Good day,

I have had some requests from people who were unable to attend my Online Safety Presentations for Parents, to see if they could get the information about **'Potentially Dangerous Apps'** and **'Tips For Keeping Teens/Kids Safe Online.'**

Could you please distribute/forward to any parents interested?

Thanks,

Orlando

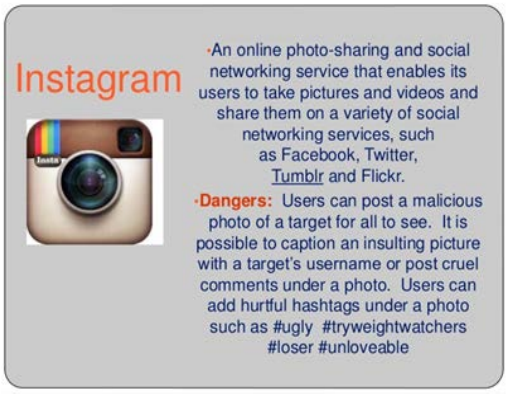
Tips for Keeping Teens/Kids Safe Online:

- **Educate yourself and your child about your devices, apps, etc. Learn how to use your devices and apps and look at the sites your child/teen visits**
- **Understand the dangers and be motivated to act. Two, start a conversation and keep it going!**
- **Use Parental Controls: Including limiting software, accountability software and filters on all internet connected devices.**
- **Do not let your children take their devices to bed and set limits for time allowed on the device**
- **Talk to your kids about the dangers we have discussed online – talk about anything and everything (pedophiles, bullying, sexting, etc.)**
- **Get involved/Ask questions about games/apps/sites they like to visit (ie.Minecraft, TFT, etc)**
- **Be open, approachable and understanding about what kids are up to online. This way it makes it easier for them to come to you with any problems they are experiencing online, and are happy to ask for advice.**
- **BE A POSITIVE ROLE MODEL. Be sure to role model the behaviors you want to see in your kids. Enjoy the positive aspects of technology with your family and be realistic in your rules and regulations in order to guide and support safe and responsible digital citizens.**

Some Helpful Resources:

- **netnanny.com, internet filtering software**
- **X3watch, an accountability software for all internet capable devices (x3watch.com)**
- **The Screen Time Parental Control App, allows parents to oversee all of the mobile devices within the home**
- **Iparent.tv, an online resource featuring videos and posts to keep parents in the loop on all the latest tech fads that your children might be into**
- **SafeEyes, a parental control software (internetsafety.com)**
- **Cybertip.ca, Canada's national tipline for reporting the online sexual exploitation of children**
- **Overnightgeekuniversity (Internet Safety Expert Jesse Weinberger) also on Facebook**

Potentially Dangerous Apps



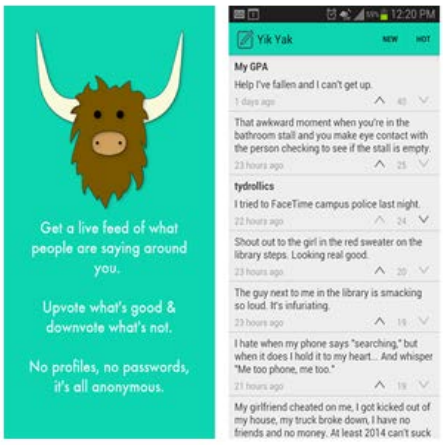
Please see link: Dangers on Instagram for Kids:
http://www.socialschool101.com/7-dangers-on-instagram-for-kids/

Please see link: The Dangers of SnapChat

https://netguide.co.nz/story/the-dangers-of-snapchat/

Please see link from CBCNEWS:

http://www.cbc.ca/news/technology/kik-chat-app-messaging-children-predators-pornography-police-1.3553355



Yik Yak is a free mobile app that allows anyone to post public anonymous messages — not even a profile or password is required.
Unlike many similar apps, it's location-based, so the messages are targeted at those within 2.5 kilometres.
Yik Yak bills itself as an app that lets you "get a live feed of what everyone's saying around you."

Concerns:

In some cases, the app has been linked to problems such as threats, pranks and cyberbullying. The "anonymous" nature of this app tends to lull teens into thinking that what they say and share won't be connected to them, which makes them more likely to behave inappropriately.

