

PARENT IgNIGHT







SAFEGUARDING OUR CHILDREN, PART I: *Protecting our Children in the Digital World*

Dangerous Apps Every Parent Should Know About

It's safe to say that the advent of the digital age—and specifically the Internet, smartphones and social media—have brought unique and daunting challenges to the current generation of parents. As a “bonus” challenge, the technology, that both helps us parent and also poses danger to our kids’ safety, is ever-changing. As soon as you have one dangerous app deleted from a mobile device or have installed safety software on a computer, another scary app or Internet safety issue appears. The best way to face these parenting obstacles is to educate yourself about them.

Here are 15 dangerous apps or websites that your kids might be using— and why they shouldn't be.

App	What it is	Why it's bad
Tinder 	An app used to find dates and hook-ups using GPS tracking.	It is easy for adults and minors to find each other, and the “rating” system can be used for bullying.
Snapchat 	A photo-sharing app that allows users to send photos to specific people, assigning the photos an allotted time--after which they will “disappear.”	It's very popular for sexting. Users have figured out how to save or screenshot the images, so they aren't really gone and can be used against the sender later for “revenge porn” or any other nefarious purpose.
Blender 	A “flirting” app allowing users to send photos/videos to anyone on their “friends” list and rate their “hotness.”	This app uses GPS and is not authenticated, so predators can find minors or anyone they are looking for. It's also popular for sexting, and the “hotness” rating allows for bullying.
Kik Messenger 	An instant messaging app that allows sending of videos, pics, and GIFs.	It's very popular for sexting. There are no parental controls or authenticating, so it's really easy for predators to find your child on Kik.
Whisper 	An anonymous confession app.	Since it's “anonymous,” you can post pics and confessions of someone who isn't you (bullying). It also uses GPS, so predators can find you pretty easily.
Ask.fm 	A popular Q&A social networking site used almost exclusively by kids.	Its anonymous question-asking leads to consequence-free cyber bullying.
Yik Yak 	An app that allows users to post 200-character “Yaks” which can be viewed by the 500 closest to them as determined by GPS.	Users are putting logs of sexually explicit content on Yik Yak, and although it's anonymous, it can reveal personal details that make users easy to find.
Poof, Hidden Apps, Hide it Pro, App Lock 	These are all apps designed to hide other apps on your phone. Not all are available any longer, but if your child already has them, they can still use them.	These allow your child to conceal apps from their phone screen, so you will have to be diligent about searching for them.
Omegle 	A video chatting app.	Although you don't identify yourself, it's pretty easy for your child to make friends with a predator. It's known to be a predator favorite.

App	What it is	Why it's bad
Down 	A dating app connected to Facebook.	It allows you to classify your friends into people you would be "down" with "hooking up" with, creating normalcy for a sexual hook-up culture for your child.
Oovoo 	A video chatting app where users can chat with up to 12 people at a time.	While not terrible in itself, your kids MUST use the privacy settings and only let people who know them, chat with them.
Meerkat/ Periscope  	Similar live streaming video apps that stream video to Twitter.	Although it's against the apps' terms of service, since it's live streamed it's difficult to keep users from producing images with nudity or pornographic content, which makes it a favorite for predators to watch.
MeetMe 	An app that uses GPS to allow users to meet new people who live nearby	There's no age verification, and your account is linked to Facebook so you and your location are easily identifiable to predators. The popularity rating makes seeking approval from strangers seem like a game.
Skout 	A flirting app used to meet new people.	Ages aren't verified, and although there is a teen version with slightly more safety features, all you have to do to bypass is put in a fake birthday. This leaves children open to the adult version of Skout, which includes plenty of profanity, suggestive pictures, and private messaging with strangers who can see their location.
ChatRoulette 	A video chat site that randomly matches you up with someone around the globe to have a video chat.	It's very popular for cybersex and pornography, and it's not uncommon to be randomly matched up with a chat partner who's completely nude in front of their webcam.

Social Media Checklist for Parents

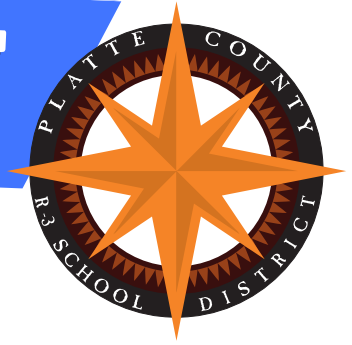
- Talk openly and often about online safety with your kids.
- Install safety monitoring software on all devices and limit screen time.
- Designate specific areas for internet use.
- Establish clear ground rules and safety principles.
- Stay up to date on social media and online trends.
- Monitor and know who your kids are interacting with online.

