


CHILDREN'S  
HOME  
SOCIETY



**Child Advocacy Center**


# APPS YOU NEED TO KNOW ABOUT

The following are just a sampling of common apps that are being used by youth. Just because your child uses these apps doesn't mean they are engaged in risky behavior... but as a parent you should know the risks so you can educate your children. As with all technology, your best weapon is communication and monitoring. Know what your child is up to, turn off their access to wi-fi when you are concerned, and watch their emotional state for cues that something may be bothering them.

 **Whisper** (available as an APP or Website <http://whisper.sh/>)

This free app allows you to post secrets anonymously and to chat with other users in your geographic area.

*Risks:* This app is a perfect tool for ill-intentioned strangers looking to connect with young people because it allows you to exchange messages with people nearest to you. There is plenty of suggestive content and there is no supervision or control over what is posted.

 **YikYak** (available as an APP)

All Yik Yak users are anonymous, and they can post comments that are accessible to the nearest 500 people within a 1-5 mile radius. Untruthful, mean, character-assassinating short messages are immediately seen by all users in a specific geographic area."

*Risks:* This app is causing problems in schools across the United States, with students maliciously slandering teacher, staff, and other students. YikYak has begun to create geo-fences around middle schools and high schools to prevent use within those "fences" but inappropriate usage can continue anywhere.

 **Kik** (available as an APP)

A free app-based alternative texting service that allows texts/pictures to be sent without being logged in the phone history. **(Note: Similar to Viber, WhatsApp, Bee Talk, GroupMe, Fling, ooVoo)**

*Risk:* There is an internet browser within KIK, giving you access to any website, image, or video search. Web filters do not control content accessed within the APP. Children can reach out to public communities with just a click. KIK can make it difficult for Law Enforcement to access its records, increasing the risk since information is easily deleted. Parents should use extreme caution when deciding if their youth should have this APP.

 **Snapchat** (available as an APP)

Allows you to capture an image or video and make it available to a recipient for a specific time. After that time limit is up, the picture/video automatically disappears forever...or so Snapchat claims. **(Note: Similar apps:**

## **Poke, Wire, and Wickr**

*Risks:* Kids can receive (or send ) sexually inappropriate photos. This app also makes kids feel like they can “sext” or send inappropriate pictures without consequences because the image will self-destruct automatically. However, the sender and user can take a screenshot and redistribute the image. With the addition of “Snapchat Story”, snaps can be saved for up to 24 hours. There is now a Snap Cash feature which might increase the chance of offering money for photos through the APP.



**Vine** (available as an APP or website, <https://vine.co/#feed>)

Allows users to watch, post, and share short/looping videos.

*Risks:* While many of the videos are harmless, porn videos do pop up into the feed, exposing your children to sexually explicit material. You can also easily search for/access porn videos on this app, without creating an account. Predators utilize this app to search for teens and find their location and then try to connect with them via other messaging apps.



**Omegle** (available as an APP or website, [www.omegle.com](http://www.omegle.com))

This is a free online chat website that allows you to communicate with others without registering. This service will anonymously pair “strangers” together for one on one chat sessions. NOTE: this is similar to **ChatRoulette**.

*Risks:* Not only are users chatting with strangers, they could be chatting with a fake stranger. “Chat sites like Chatroulette and Omegle have done their best to produce systems that warns users when the people they are chatting to are potentially using fake webcam software, however developers still manage to slip under their radars with frequent updates.” At the end of the chat the users can “save the log” preserving private/sensitive information to be potentially used later. Typically Omegle users will offer their KIK username to continue conversations.



**Tinder** (available as an APP)

Users post pictures and scroll through the images of other users. When they think someone is attractive they can “flag” the image. If that person has also “flagged” them in return, the app allows you to contact them.

*Risks:* This app, and similar apps such as **Bumble, Grindr, Pure Dating, Hot or Not, Down Dating, Scruff, and Blendr**, are primarily used for hooking up.



**Ask.fm** (available as an APP or website, <http://www.ask.fm>)

This app allows users to interact in a question-and-answer format — with friends, peers, and anonymous users alike.

*Risks:* This APP has been linked to cyber-bullying, fantasy violence, or other suggestive material. The APP is integrated with Facebook and Twitter, easily cross-sharing posts. One user can block another user, but the blocked person can still access any profile to view other interactions. There is also a function in which users can ask questions anonymously of other users.



### **Voxer** (available as an APP)

This walkie-talkie PTT (push-to-talk) app allows users to quickly exchange short voice messages. They can have chats going on with multiple people at a time and just have to tap the play button to hear any messages they receive.

*Risks:* Hurtful messages from cyberbullies can be even more biting when they're spoken and can be played repeatedly. The APP also allows location to be shared and can turn off the privacy notifications.



### **Textfree** (available as an APP)

This is a free SMS texting app that provides you with your own phone number, free unlimited text messaging, plus calling to any phone, including landlines, in the US and Canada. This works with any device with Wi-Fi.

*Risks:* This can be used similarly to any other texting APP. The concern is that without a phone, this APP can be used on other devices to have secret conversations that parents are unaware of.



### **Tumblr** (available as an APP or website, [www.tumblr.com](http://www.tumblr.com))

This platform can be used for sharing text, photos, vidoes, links, music, etc. This is one of the more commonly used services.