Kids have used this app to spread rumors and harass their peers, thinking that they are anonymous. Of course, this isn't entirely the case, and authorities do have the ability to track users. Other worrisome issues include the prevalence of graphic nudity and sexual content. The app encourages users to share just about anything, and because they think it's private, they often do.

The app lets users stream both audio and video to their audience for an interactive experience that includes feedback and comments. Audiences can not only interact, but watch and replay the video up to 24 hours after the broadcast ends.

Concerns:

- The potential for **real-time cyberbullying.**
- **Sexual harassment,** requests for teens to stream inappropriate broadcasts and inappropriate broadcasts being streamed to teens.
- The potential for viewers to **uncover the broadcaster's personal information**, such as username or Twitter account.
- **Location services reveal your teen's physical location**. Once the user's location was identified, the news investigation plugged that information into a free website that allowed them to track the user's exact location, giving them location updates every time the broadcaster posted something on social media. Even more troubling is that the location

marks are timestamped, leaving a “trail of breadcrumbs” to identify the user’s exact movements, allowing the tracker to follow the user’s physical movements as they go.

Ask.fm is an anonymous question and answer platform website used regularly by lots of young people in Ireland and around the world. It allows anyone to post anonymous comments and questions to a person's profile and is increasingly being used as a means to communicate abusive, bullying and sexualized content.

Whisper is an app built specifically for spreading rumors and secrets. It lets users post pictures and text anonymously. Apps like Whisper could potentially be a good outlet for teens as anonymous confessions can help people unburden themselves.

Concerns:
Whisper shares the secrets based on geographic location, so the users nearest to you are the ones more likely to see your secret. If your child reveals too much, it can put them in a dangerous situation with friends or adversaries.

The most dangerous apps for teens use GPS tracking to bring people physically together. Cyberbullying is much more hurtful when the person bullying your child moves from online to in-person abuse. In this case, Whisper seems like it could cause teens more harm than good.

Burn Note – This is a messaging app where all messages self-destruct (delete) after reading. This app only uses text messaging. Users cannot send images or videos. Parents would have no evidence that a conversation took place. This can lead to bullying or sexting or any other dangerous practice, and parents would have no idea.

9Gag.com – This is an image and video sharing site. Users can upload a video or image to share. Then the videos or images are voted up or down, and users can leave comments. Some posts are cute and fun. But most are not. Users can even browse the NSFW (Not Safe For Work) section. NSFW videos are blacked out until a user clicks the button to play the video. But nothing is stopping anyone, including children and teens, from seeing the inappropriate content.

Flinch is an app by the makers of OoVoo. The premise of this app sounds fun – it's basically the digital version of a staring contest. The first person who smiles, loses the game. While the technology behind the app is impressive, parents should know that kids using Flinch can stare down with complete strangers.

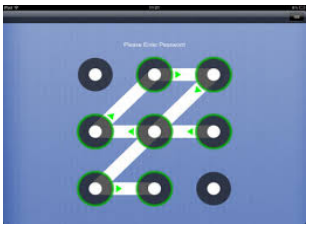
Concerns:
The main concern here is that when using Flinch you are **inviting a stranger into your home through a live video session**, similar to Facetime or Omegle. While the interaction time may be short, you are face to face with a complete stranger and anything goes. The app doesn't provide any recording/saving options but that doesn't mean the game can't be recorded or saved by taking a screenshot or using another camera to record the screen. Evidence of this is easily found on YouTube.

ooVoo is a video chat app. It lets you make video calls, voice calls and send texts to friends and family. You can also start a group video chat with up to 12 people. The default privacy settings are set to 'public', so you can talk to people you don't know, but they can be changed so that you can just talk to your friends.

Concerns:

While ooVoo has many great qualities and can be used in a completely innocuous and beneficial way, it's also home to **many adult users** and a lot of **inappropriate content.** A quick search for the #ooVoo hashtag on Instagram or Twitter reveals many images and videos that aren't appropriate for children and need to be filtered out using privacy settings.

