

Navigating the Digital World: Parent Tip Sheet

Duplicate Calculators: Your device should only have one calculator. If you are showing more than one, check your settings under Apps or usage to find the hiding app.

Hidden folders or apps: A folder can be hidden when you hold it down to toggle, and press the home button twice. Swiping it away hides it from any home screen. To locate it, you must use the Spotlight feature (swipe left and search in the upper spotlight bar).

Other hiding apps:

-My Utilities:

Disguises “Best Secret Holder” and keeps private photos tucked away
ios8 Now has a ‘hidden’ album

Private Me: Goes into incognito mode and hides apps and pictures

Apps to watch for:

What’s App: Owned by Facebook and lets you text, post status updates, send videos, share your location and make video and voice calls over the internet. For 16 and up, but being used by younger. Once connected, it wants access to address book.

KIK: Often linked through Instagram, another messenger. works with Android, iOS, Amazon and Microsoft. this allows communication with strangers, and has been used in high profile crimes. There is a community of bloggers where users submit photos of themselves for contests and displays users full names. It promotes in app purchases and promotes chats.

IMVU: 3D Avatar Creator & Chat: Build alter-egos, dress in sexy clothes (vulgar and exaggerated image), contains DM (direct messenger) and chat rooms. The App will ask you to take invasive surveys (which gives age & location) to earn app currency. Virtual sex is COMMON.

Whisper: Social Confessional, mostly sexual in nature with a strong reference for “hook ups”. Pictures show nearly nude photos, content can be dark, and confessions include depression, substance abuse and lies told to employers or teachers. Though it’s “anonymous” the app encourages users to exchange persona info in the “meet up section”

SnapChat: The dangers of kids truly believing that photos and stories disappear after being viewed. If profiles aren’t private, they can be friended or followed by strangers

Telegram: Creates secret chats that dissolve messages on a timer

WeChat: Sign up with your phone number, with this you have a “shake” button that lets you find other users who are shaking as well. There’s aa People nearby section to chat with local users, and you can send audio clips and albums.

Tumblr: Most popular blogging platform, but easy to find porn, includes violence, self-harm, drug use, and offensive language. posts are copied and shared- which is normally the goal, and profiles are automatically public so most create a second profile

Askfm: Q&A based website and app, encourages youngsters to talk about themselves and take selfies...

GroupMe: Has no limits for direct or group messages, and encourages users to send photos, videos and calendar links. The embedded GIF's have adult themes such as drinking and sex.

Down: Basically an app that says you are down to...

TikTok: Currently the most downloaded app, lacks privacy settings and is a sister app of musically. Children as young as 9 are exposing their identities, and opening them up for harassment.

Live Streaming Apps: Houseparty, liveme

Monkey: Fun chatting and meeting app, users are randomly matched with strangers for a video chat using snapchat to connect. They have a 10 second video chat with a stranger.. Before accepting or rejecting, age, gender, and location are given.

MeetMe: An open network to chat with anyone online. Several details are required- first AND last name, age and zip code at registration- or you can use your FB account. App wants to use location services to find closest matches wherever they go

Yubo: Tinder for Teens: swipe right or left to accept or reject profiles. if you accept you can hook up via snapchat or instagram. It's VERY easy to lie about your age, even if you enter your true age of under 13 the app will default you to 13 to let create an account. You have to share your location as well as other personal information, and it encourages you to interact with strangers.

YOLO: This is an anonymous add-on app that works in conjunction with SnapChat (user must have SnapChat to use the app). This app allows the user to provide feedback on another person's photo anonymously. Cyberbullying and inappropriate/ suggestive language are common.

Blendr: Hook-up app known for providing too much personal information. Similar to Grindr and Tinder, though it aims to be less sexual, it still uses location services, and allows you to see the faces of nearby users. The app keeps track of you throughout the day, and also who you've run into, with photos of them- when and where- providing the information to others as well. It has chat rooms, and no way to verify information provided by users, though it has a lengthy questionnaire.

Mappen: "Make Something Happen" 4+ age bracket on apple store, though creators say 13+. It requests ALL contacts in phone, collects personal information, and uses location services. Mappen shares your locations with all your friends- but they don't know if you actually know those people.

There is no way for Mappen to regulate or moderate your child's "friends" on their app. Your child can accept a request from ANYONE that wants to connect. Mappen does not verify true identities, and after they are connected it will notify them they are geographically close.

