MESSAGING APPS

STREET GRACE™

Messaging apps are used in place of texts for convenience, privacy, and discretion. Perpetrators often switch to these apps before the inappropriate requests begin so there is no trail left to find. Parents need to be aware of the "reason" youth are switching to these messaging apps and the traits of each that may put users at risk for exploitation. Youth who frequently use game systems are especially prone to these risks because game system messaging features have strong censorship guidelines leading users to communicate through other means. Messaging app users need to be reminded that the "never go to a second location with a stranger" rule still applies online.

Whatsapp:

- Unlimited audio, text, photo, and video messages can be exchanged
- Anyone can create an account and there are no filters for adult content
- "Friends" of "Friends" can join group chats
- Messages are hosted on a platform other than the phone which protects it from normal "phone checks"
- An account can be accessed via a web browser as well
- Offers "end-to-end" encryption allowing users to create a code required to open each message
- Private photos can be downloaded or screenshotted and shared
- Hundreds of users can be in one group chat which can create an environment of hostility including sextortion and cyberbullying

GroupMe:

- Users can enable geo-location to communicate with people nearby
- Messages can be liked which can increase the impact of an unkind message
- Users can search the web within the app and there is no way to monitor this content
- Many users receive spam phone calls after verifying their number with GroupMe
- GIFs available through GroupMe can showcase inappropriate content
- Users can be added or removed from a conversation which can result in youth feeling ostracized and bullied

Discord:

- A third-party app used for game messaging
- Although it is designed for 13+ the creator of the messaging thread determines the age restriction
- Users can use the "join a server" function as a search bar which will provide easy access to inappropriate and lewd threads
- Direct message privacy settings are: "Keep me safe" which scans messages from everyone, "My friends are nice" which scans messages unless they are from a friend and " I live on the edge" which states "Turn this off. Don't scan anything. Go straight to the dark side."
- Predators can gain information on someone's likes or dislikes by what threads they follow which allows them to build rapport with potential victimized persons

If you would like more social media resources, please do not hesitate to email info@streetgrace.org.

PHOTO & VIDEO SHARING APPS

STREET GRACE™

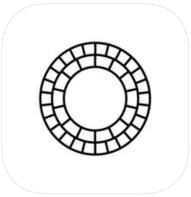
Photo and Video Sharing apps are probably the most common among social media platforms. The main danger with these applications is that users do not realize photos and videos do not always remain private. Screenshotting and forwarding are often the start of many sextortion and black mailing cases. Editing software now allows users to place faces upon the bodies of others allowing false depictions to be created and used as blackmail. It is also important for users to remember that our online foot print says a lot about ourselves both professionally and personally.

TikTok

- Users share comedy, lip-sync, or talent videos
- Profiles are made public by default (change this in your profile privacy settings)
- Everyone can view the videos and direct message users if not private
- In-app purchases are available and gifted among users which can encourage lewd behavior or dancing
- Under-aged users are exposed to the inappropriate lyrics of thousands of pop-songs which are often accompanied with sexualized movements
- Users can search via hashtag which can result in material that showcases sexualized dancing or lyrics, drug and alcohol abuse, self-harm themes, and explicit language
- Challenges and dares are common within this community and can lead users to commit dangerous acts

Snapchat:

- Time-restricted photos are sent between users
- The lack of permanency can lead to inappropriate behavior
- Although the “producer” is notified, users can screenshot the time-restricted photos
- “SnapStreaks” occur when two users have snapped back and forth within a 24 hr period for three days in a row – this is designated by a flame emoji, which can leave users feeling ostracized and can encourage cyberbullying behavior
- There is an age restriction of 13 and a “kid version” available but underage users can enter a false birth date to work around these restrictions
- “Snap Map” has to be activated since all profiles are automatically in “ghost-mode” but if activated it can show your location down to the street name and building
- The “Our Story” feature allows users to post photos or videos to a location’s story and allows users all over the world to access this material



VSCO:

- Many parents don’t know that VSCO is not just a photo editing app but also a sharing platform
- Users can create “Journals” that are similar to blog posts and often over-share
- Users can favorite a post and repost it to their profile which can spread harmful material cultivating a cyberbullying environment
- Profiles are public and content can be shared to other social media outlets
- Commonly used as a “secret” Instagram
- If both users follow each other they can exchange direct messages
- Location data is shared unless turned off in the privacy settings
- Users can search by hashtag which can lead to youth stumbling upon inappropriate content including sexual pictures/videos, drug & alcohol content, and explicit themes

If you would like more social media resources, please do not hesitate to email info@streetgrace.org.

LIVE STREAMING

STREET GRACE™

Live streaming apps are a risk for youth users because the content is not easily policed. Although many apps have flagging features and safety restrictions the images are often already seen before they are taken down or the creator is restricted from the app. Youth users often broadcast from their bedrooms unaware of how much information is shared through the background, including school or location information. Another major risk is screen recording which youth users may not consider when streaming themselves online. Below is some helpful information that explains the risks of three common live-streaming apps. Please note that age restrictions can easily be worked around or avoided and that more in-depth information on privacy settings and usage can be found in the terms & conditions of each application.

Houseparty:

- Unless you choose to "lock" your room any user can join the live-feed conversation.
- Friends-of-friends can join a "locked" room enabling contact with strangers. (There is a warning that pops up if the new attendee is not on your friends list but the live content seen before leaving a chat could be inappropriate.)
- There are no admins monitoring this app and since the content is live it is easy for youth to stumble upon or receive inappropriate content.
- Chat feature allows users to send photos/messages which might evade normal parental phone checks.
- Within even "locked" private groups members can take screenshots of their group
- Provides opportunity for bullying by excluding regular chat members and instills fear/anxiety that users are the subject of gossip within "locked" rooms.

