Online Safety

A study by Common Sense Media in 2015 found that teens spend an average of 9 hours a day consuming media (such as: television, gaming, social media, telephones). That's more time than they spend sleeping. Tweens (8-12 years old) spend an average of 6 hours a day. Teens are online an average of 5 hours a day and 73% of teens are on a social network. As caregivers, it is crucial to learn about the social media children and teenagers are using and the risks thereof. Those risks include:

- Cyberbullying – over half of teenagers have reported being bullied online.
- Sexting – 20% of teenagers have acknowledged that they have engaged in sexting and two-thirds have felt pressured to do so.
- Online predators – Predators are using social media to gain access to potential victims.
- Adult content – Over a quarter of children ages 10-17 have been exposed to unwanted sexual material. One in three youth have viewed pornography intentionally.

Social Media Dangers to Watch For:

1. <u>Age-inappropriate content:</u> apps that feature user-generated content may include content not appropriate to your child's age (e.g., Ask.fm, Tumblr, VinTV)
2. <u>Public default settings:</u> apps with default public setting allow anyone to see your child's profile or send friend requests (e.g., Instagram, Tumblr, Twitter, Ask.fm)
3. <u>Location tracking and sharing:</u> apps that can include your child's location in their posts (e.g, Twitter, Facebook, SnapChat, Instagram, Messenger)
4. <u>Real-time video streaming:</u> live streaming makes it possible to share unintended things, such as the layout of your child's bedroom (e.g., You Now, Twitch, BIGO Live, Periscope, Facebook)
5. <u>Ads and in-app purchases:</u> apps that track purchases and show targeted ads (e.g., Kik, Line, SnapChat, Facebook)
6. "<u>Temporary" pictures and videos:</u> apps allow pictures and videos to be shared across devices with the idea that these disappear. However, they can be screenshot with any mobile device (e.g., SnapChat, Line, Periscope, YouNow).
7. <u>Subpar reporting tools:</u> levels of moderation and ability to report abuse vary across apps. Look into reporting ability and how easy it is to access for any social media your child uses.
8. <u>Anonymity:</u> apps that allow people to be anonymous which then makes cyberbullying a very real threat (e.g., Lipsi, YOLO, Whisper, Ask.fm, Chatspin, Holla).
9. <u>Cyberbullying:</u> this remains one of the biggest threats your child will face in the online world. Certain apps make it easier to cyberbully due to anonymity features (e.g., YOLO, Lipsi, Ask.fm).
10. <u>Secret Apps:</u> apps designed to hide photos, videos and notes (e.g., Photo Video Vault, Secret Calculator Photo Album, Photo Vault, Secret Apps Photo Lock)

Most Dangerous Apps (updated at least once a year):

Social Media Apps:

1. <u>Instagram:</u> This is a photo and video sharing app where users can also share private messages now, including disappearing photos and "stories". Youth make fake Instagram (Sinsta) accounts for close friends or to avoid the watchful eyes of parents. In addition, a number of fake profiles

have been created with the purpose of bullying. Instagram also has a default Public setting for privacy, meaning anyone can "friend" a user until the privacy settings are changed.

2. Twitter: This site openly allows pornography and has a poor record of ending bullying.
3. SnapChat: This is a disappearing messaging app that allows users to send photos and videos to others which "disappear" after 10 seconds. However, the recipient can still take a screenshot of the picture. In addition, SnapChat allows for live streaming and location sharing where other users can track their "friend's" location whenever the app is opened.
4. Reddit: Anyone with the Reddit App can also access the subreddit, "Reddit Gone Wild", which includes pornographic images. Reddit rules don't prohibit nude selfies as long as they are voluntarily posted. Reddit does not verify age, thus users under 18 can access these images.
5. Kik: Users can connect with others through just a username, meaning individuals can use Kik to meet strangers for sexting, cyberbullying, etc. There is no age verification when downloading it or registering.
6. Voxer: This is a walkie-talkie app that allows users to quickly exchange short messages with one or more people. This has also been linked to cyberbullying and is rated at ages 4+. Marco Polo has also become a popular video-messaging/walkie-talkie app.
7. Tumblr: This was designed for photo sharing and can also be used for sharing videos and chatting. Users can access pornographic, violent, and damaging content. The privacy settings are difficult to find and the default is public.
8. Whatsapp: This popular messaging app allows users to send texts, photos, voicemails, make calls and video chats worldwide.
9. Discord: This app allows gamers to connect via text, voice, and video. It exposes youth to adult content and the ability to chat with strangers.

Live Streaming Apps:

10. LiveMe: Users can create videos, send photos, or messages with people all over the world or nearby. Youth may be exposed to inappropriate messages and videos.
11. Tik Tok: This app is described as "raw, real, and without boundaries…It's from the gut, 'come as you are' storytelling told in 15 seconds."
12. Likee: Users create short lip-syncing videos to share and encourages frequent posting to gather likes. It also allows strangers to interact.
13. Houseparty: This is a group video chat app that allows friends to connect in a party line format. If one person in the chat knows two unconnected people, they can connect them via House Party. People can take screenshots during the chat without the other person(s) knowing it.
14. HOLLA: This app is designed to connect users with strangers immediately via camera. Location tracking is an option and users have reported exposure to sexual behavior, fake identities, and negative comments.
15. Bigo Live: Not only can teens live stream themselves and receive immediate feedback, but this app also rewards people with popularity rankings for giving out virtual gifts that cost real money. User comments are often explicit.

