

# Online Safety Toolkit



# KEEPING CHILDREN SAFE ONLINE

## (via U.S. Department of Justice)

- **DISCUSS INTERNET SAFETY AND DEVELOP AN ONLINE SAFETY PLAN** with children before they engage in online activity. Establish clear guidelines, teach children to spot red flags, and encourage children to have open communication with you.
- **SUPERVISE YOUNG CHILDREN'S USE OF THE INTERNET**, including periodically checking their profiles and posts. Keep electronic devices in open, common areas of the home and consider setting time limits for their use.
- **REVIEW GAMES, APPS, AND SOCIAL MEDIA SITES** before they are downloaded or used by children. Pay particular attention to apps and sites that feature end-to-end encryption, direct messaging, video chats, file uploads, and user anonymity, which are frequently relied upon by online child predators.
- **ADJUST PRIVACY SETTINGS AND USE PARENTAL CONTROLS** for online games, apps, social media sites, and electronic devices.
- **TELL CHILDREN TO AVOID SHARING PERSONAL INFORMATION, PHOTOS, AND VIDEOS ONLINE** in public forums or with people they do not know in real life. Explain to your children that images posted online will be permanently on the internet.
- **TEACH CHILDREN ABOUT BODY SAFETY AND BOUNDARIES**, including the importance of saying 'no' to inappropriate requests both in the physical world and the virtual world.
- **BE ALERT TO POTENTIAL SIGNS OF ABUSE**, including changes in children's use of electronic devices, attempts to conceal online activity, withdrawn behavior, angry outbursts, anxiety, and depression.
- **ENCOURAGE CHILDREN TO TELL A PARENT, GUARDIAN, OR OTHER TRUSTED ADULT** if anyone asks them to engage in sexual activity or other inappropriate behavior.
- **IMMEDIATELY REPORT SUSPECTED ONLINE ENTICEMENT OR SEXUAL EXPLOITATION OF A CHILD** by calling 911, contacting the FBI at [tips.fbi.gov](http://tips.fbi.gov), or **filings a report with the National Center for Missing & Exploited Children (NCMEC) at 1-800-843-5678 or [report.cybertip.org](http://report.cybertip.org)**.

# Online Enticement

Via: National Center for Missing & Exploited Children

## OVERVIEW

**Online Enticement** involves an individual communicating with someone believed to be a child via the internet with the intent to commit a sexual offense or abduction. This is a broad category of online exploitation and includes sextortion, in which a child is being groomed to take sexually explicit images and/or ultimately meet face-to-face with someone for sexual purposes, or to engage in a sexual conversation online or, in some instances, to sell/trade the child's sexual images. This type of victimization takes place across every platform: social media, messaging apps, gaming platforms, etc.

## RED FLAGS

- 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. Sending or offering sexually explicit images of themselves. Pretending to be younger.
- Offering an incentive such as a gift card, alcohol, drugs, lodging, transportation or food.

## RISK FACTORS

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

- Lying about being older in order 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.

Between 2021 and 2023, the number of online enticement reports increased by more than **300%**

# Social Media

Beyond the Big 3



# Apps

## PARENTS SHOULD KNOW ABOUT

### Snapchat



One of the most popular apps in recent years. While it promises users can take photo/video and it will disappear, new features including stories allow users to view content for up to 24 hours. Snapchat also allows users to see your location on their Snap Map.

### WhatsApp



A popular messaging app that allows users to send texts, photos, voicemail, make calls and video chats worldwide. WhatsApp uses an internet connection on smartphones and computers.

### Kik



A mobile that allows anyone to contact and direct message your child. Kids can bypass traditional text messaging features. Kik gives users unlimited access to anyone, anywhere, anytime.

### MeetMe



A dating social media app that allows users to connect with people based on geographic proximity. As the name suggests, users are encouraged to meet each other in person.

### Whisper



An anonymous social network that promotes sharing secrets with strangers. It also reveals a user's location so people can meet up.

### Live.Me



A live-streaming video app that uses geolocation to share videos so users can find out a broadcaster's exact location. Users can earn "coins" as a way to "pay" minors for photos.

### Discord



An app that allows users to talk to friends and strangers in real-time via voice, text, or video chat while playing video games.

### TikTok



An app popular with kids for creating and sharing short videos. With very limited privacy controls, users are vulnerable to cyberbullying and explicit content.

# Use Parental Controls and Restrictions on Devices



## For iPhones, iPads, and other Apple products:

Parental controls and restrictions can be set up in Screen Time found in Settings. For more information see Apple's instructions at [support.apple.com/en-us/HT201304](https://support.apple.com/en-us/HT201304)

## For Android products:

Parental controls can be set up via the Google Play App. For more information see Google's instructions at [support.google.com/googleplay/answer/1075738?hl=en](https://support.google.com/googleplay/answer/1075738?hl=en)

# Resources

**For additional resources on online child safety  
visit the sites linked below:**

**National Center for Missing & Exploited Children's website:**

[missingkids.org/netsmartz/home](http://missingkids.org/netsmartz/home)

**NCMEC's Cyber Tipline:** [missingkids.org/gethelpnow/cybertipline](http://missingkids.org/gethelpnow/cybertipline)

**U.S. Department of Justice's KEEPING CHILDREN SAFE ONLINE:**

[justice.gov/coronavirus/keeping-children-safe-online](http://justice.gov/coronavirus/keeping-children-safe-online)

**Spanish (en ESPAÑOL):**

[esp.missingkids.org/gethelpnow/cybertipline](http://esp.missingkids.org/gethelpnow/cybertipline)

[esp.missingkids.org/netsmartz/home](http://esp.missingkids.org/netsmartz/home)