Younow:

- An account is not required to view the live content of other users
- There is an in-app chat feature
- You can flag or block a user but as with all live-streaming apps the content is difficult to police
- Hashtags and categories are also used, a common one being #sleepingsquad where users broadcast themselves sleeping
- Unlike other live-feed apps Younow users typically live-stream for longer periods of time
- In-app purchases are available, the app's currency is "bars"
- Users can gift each other "bars" within Younow as a tip as well as use them to praise content, or get noticed by the live-streamer
- "Moments" are available in the app and screen record the last 25 seconds of live-feed, these snippets are then easily shared via a link
- Other users can create "moments" of you and they show up on the subject's profile in chronological order (you can hide these from your profile)

LiveMe:

- This app uses geo-location, so users' location is readily accessible
- Viewers can comment on broadcasts
- Anyone can view your live-feed
- In app purchases are available, the app's currency is "coins"
- Users can gift each other "coins" (These can be used to "pay" for photos)
- Broadcasts can contain illegal and inappropriate content

If you would like more social media resources, please do not hesitate to email info@streetgrace.org.

MEETING APPS

STREET GRACE™

Meeting apps are used to connect users with new friends i.e. strangers. Many of these apps use geo-location settings to match users with other near-by. Although almost all meeting apps have an age restriction, these are easily worked around by both underaged and overaged users. Predators often discover a teen's interests using social media and then contact them on a meeting app using a false name and photo. Meeting apps can then be used to "groom" potential victimized persons since the purpose of each is to connect and build relationships. In-app likes and currency can create an addictive environment and encourage inappropriate behavior. Parental phone checks should always include any meeting or dating app since all have chat features that may include more mature content than the text conversations that are accessible through your cellular provider.

Monkey:

- Allows users to talk with strangers with a 15 second intro-video using their snapchat usernames
- Users earn "bananas" which encourages extreme or lewd behavior
- Users can see the age and gender before connecting with them but there is no way to verify that this information is correct
- Direct messaging allows users to communicate privately and users can post "moments" for all of their followers to see
- Since this messaging app is in live-time the content is difficult to police and many underage users report seeing unsolicited nudity and inappropriate behavior

MeetMe:

- Uses geo-location to match users with others nearby
- No age verification and users sign up using an email and Facebook account
- There is no information verification which allows predators to pose as teens
- No privacy settings
- Currency is available which can be purchased with funds or by activity in the app encouraging users to meet more people – this aspect can create a very addictive environment for young users
- There is an "Ask Me" portion which is anonymous creating an environment for inappropriate and cruel behavior
- Users are encouraged to chat often, meet other users in person, and are even rewarded for chatting with users of the opposite sex

Yubo:

- Previously known as "Yellow", Yubo has been dubbed the Tinder for teens and was announced just after Tinder enacted its age restrictions
- Users can host live-video streams for an audience of friends and others
- Yubo connects users with others nearby – male, female, or I don't care – then swipe left to accept and right to decline
- Users can search or identify themselves by emoji, and research says that half of the top eight emojis used were sexual in meaning which given the targeted age is unsettling
- Profiles are image-based which can lead to users falsely claiming to be younger or of the opposite sex
- It is marketed to teens age 13-17 making it a destination for predators seeking those underaged
- There are safety settings such as the Yoti verification check which will show on a user's profile

If you would like more social media resources, please do not hesitate to email info@streetgrace.org.

DECEPTIVE APPS

STREET GRACE™

Deceptive Apps are those that market and profit off of discretion and anonymity. These apps can foster an environment of secrets and hostility in relationships and in the lives of youth. The tech savvy younger generations have found loop-holes for the standard phone checks and the apps below can help keep dangerous behavior secret. Traffickers prey on those who feel ostracized, abandoned, and insecure which is why cyberbullying is so closely linked with sex trafficking. Sextortion cases are also prolonged by threats of exposure and the apps below could prevent a helpful friend or parent from discovering unhealthy or dangerous behavior before it becomes a problem. These apps aren't adherently harmful but can open up a world of secrets, inappropriate behavior, and danger for youth.

Calculator#:

- Hides photos and videos which can only be accessed through entering a numerical code into the calculator
- Apps can always be hacked and the material found can be used in blackmail and sextortion cases
- Commonly used for sexting and viewing pornography

Whisper:

- Anonymous platform for users to express themselves
- Reveals a user's location making it easy to connect with others including predators
- Frequently used to cyberbully due to the anonymity feature
- "Terms of Use" ask the user to acknowledge that the app cannot guarantee users will not encounter objectionable content
- All posts created on the app become the property of Whisper and can be shown again

ASKfm:

- Encourages users to allow anonymous people to ask them questions
- Known for cyberbullying
- Users link their account to their other social pages providing even more information about themselves
- You do not need to be "friends" with someone to see their photos, chitchat, and answered questions

Tellonym:

- Anonymous messenger app
- Every profile is public by default
- In-app access to the internet that is not restricted
- Inappropriate messages can be accompanied by images since accounts can be linked to other social media pages
- Users can filter content based on keywords
- Users can search for others by location, age, or gender

If you would like more social media resources, please do not hesitate to email info@streetgrace.org.