Dating Apps:

16. The Game by Hot or Not: Although this app says that users must be 13 or older and users 13 to 17 can't chat or share photos with users older than 17, there is no age verification process. Furthermore, youth can post their pictures for people to rate as "Hot" or "Not".
17. Down: The tagline says it all – "The secret way to get down with people nearby…if you want to hook up, say so!"

18. Bumble: Similar to Tinder, this requires women to make the first contact. Children have been known to create false accounts to use it.
19. Yubo (formerly Yellow): This app has been called the “Tinder for kids” and is marketed to 13 to 17 year-olds as a way to make new friends. Youth can pretend to be adults and swipe to hook up with others. There is no age verification process when users create an account.
20. Tinder: This app is advertised to users 17 and up but the privacy policy allows for children 13 and up to register. There are geolocation features and people can seek anonymous hook-ups.
21. Grindr: This Dating app is geared towards gay, bi, and transgender people. It gives users the option to chat, share photos and meet up based on GPS location.
22. Skout: This is another location-based dating app and website. Children can falsify their age to get around the prohibition from users under 17 sharing private photos.
23. Meetme: this is a dating social media app that allows users to connect with people based on location. Users are encouraged to meet each other in person.
24. Badoo: This dating and social networking app allows users to chat, share videos and connect based on location.

Anonymous Apps:

25. Yik Yak: Users are able to create and view threads within a 5-mile radius. All users are anonymous with registration requiring no personal information aside from user’s location.
26. Ask.fm: Users can send each other questions anonymously or using real identities. This app has been used in many cyberbullying cases, including ones that have been linked to suicides.
27. YOLO: Advertised as the “most fun and spontaneous way to get honest and genuine messages from your friends”, it allows people to send any form of message anonymously.
28. Whisper: The motto of this app is “Share Secrets, Express Yourself, Meet New People.” Users are anonymous as they share messages or confessions. It also shares the user’s location.
29. Wishbone: Users can send private messages to “friends” and create cards for comparison or would you rather questions.
30. Lipsi: Lipsi is described by it’s creators as “more than just an anonymous app. It’s a platform that attacks the boldest who want to step out of their comfort zone…Lipsi has proven to be an indispensable tool for many of the youngest generation yet.” This app allows users to link to their Instagram account so that the anonymous comments appear in their Instagram feeds.
31. Tellonym: This messaging app invites users to follow their contacts and share anonymous feedback with each other. Reviewers have noted bullying and users telling others to kill themselves.

Other Apps:

32. Vora: This is a fasting app that teenagers with eating disorders are using to celebrate and promote anorexia. Other apps popular on pro-ana forums include Eating Thin, Toilet Tracker, CalorieKing, Plant Nanny, Chronometer, MyFitnessPal, and Carrot Fit.
33. Roblox and Fortnite: While this seems like a nice game, it allows for chatting with strangers. Parents can disable in-game chats.
34. Calculator%: This is one of multiple secret apps where users can hide photos, videos, files and browser history.
35. Socratic Math & Homework Help: This app allows users to take a picture of a homework problem and essentially gives the answers (cheating).
36. BitLife: This simulation game takes the character from infancy to death with the player making text-based choices. It exposes players to hook ups, drug use, criminal activity, etc. as options for the character when it is older.

37. IMVU (3D Avatar Creator & Chat): This website/app allows users to interact via 3D avatars in public or private chat rooms, as well as buy objects to decorate their rooms or avatars with virtual coins obtained via surveys, watching ads, or using real money.

Parents don’t have to prohibit all social media apps. However, they do need to be aware of what apps their children are using and set up basic online expectations. Social media apps and their popularity continually shift, thus it is important to stay attuned to the newest fad among youth. **One of the best websites for parents to check is commonsensemedia.org.**

Enhancing Internet Safety

Rules for Youth

- Never give out identifying information in a chat room or bulletin board including: home address, school name, telephone number.
- Be sure someone is known and trusted before “friending” them.
- Never respond to messages that are suggestive, obscene, belligerent, threatening or uncomfortable.
- Remember people online may not be who they seem.
- Keep phones out of the bedroom after bedtime.
- Parents should approve and review apps before they’re installed.

Rules for Caregivers

- Get to know the services your child uses. Popular social media accounts at the moment include Instagram, SnapChat, Kik, Facebook, and Ask.fm.
- Social media sites change fairly often and it is important to be aware of privacy controls and use them!
- Set reasonable rules and guidelines for computer use by your teen.
- Get to know your teen’s online friends just as you would their other friends (those they communicate with regularly).
- Set the boundaries and consequences upfront.

Additional Resources for Online Safety

- https://dojmt.gov/safeinyourspace/parents-steps/
- http://www.aap.org/en-us/about-the-aap/aap-press-room/news-features-and-safety-tips/Pages/Talking-to-Kids-and-Teens-About-Social-Media-and-Sexting.aspx
- http://www.microsoft.com/security/family-safety/childsafety-steps.aspx
- http://www.fbi.gov/stats-services/publications/parent-guide/parentsguide.pdf
- http://www.connectsafely.org/wp-content/uploads/sexting_tips.pdf
- http://promos.mcafee.com/en-US/PDF/SocialNetworkinge-guide.pdf
- http://pediatrics.aappublications.org/content/127/4/800.full.pdf+html
- https://www.moneysavingpro.com/internet-providers/internet-safety-for-kids/