Fostering Family

SOCIAL MEDIA STUDYGUIDE

More resources available at **fosteringfamily.com**

Facebook
A newsfeed is the first thing you see when you log into Facebook, you'll see what your friends are saying, what they're talking about, pictures or media that they're sharing, you'll see news articles, you'll see advertisements. This will all be shown as a news feed.

There's also groups on Facebook. Groups can be where groups of people can share like-minded content. You'll see groups that buy/sell/trade, you'll see groups for hobbies, politics, religion—there are all kinds of groups available.

Facebook has a Messenger application. This is where people can private message others, or they can even have group messages with folks. This also has its own application, Facebook Messenger, and it can be accessed from inside the Facebook application. Facebook has a Marketplace. This is where folks can go to sell things.

Some of the vulnerabilities that Facebook is getting hacked. This is a common theme with all the applications that we talked about today. When somebody says that they've gotten hacked, usually that means that their password was compromised. Somebody figured out their password or maybe they left their phone unlocked and somebody was able to physically access their social media applications. Another vulnerability is called catfishing. Catfishing is where somebody pretends to be someone or something that they are not. You'll see this where people are trying to commit fraud in one way or another by pretending to be somebody or something that they're not.

There's many different sorts of scams on Facebook. You'll see some where somebody says go to this link and win all this money. That can be dangerous because that link could lead to a virus, or it could lead to a page where somebody's asking for personal information. You'll see your fair share of misinformation on Facebook. Not everything you see on Facebook is true. Make sure to do your own research.

We touched on this shortly, about malware or viruses. Always be sure if you're clicking on a link in Facebook, you know where it's going to take you. Sometimes it could direct you to a website that can install viruses and malware on your computer. Then bullying. Bullying has been and continues to be rampant on Facebook. This affects certain people pretty severely, or people will gang up on others, or share images about others or stories about others, and that can be really hurtful. You'll also see bullying common throughout all these social media applications for the most part. Just keep that in mind.

Snapchat
This site is famous for private, temporary photos and video sharing, and messaging. That means if you go to maybe look at your children's Snapchat, you probably won't be seeing any of the content that is being shared with them or they're sharing with others. That can be dangerous because you don't know what kind of content your young person is accessing on Snapchat.

As above, one vulnerability is getting hacked. Another vulnerability on Snapchat is location sharing. You can see where your friends are in real-time on a map. This is dangerous for people that may be stalking others. This is dangerous because there's been robberies involved. This can be disabled, but it is on by default. Just keep that in mind.

Twitter
This is micro-blogging social media. You're allowed to share text or media text up to 142 characters.. It's real short journaling and sharing ideas and events with others. You can share videos, you can share pictures.

Some of the vulnerabilities again are getting hacked, bullying, a lot of misinformation, fraud, and it could also be a very toxic environment. There's a lot of putting down other people and a lot of negativity on this application.

TikTok
This is mostly about short video journaling and publishing, where users can broadcast and subscribe to each other's streams. There's also messaging integrated into the application. Some of the vulnerabilities are extended app permissions. What this means is when you go to install TikTok, you should always get a box that tells you, hey, this app wants access to these features on your phone. This could include the GPS on your phone telling where you are in the world, this could include access to the contents of the other contacts on your phone, the names and phone numbers. This could also include access to the files on your phone.

Instagram
This features photo and video sharing. Messaging is also integrated. Vulnerabilities include getting hacked, and unattainable beauty standards. You may have heard about celebrities photoshopping their pictures on Instagram, making them look extremely skinny or making their bodies look in ways that are unattainable. This can make young people feel like they should look that way. It's very dangerous. There's also adult content on Instagram. They try to moderate it, but there's still a lot. Just be wary of that.

Discord
This is a voice and text messaging application. You can also live stream your screen or video gaming. It is popular with gamers. There are also chat features and group chat features in Discord. Some of the vulnerabilities are getting hacked, bullying, viruses. This is viruses that can be both embedded into Discord through some sort of media like a picture or file that has nefarious code in it. The content in Discord is largely unmoderated, meaning that nobody from Discord is really monitoring what kind of content is being posted or written in Discord. This can include adult content. It's also been linked to human trafficking. If your child uses Discord, pay attention to what they're using it for, and if anybody is trying to speak to them directly.

Twitch
This video streaming platform is popular with gamers. Some of the vulnerabilities are getting hacked and adult content. It can be a very toxic environment. If you ever look at a very popular streamer's chat room, you'll see a lot of very negative talk, a lot of very inappropriate speech.

Reddit
This is a social news platform with discussion forums. Content is rated by users. This means that the content that users see first is rated by other users. Reddit is largely unmoderated. You'll find a lot of adult content, misinformation, bullying, and negative or inappropriate content.

Youtube
This is a video sharing platform. Some vulnerabilities include misinformation and inappropriate content. YouTube is moderated by unfortunately, they can't pay attention to every video that's uploaded and what is in it. Inappropriate or adult content will stay on the platform until it's reported.

Omegle
This is where you can video chat with strangers. Some of the vulnerabilities that Omegle has is it pairs you with a complete stranger over video so you can see some very inappropriate things that people are doing, other people are saying. Be very careful about letting your young people use Omegle. It is unmoderated, nobody at Omegle is supervising what is going on live.

Messaging Apps
Almost all social media applications have chat. Vulnerabilities include hacking, catfishing, inappropriate content, and scams. Chat messaging can connect to Wi-Fi so it can function without cell phone data.

Parental Monitoring
Caregivers have the authority to monitor, remove, and/or restrict their children's devices and/or access to these devices. Your community support worker can help you go through this process of setting up restrictions.

Physical monitoring of devices. Know what devices that your child has access to: phone, tablet, computer, console, or anything that has internet access and can have apps. Even your child's devices that are sent home from school. Physically review messages and/or notifications in the different social media apps. Every family will have different strategies as far as physical monitoring.

Know the code to your child's phone and know the passwords to the social media accounts they use. Don't let them use every application they want to. Only allow the applications that you feel are safe and that the child is mature enough to access.

Physical monitoring is very direct and requires minimal technical skills. At any time, ask "Hey, let me look at your phone." Briefly go through the messages and the activity. It obviously requires the compliance of the child, and they may not always like it but make some sort of agreement. "You can use these applications if I can look at your phone." "You can have this phone as long as I can look through it." Set expectations.

Let your child know that you don't want them talking to strangers or accessing certain types of content. There's trust there. As long as that trust isn't broken, continue to allow them to use the phone and the social media applications. There's phone-based restrictions. The caregiver can have the password for the phone to monitor and set restrictions for online activity. Some of the examples can be restricting the minutes the youth has access, banning specific sites, or even receiving notifications if the youth is trying to access restricted sites.

You may need to be able to change the Wi-Fi or phone password. It can require slightly more technical knowledge. There are third party apps for monitoring and restrictions that you can use to monitor activity on the phone, like Net Nanny, Qustodio, Norton Family or FamilyTime. Apple has built-in parental features. You can allow them to only download specific applications that are rated a certain way. You can monitor how much time they're spending on the phone, how much time they're spending on each app. It's very powerful.

Restrict Wi-Fi Access
Physically unplug the modem at night. Even better, access built-in parental controls which wont disable Wi-Fi for every other device in the house. Cell phone data will continue to be allowed to be used even if your Wi-Fi router is unplugged.

It's important to use strong passwords because it makes it harder for hackers to guess. A strong password is usually eight or more characters long, including an uppercase letter, a lowercase letter, a number, and a special character.

Fostering Family

More resources available at
fosteringfamily.com