer

Privacy

Personally identifiable information should be protected by all gamers in usernames and chat

- Creative and ability to play single player

- Limited violence and gore

- Highly addictive

- Hidden purchases

- Can have access to personal information and links

Safety:
Parental settings must have Microsoft Account- Microsoft safety settings
- Screen time   - Content restrictions

What Can I Do?

Open communication!

- Ask questions

- Know meanings of texts and emojis

- Set up your household boundaries and expectations

- 100- 1 min conversations.

- Know all passwords

- Create a contract

- Take trainings- i.e., NetSmartz

- Set-up safety words to communicate with youth during emergencies.

- Help youth identify healthy and unhealthy relationships.

- Teach youth not to forward any sexually explicit pictures or messages

But It Already Happened

Get help before deciding whether to pay money or otherwise comply with the blackmailer. Cooperating or paying rarely stops the blackmail.

REPORT the account via the platform's safety feature

BLOCK the suspect but DO NOT DELETE your profile or messages because that can be helpful in stopping the blackmailer.

Take It Down

Having nudes online is scary, but there is hope to get it taken down.

Take It Down is a free service that can help you remove or stop the online sharing of nude, partially nude, or sexually explicit images or videos taken of you when you were under 18 years old.

Recommendations

Monitoring apps on internet related devices:

- Bark APP
- MSPY
- NetNanny
- Famisafe

Websites:

- Bcfstrafficking.org
- Carlyryanfoundation.com
- Cybersafetycop.com
- Parentprotech.com
- Takeitdown.ncmec.org

Call 911

- If the situation is an emergency or you believe someone is in immediate danger, call 911 and alert the authorities. Tell them it is <u>Human Trafficking</u>, so that it can be routed to the proper investigators. Be sure to share all actionable information you have- including descriptions of cars and people, when and where you saw the conduct.

Call the National Human Trafficking Hotline

- After contacting law enforcement, call the National Human Trafficking Hotline at **1-888-3737-888**. You can also text "Help" or "Info" to 233733. Additionally, you can reach the hotline by email: Report@PolarisProject.org.

Contact Information

BCFS

Health and Human Services • Est. 1944

HUMAN TRAFFICKING INTERDICTION

24/7 Hotline for referrals:

1-888-8THREAD (1-888-884-7323)

Helen Browning
Chief of Staff
Hb3941@bcfs.net

www.bcfstrafficking.org