

Parent Technology Workshop: Cyber Safety

Part 1: Awareness and Resources

Identifying common social media:

Texting apps: Kik Messenger, ooVoo, WhatsApp

Microblogging apps and sites: Instagram, Tumblr, Twitter, Vine

Self-Destructing/Secret apps: Burn Note, Snapchat, Whisper, Yik Yak, Tango

Chatting, Meeting, Dating apps and sites: MeetMe, Omegle, Skout, Tinder

Be aware of where students can hide information

Parental controls for SmartPhones/App Lock - on desktop, laptop, and

SmartPhones (Apple and Android)

Part 2: Windows/PC Parental Controls

1. [Parental controls in Windows 7](#)
2. [Parental controls in Windows 8/8.1](#)
3. [Parental controls in Windows 10](#)
4. [Parental controls for OS \(Macs\) and How to Geek Info](#)
5. [Parental Controls on iPhone, iPad, and iPod touch](#)



WebSafety.com

Part 3: Resources:

[California Technology Assistance Project:](#)

[A Parent's Guide to Internet Safety, FBI](#)

[Where to hide photos](#)



Cyber Safety: Awareness and Resources

15 Apps and Websites Kids Are Heading to After Facebook

Social media apps that let teens do it all -- text, chat, meet people, and share their pics and videos -- often fly under parents' radars.

Apps To Watch Out For: How do you know what to look for? Here are a few apps that are considered to be the most dangerous:

Yik Yak – This app is fairly new and already being blocked by schools. It allows posters to submit up to 200 characters which can be view by their closest 500 “Yakkers,” determined by GPS tracking. It’s gaining the reputation of an app that allows you to anonymously post sexually explicit and abusive language.

Down – This app has a slogan that goes something like, “The anonymous, simple, fun way to find friends who are down for the night.” Connected with Facebook, friends are categorized in either someone they would like to hang around or someone to hook up with. Originally, this app was known as “Bang with Friends.”

Omegle – Using this app, you can video chat with someone else. Although you may remain anonymous,

it works by using your Facebook “likes” to match you with someone you don’t know but has similar “likes” as you. Because you are matched with a stranger, there is a high risk that the stranger will be a sexual predator.

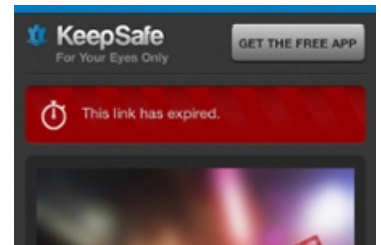
Whisper– Just two short years ago, a 12-year-old girl was raped by man she met while using this app. This app is for telling secrets, and although anonymous, it does display the area you are posting from. It’s easy for kids to begin to feel comfortable with a stranger they are confiding in and eventually give out personal information.

Kik Messenger– Kik will also your kids to send messages that you can’t see and verifying the identities of the sender or receiver is very difficult. This is a very popular app for kids under age 18, and it’s also very popular with sexual predators. For your child’s safety, it is suggested that this app be deleted from your child’s phone.

Hiding Apps

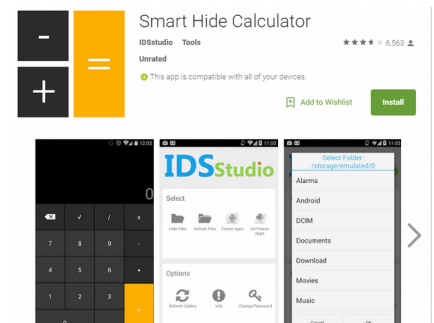
The most popular way to hide apps or any other content on your phone is by using an app that does that. Both Apple Store and Google Play have a lot of hiding apps for download and the majority of them are free.

One such app is **KeepSafe** (Android or iPhone, free). It allows you to upload pictures and videos into the app from the phone gallery and keeps them secured under a password. An interesting aspect of this app is that it has a built in feature called Safe Send. You can send a picture that will be visible for 20 seconds before self-destructing. The application developers claim that KeepSafe Safe Send is like Snapchat but works with everyone, even if they don’t have the app. The recipient receives a link via text message that takes them to the picture that the KeepSafe user sent.



Vault (or Vaulty) (Android or iPhone, free), is also a popular hiding app that allows users to hide photos, videos, text messages, contacts and apps. Just like KeepSafe, it is only accessible via password. The application is free, however if you upgrade you can have additional features such as creating a decoy Vault account. When a parent or adult insists on seeing the content of an app, teens can show them a fake app through Vault. Vault will also take a picture of any person who tries to access the Vault with the wrong password.