*Risks:* Users can easily access pornographic, violent, and inappropriate content. Common Sense notes that users need to jump through hoops to set up privacy settings — and until then, all of a user's photo and content is public for all to see. There does not need to be an account set up to access all of the information shared.



### **Instagram** (available as an APP)

This hugely popular photo-sharing site is owned by Facebook, so you may be more familiar with it than with other photo-sharing apps. Users can add cool filters or create collages of their photos and share them across Facebook and other social media platforms. Users can also go “live” and create stories.

*Risks:* Users can find mature or inappropriate content and comments throughout the app (there is a way to flag inappropriate content for review). "Trolls" — or people making vicious, usually anonymous comments — are common. A user can change the settings to block their location or certain followers, but many users are casual about their settings, connecting with people they don't know well or at all. Check out [connectsafely.org](http://connectsafely.org)'s "A Parents' Guide to Instagram."



### **Pinterest** (available as an APP or website, [www.pinterest.com](http://www.pinterest.com))

This is one of the most widely used social platforms. Users can “pin” creative ideas on their “boards”. Users can create secret boards, which can be shared with specific other users. There is also a “chat option” in which you can share pins or other information.

*Risks:* There is limited control regarding inappropriate items, unless it is user reported. Users can post and share any information they want, despite graphic nature. The APP can also be used solely for its chat option, hiding communication from parents. The content is visible to searches, unless steps are taken to ensure the user's privacy.



Facebook



Twitter

(available through an APP or website)

Facebook users are allowed to post videos, text, photos, etc. There is a “live” function, which has been most recently to stream suicides, beatings, or other graphic content. Twitter users are allowed to post up to 140 characters at a time, allowing others to respond, and repost the information.

*Risks:* Youth are being contacted or “friended” by unknown individuals, and the messenger or direct message options in either APP allow for direct contact. Personal information can be collected from these sites, and used to threaten or intimidate the user. User’s information may also be collected and then when speaking with someone in a different platform, that information is used against them or used to gain trust.



**MeetMe** (available through an APP)

“Chat and Meet New People,” says it all. Although not marketed as a dating app, *MeetMe* does have a “Match” feature whereby users can “secretly admire” others, and its large user base means fast-paced communication and guaranteed attention.

*Risks:* It’s an open network. Users can chat with whoever’s online, as well as search locally, opening the door for potential trouble. Lots of details are required. First and last name, age, and ZIP code are requested at registration, or you can log in using a Facebook account. The app also asks permission to use location services on your teens’ mobile devices, meaning they can find the closest matches wherever they go. **Note: Other Blendr, Pure Dating, Hot or Not**



**Musical.ly** (available through an APP)

This is a social media music APP where users watch themselves or other’s lip-synced videos. The videos can be shared privately or publicly.

*Risks:* Users can add friends on this APP and watch the videos of others and make comments. If the privacy settings are not monitored unwanted comments can be made on the user’s videos. Even when the user’s account is set as private there is nothing to limit them from search videos and finding pornographic videos set to music. These inappropriate videos can then be sent to other users. **Note: Musical.ly has also created Live.ly which is a live broadcast streaming platform.**

## APP Hiders



**Poof!**

Hides other apps on your phone. You select which apps you would like to hide and their icons will no longer show up on your smartphone screen.

*Risks:* If children have apps that they want to keep hidden from their parents, all they have to do is download this app and “poof,” their screen is clear of any questionable apps. So, if you see the poof app on their phone, you may want to ask them what they are hiding.



## AppLocker

This is an APP in which the user can “hide” other installed APPs.

*Risk:* Although the icon will be visible on the phone, the user can passcode protect to prevent access. The phone user can access any programs inside with the use of the passcode. **(Note: Similar APPs are Hide It Pro, Vault Hide, and Hide Pictures in Vaulty)**



## Smart Hide Calculator

This is a fully functional calculator which also allows the user to hide files/APPs inside.

*Risks:* This calculator looks and acts like a normal calculator APP, but when a passcode is entered all of the hidden APPs appear. Photos, videos and other files can also be hidden using this application.

**\*\*Children/Teen** may also utilize the “hide applications” feature in Android phones, which takes about 20 seconds to hide all APPs on the phone. Those with smart phones may simply use the “folders” option to hide APPs, and mislabel the folder to discourage parents from looking. They may also place folders on a different screen, to limit the viewing of them.



## Jailbreak Programs

*Risks:* "Jailbreaking" an iPhone or "rooting" an Android phone basically means hacking your own device to lift restrictions on allowable applications — meaning, the user can then download third-party apps not sold in the App Store or Google Play store (read: sometimes sketchy apps). It's hard to say how many teens have jailbroken their mobile device, but instructions on how to do it are readily available on the Internet. Cydia is a popular application for jailbroken phones, and it's a gateway to other apps called Poof and SBSettings — which are icon-hiding apps. These apps are supposedly intended to help users clear the clutter from their screens, but some young people are using them to hide questionable apps and violent games from their parents. Be aware of what the Cydia app icons look like so you know if you're getting a complete picture of your teen's app use.

The best line of defense is to check your child’s download history, and have a conversation with them about what is on their phone. It’s important for children to understand the dangers of the online world, and the more you know, the more you can be prepared to have those tough “What If...?” conversations!

For more tips check out [www.NetSmartz.org](http://www.NetSmartz.org).