Sources

There are many websites that can help you keep up-to-date with the latest social media apps that could be dangerous for your child and ways to teach various ages about being safe online. This list of apps was adapted from www.foreverymom.com. Other websites that report on the latest social media and cyber safety:

- www.common sense media.org
- www.bewebsmart.com
- www.thecybersafetylady.com
- www.netsmartz.org
- www.qustodio.com/en/blog/
- <https://sos.fbi.gov/>

PARENT IgNIGHT



SAFEGUARDING OUR CHILDREN, PART I: *Protecting our Children in the Digital World*

Practical Help for Parents and Caring Adults

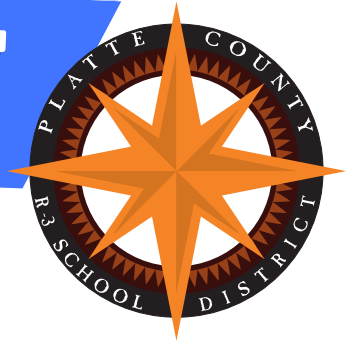
The following tips were shared by our speaker, **Russ Tuttle**. He is the president and founder of the **Stop Trafficking Project**, which includes serving as the director for **BeAlert**, an awareness and prevention strategy for the project.

Tips for Parents to Help Protect our Children in the Digital World

- Don't live in fear, but be wise.
- Be the parent before the best friend.
- Monitor social media. There are various products available for this purpose, i.e. <http://www.covenanteyes.com/>.
- Don't ever think/say, "Not my kid!"
- Student surveys indicate students are afraid/nervous/hesitant to ask parents for help after encountering tough issues online.
- Provide your child with the "X-Plan": they text you an "X" and you immediately respond with a call informing them you need to know where they are as there's a situation at home you need them to be there for...arrive quickly and listen to your child without saying, "how did you get into this mess?" or "I told you not to hang out with them," etc. The goal is to appreciate the fact they sent you a message admitting they need your help, so provide them that help because the ultimate goal is to keep them safe.
- Be careful with your own social media posts, especially pictures of your children.
- Do understand you are going against culture.
- Do understand every family will deal with this issue differently.
- Do be consistent in your plan after discussing it clearly with your children.
- Remember - you own their devices, have the right to know all the passwords, and should check their devices as often as you feel necessary.
- Remember - it's not **if** your child will encounter challenges via social media, it's **when**, and you need to be ready.
- It's easier to teach than un-teach. Teach them well, and teach them early. Lead by example.
- You are only as safe as your stupidest friend(s) online. This applies to adults, too.
- Ready to get radical? Try these actions with your child:
 - Controlled text groups only
 - No technology in any bedroom ever (an alarm clock can wake you up)
 - Be sure your student knows you are willing to trust them until they give you a reason not to
 - Continue to educate yourself on recent social media apps and ways to stay safer
 - Start a parent discussion group
- Never forget you can make a difference when you truly understand that it's all about the **exploitation of vulnerability**. Anything and everything you can do to lessen the vulnerability of your student to being exploited is a win!



PARENT IgNIGHT



SAFEGUARDING OUR CHILDREN, PART I: *Protecting our Children in the Digital World*

Set Rules, Limits, and Privacy Settings on Your Child's Devices

Sit down with your child and determine which sites and apps are appropriate to use, and set limits on what can be communicated and shared on each one. This includes photos, posts, comments, and anything else that exposes your child's identity. Set privacy settings together. Without proper privacy settings in place, anyone might have access to photos and information your child posts. For example, if your child has an unrestricted social media account, friends of friends (of friends...of friends) can see all the status updates, photos, tweets, and more, that he/she posts. Consider having access to any accounts your child has set up in his/her name. Insist your child become your "friend" or be a part of your network. This will allow you to be aware of any inappropriate behavior that might be going on, and it will also act as a reminder to your child of the transparency of this virtual world. Set time limits to avoid technology overload, and to ensure your child isn't neglecting other areas of his/her life. Also, limit technology use to common areas of your house.

You can also set restrictions and time limits on devices using the following steps.

Setting Up Parental Controls on iPhone Devices

Screen Time — a new feature of iOS 12 — lets you know how much time you and your kids spend on apps, websites, and more. You can make more informed decisions about how you use your devices, and set limits if you'd like to.

- Go to Settings and tap Screen Time on your child's device.
- First set a Screen Time Passcode that you'll only know.
- In the Downtime section, you can schedule time away from the screen in the Downtime section.
- In the App Limits section, you can set time limits for specific apps.
- In the Always Allowed section, you can choose apps that are always allowed (phone, text, map, etc.), even if within the downtime you have set.
- In the Content & Privacy Restrictions section, you can:
 - Prevent iTunes & App Store purchases
 - Set Content Restrictions for music, movies, apps, books, web content, and more
 - Control which apps have access to information stored on your device, such as photos, camera, location, contacts, etc.

Setting Up Parental Controls on Android Devices

The Family Link app from Google helps parents stay in the loop as their child or teen explores on their Android device, and lets parents set certain digital ground rules for their family. First, a child will need a compatible device. Then, parents can start by downloading Family Link onto their own device. If a child already has an account, Family Link will walk their parent through linking their account to their child's account. Once the accounts are linked, parents can use Family Link to help them do things like keep an eye on screen time and manage the content they use.

- Install Google Family Link from the Play Store app. (Parents can run Family Link on Android devices running version 4.4 and higher)
- Create a Google account for your child if they don't already have one.
- Open the Family Link app.
- Within the Family Link app, you can:
 - View their activity
 - Manage their apps (approve or block apps your child wants to download and manage in-app purchases)
 - Set time limits and a bedtime for their device
 - Remotely lock a device
 - Locate them if they are carrying their device