Hide It Pro (Android or iPhone, free) is similar to Vaulty. It allows you to hide media, and the app itself is disguised as an “Audio Manager” that seemingly controls the volume of the smartphone. The user usually has to perform a combination of tasks in order to access the content, for example, pressing and holding the app reveals a lock screen behind which users can hide messages, photos, videos, and apps.



Another category of hiding apps that parents should be aware of are **disguise apps**. **Secret Calculator** (iPhone, free), **KYMS** (iOS devices, free) and **Smart Hide Calculator** (Android, free) appear as calculators on the icon and when you open them. This is the exact description from the Google Play store:

"Smart Hide Calculator" is a fully functional calculator app but with a little twist. Once you enter the password(u get to set it on first start of app and can also be changed in future) and press the '=' button then boom you are presented to an interface where you can hide, unhide pictures, videos, documents or files with any file extension placed in a folder on sdcard, and if your device have root you can also hide (freeze) and unhide (un-freeze) apps.



(iOS fully punch in your 4-digit PIN number and the equal sign, and you have access. Along with hidden photos,



KYMS

devices, free)- When you download KYMS, the app's disguised as a calculator. When you launch the app, a functional calculator appears. All you have to do is

you can store PDFs, Word documents, Excel spreadsheets, PowerPoint presentations and text files. KYMS allows you to import media from your computer, camera roll, the web and more. It also supports Wi-Fi, so you can easily sync your collections between devices.

Poof is an app that you definitely need to be familiar with, because it allows teens to make other apps they don't want you see disappear. Although this particular app is no longer available, your child may still have it and use it. Also, similar apps are created regularly, so it's a good idea to search online periodically for newer apps with these capabilities and see if your child has downloaded any of them.

This is definitely not a complete list of apps your child may not want you to know about, but it's a start. If you see an app on your child's phone that is new to you, google to find out what it does, and if it is safe for your teen to be using.

Other ways to find hidden activity is through unexplained blanks or missing data from their smartphones. If you check your child's phone and see that they suddenly have no browser history, or there is obviously chunks missing from various text conversations, it's safe to assume they're taken steps to hide that from you. Other red-flag behaviors include...

- Hiding their screen or turning off their device when you enter the room.
- Refusing to hand over their passwords. If they have nothing to hide, there should be no issue.
- A sudden increase in media usage. New apps can be "addictive" and take up a lot of time.

While monitoring can help you discover if your teen is hiding information from you, the next step is just as important: talking to them. If you discover any of these apps on your child's phone, don't overreact. Discuss with them how these apps are being used inappropriately and the consequences. Continue to calmly talk to them about your concerns, and by doing so, your child will feel more comfortable opening up to you when they need to.

Device Settings

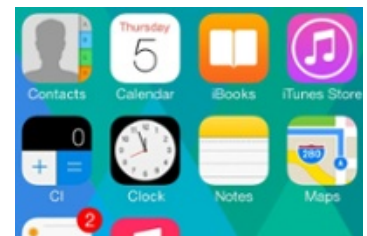
Although teens are more likely to use apps when it comes to hiding their pictures, applications, text messages, and other data on their smartphones, it is still important to know what devices offer in terms of hiding apps and content.

On the iPhone, you can hide applications by going into the Settings > General > Restrictions and checking off next to applications that you don't want to show up on the screen. To make them reappear, you can go back and repeat the process.

Androids offer the same option of hiding apps from the home screen. You can do so by going to the App Drawer > Home > Settings > Hide Applications and choosing apps that you would like to hide. Just like on the iPhone, you will have to repeat the process to unhide the apps.

From a hidden app to [social steganography](#), teenagers will always find ways to hide their pictures and messages and other content on their phones. If you find that your child is using one of these applications or similar ones to hide their activities, try not to jump directly into the "Show me what's there" request. First, by doing so, you will be pushing your child away and they will be less likely to open up to you. Second, as we mentioned earlier, a lot of apps have a decoy mode and your child might show you an account with curated data, created especially for situations like this.

As a precaution, parents can keep tabs on teens and tweens' digital activities by using parental intelligence tool uKnowKids to ensure that kids aren't hiding things that could get them into trouble.



Helpful article: [Calculator or Hidden App? Teens Are Disguising Content With Apps](#)