Omegle: Chat Website that puts two strangers together to either text chat or video chat. this is a very easy no fuss way to meet strangers and has "interest boxes" to filter potential chat partners. This site is filled with people looking for sexual chat, and links to porn sites.

AfterSchool: An anonymous app that lets you sign in to your high school by identifying familiar names of students and creating a fake profile name to talk poorly about others at the school.

***Fortnite:** Mild Violence. In the UK it's illegal for anyone under 12 to purchase it. The US has the same age rating of 13, and IOS gave it 12, though they don't consider it "illegal"- violence however is classified as "using whatever weapons you can find or make to fend off the monsters of the Storm and save the survivors. Damage is dealt by numbers and life bars and monsters disappear in a purple flash when defeated." With the chat ability- kids are exposed to profanity, racism,

and voice chat messages with strangers. If you hear them talk about “battle Royale” it is a huge battle with 100’s of strangers. One way to overcome that is take off the headphones and play with the sound on around you. Text chat cannot be turned off, and there are no filters. You can report or mute Those pesky “in-app” costs... from subscriptions to skins. There is no pause button at all in the game. Epic Games, shocked the industry when it announced at the start of August that it would release the app directly to consumers instead of through the official Google Play store (although it’s still available through Apple’s App Store). In addition, the Fortnite installation process requires gamers to enable installations from unknown apps. But doing so puts users at higher risk. A user would need to navigate to this setting later to disable third- party installations as it does not reset automatically. The result of these actions will be further malware infections and a higher compromise in privacy and security. There are benefits: teamwork, cooperation, and reflexes.

What can parents do?

Follow your children online. (Create those accounts)

Check unknown utilities!

Check your own location services.

Count your tags & Check-ins.

Sync your devices

Check App Store Regularly

Check age restrictions for downloads

Follow friends for duplicate accounts.

iphone Security Options:

Sync messages: Go to settings ->Messages

(Turn on read receipts on theirs!)

Send & Receive

Choose to be reached by iMessage at those numbers

*I suggest NOT checking to send as that number for confusion

Turn on your iCloud Family Account:

Sync your safari for a search history

Sync your contacts for new friends

Sync your Apps for new downloads

Sync your Updates for any updates they put on their phone

**Remember this works two ways. If you have an extra iPad or Mac this may be your best device to use rather than your daily phone.

If you do not see these options, you will need to have the Apple store put you on the same iCloud account.

Other options:

Family Share: group all iphones in the family together and set restrictions to all devices in the group (Downtime, Always Allowed Apps, App Limits and Content/ Privacy Restrictions)

Disney: Great for Wifi but doesn't work on cellular data at all. \$89 up to 250 devices. limits apps, websites, and usage. easy to install.

Bark- monthly fee \$10 or \$99 yearly. Provides alerts when concerning messages are written, easier for android then for iPhone. Watches for cyberbullying, sexting, drug related content and depression.

Gallery Guardian: Free- location with geo fencing and watches for inappropriate photos. No websites.

Android Options:

Net Nanny – Excellent web filtering, location tracking, time monitoring & ability to block apps, but does not have text/ call monitoring.

Norton Family Premier - Location Tracking, ability to block individual apps, easy to configure, but is a bit clunky and does not allow for geofencing.

Kaspersky Safe Kids – Very affordable, web filtering, screen time management & location tracking. They also have a free version with several features.

Family Link: Gives parents more control over their child's Android devices – screen time, time of day controls, and apps downloads, but also gives the child access to a Google account with an email address.

Update Location Services:

Settings, Privacy, Location.

Never or While Using. Debate: Does the app truly need to use your location?

note: the same can be said for camera, microphone, and photos.

Restrictions for phones:

Settings -> General -> Restrictions -> Create Passcode -> Create limitations

How can you stay up to date on all this?

-Set up Google alerts to your gmail account

-Watch for trending apps

-Go to the app store and look for similar apps to mentioned dangers apps

-Check out CommonSenseMedia.Com

-Cyber Safety Cop

Monitoring devices to consider:

Disney Circle	Qustodio	Avira	Net Nanny	Mspy
Nesanity	Covenant Eyes	TeenSafety Control		Web Watcher
McAfee Safe Eyes	Verity	Content Barrier		Spy Agent
Pure Sight	Mobile Watchdog	Elite Keylogger		Cyber Sitter