Omeggle has been around since 2008, with video chat added in 2009. When you use Omegle you do not identify yourself through the service – chat participants are only identified as "You" and "Stranger;" the app's slogan is "Talk to Strangers!" You don't have to register for the App. However, you can connect Omegle to your Facebook account to find chat partners with similar interests. When choosing this feature, an Omegle Facebook App will receive your Facebook "likes" and try to match you with a stranger with similar likes. This is not okay for children. This app is the perfect channel for sexual predators. Experts say these predators blackmail young children, by starting inappropriate conversations with them, then threatening to send the messages, photos, or videos to their parents if they tell anybody, therefore trapping the child in a disgusting, dangerous situation.



‘Vault Apps/Secret Hiding Apps’

Vaulty, Best Secret Folder, Gallery Lock, KYMS (Keep Your Media Safe), Private Photo

These are apps used to hide Media (photos, videos, files, porn) from parents. some of the hiding Apps look like Calculator Apps and even function the same as a calculator app. However, once a numeric code is entered it gives the user access to hidden files.

Vaulty will not only store photos and videos away from parental spying eyes, but it also will snap a photo of anyone who tries to access the “vault” with the wrong password. Parents who find it on their teens’ phones can conclude just one thing: Your kid is hiding things from you.

As with all online games, websites and apps, we need to take time to see what our kids are doing Online. Even apps that look like they are designed for children can have elements that are inappropriate or even dangerous for children.

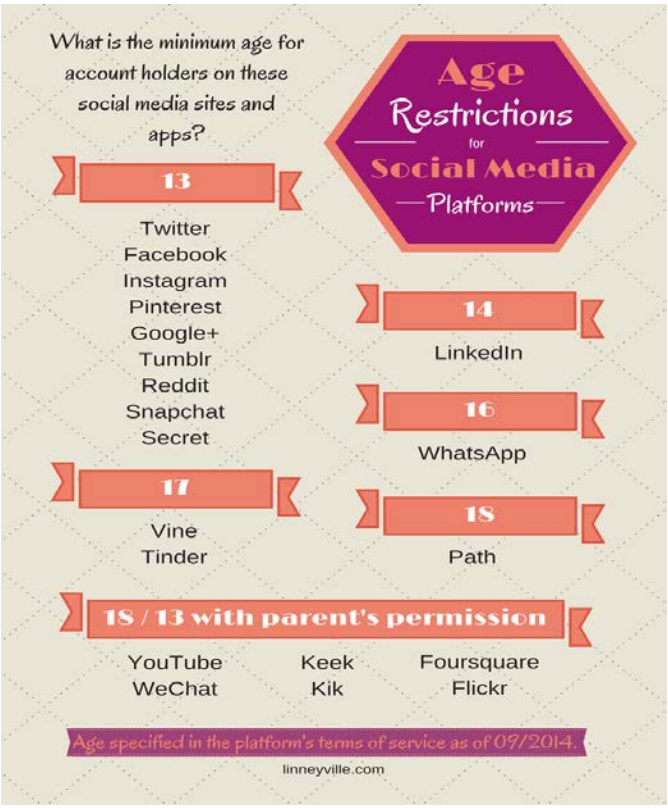
For example, Minecraft, a game designed for children, does contain elements that Parents should be concerned about.

See Link: /www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/minecraft-a-parents-guide.

Many of these apps mentioned above are fine when used properly, however, as with anything used online we need to educate ourselves and our kids about the risks involved with these apps. The list of ‘Potentially Dangerous Apps’ is constantly changing and we need to keep ourselves up to date on what our kids are using. By simply visiting some of the recommended

websites mentioned in Helpful Resources, or by typing ‘online safety’ in a Facebook Search, we can see trending/recent articles regarding what we need to know as Parents/Educators.

Finally, many Parents I have spoken with were not aware of the age requirements to legally have a Social Media Account. Please ensure that your teen meets these requirements before opening a Social Media Account and be sure you are able to access it. Know their passwords.



http://www.adweek.com/socialtimes/social-media-minimum-age/501920

If you have any questions, please feel free to contact me:

Cst. Orlando Buduhan#2249
Winnipeg Police Service
Community Relations Div.51 School Education Section
obuduhhan@winnipeg.ca
Cell: 204-794-3277