

How To Keep Your Teen Safe On Mobile Devices



HELPLYOURTEENNOW

Table of Contents

Are You Keeping Up With Your Teen & Mobile Technology?

[How much time does your child spend in front of mobile screens?](#)

[Mobile devices give today's teens unprecedented access to dangerous activities](#)

What You Can Do To Protect Your Teen

[General Guidelines](#)

[Tips For Dealing With Common Dangers](#)

How To Protect Your Teen On Specific Apps

[The Big Four](#)

[Apps On The Rise With Teens](#)

Should You Monitor Your Teen's Online Activity?

[Are Monitoring Or Geolocation Apps A Good Idea?](#)

[Examples of Monitoring Apps](#)

[How To Set Security Settings On Your Child's Mobile Device](#)

More Resources For Parents

[Child Safety On The Internet](#)

[Studies About Teens & The Internet](#)

[Talking To Your Kids About The Internet](#)

Are You Keeping Up With Your Teen & Mobile Technology?

Today the world is changing at a rapid pace. With ongoing innovations in every area of our lives, it can be a challenge to keep up-to-date on all the new technology. As wave after wave of new devices and applications come in, you may feel at best overwhelmed or even like you could get left behind. However, it's extremely important that we keep children safe online and with mobile devices because with new frontiers come new dangers.

Numerous studies reveal the frightening threats to today's online teens. Parents believe they are in control when it comes to monitoring their teen's online behaviors. However, these studies show that many parents know very little about what their children are doing online -- particularly with their mobile phones.

How much time does your child spend in front of mobile screens?

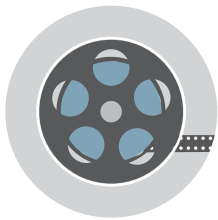
Studies vary wildly on how much screen time teens indulge in, particularly by country. However, a recent global study of 32 different countries found that teens spend about three hours on the mobile web per day.

A British study found that a child born in 2014 can expect to spend an entire year of his life -- that's 365 days for 24 hours a day -- in front of a screen by the age of seven

Another study found that people check their mobile devices on average over 200 times per day.

Mobile devices give today's teens unprecedented access to dangerous activities

The internet and its endless wealth of information can be a blessing or a curse. Teens often haven't developed the judgmental skills necessary to prevent them from making poor decisions that can negatively affect their entire future -- personally, academically, professionally, and even physically. Here are some of the most common and damaging behaviors teens exhibit online.



Pirating movies and music

An Australian study in 2014 found that **36% of adolescents admit to digital piracy**. In the US, *criminal and civil penalties can be steep:*

- Up to 5 years in prison and/or \$250,000 in fines
- Copyright holders can sue for up to \$150,000 for each work



Hacking email or social accounts

- If your child gives away an email or social media password to friends, *they can be vulnerable to being pranked, humiliated, or worse.*
- On the other hand, if your teen is engaged in hacking, they can be charged with a **misdemeanor or even a felony**.
- In a case last year, several teens hacked video games and military helicopter training software valued at **\$100 - \$200 million and face up to five years in prison.**



Oversharing

There are obvious physical dangers to revealing private information online. Unfortunately, many kids either *don't realize it or don't care:*

- **50%** of teens have posted their email address publicly online
- **30%** have posted their phone number
- **14%** of teens have publicly posted their home address

What's more, there are reputation ramifications to teens posting embarrassing confessions or compromising photographs -- which can haunt your child well into adulthood thanks to the permanence of the internet.



Cheating

With instant access to vast amounts of information makes it extremely easy for teens to cheat on their schoolwork, jeopardizing their academic and professional futures. According to a 2012 McAfee study:

- **48%** of teens found answers to tests online
- **22%** of teens admitted to cheating on a test with their phones or other online access
- **Only 5%** of parents were aware that their children were cheating on tests



Cyberbullying

Even though bullying is more common in person, mobile technology means that bullies today aren't restricted to the schoolyard. Your child could be the victim of cyberbullying -- or they might even be engaged in cyberbullying others.

- **25%** of school children say they've been a victim of cyberbullying
- **16%** of kids admitted that they had cyberbullied others
- **62%** of teens say they've witnessed cruelty online

In terms of bullying risk, over half of teens who have social media accounts say they've experienced negative situations.

- Girls are more likely to be victims or offenders of cyberbullying than boys.
- Warning signs for cyberbullying include self-esteem issues, suicidal thoughts, issues at school, antisocial behavior, drug/alcohol abuse, and other emotional and psychological problems.
- “Traditional” (in-person) bullying is correlated with cyberbullying, which means if a child experiences the former, they are likely to experience the latter and vice versa.



XXX

Pornography

The ability to easily access sexually explicit images on mobile phones means that your teen may be watching pornography -- or even participating in it -- without your knowledge. You may not think your teen is watching pornography (only 12% of parents believe their teen is accessing pornography online) but...

- **32%** of teens admit to intentionally accessing online porn
- **43%** of teens who watch pornography do it on a weekly basis or more often
- Pornography can have devastating effects on the teenage brain

In addition to watching professional pornography, many teens also engage in **“sexting”** each other. Sexting involves sending text or email messages containing pornographic images of oneself or receiving those types of messages from others..

- **38%** of teens confess to sending naked pictures of themselves to others
- **31%** admitted asking others to send them a sext

What You Can Do To Protect Your Teen

General guidelines

You may feel intimidated at the prospect of having to learn about other social networks but there are some general guidelines that can help you protect your teen without having to become a technical wizard overnight. You can remember these tips for protecting your teen on social media and other mobile apps can be remembered with the acronym “**RESPECT**”:

Reputation. Make sure your teen is aware that what they post online doesn’t have an expiration date and explain how these things can impact their future reputation.

Educate yourself. Inspect the sites/apps your teen likes to use. Read the Features, FAQs, About Us, and the Safety Center for these apps.

Signs of depression. Keep an eye out for signs of depression from cyberbullying.

Password access. Require your teens to give you their passwords for all the sites they use and check them regularly. Be sure to explain why they should give you their passwords but to **NEVER** share them with *anyone else*.

Communication. Welcome your teen’s candid questions so they can trust you with any awkward or distressing concerns.

Tighten privacy. With your teen, visit each app’s privacy settings and talk them through the settings that you feel are safest.



Tips For Dealing with Common Dangers

Pirating movies and music

- Explain how copyrights work and the ramifications to their favorite entertainers if their work is stolen. You can also explain that *legal and financial penalties* can be applied to both your teen and yourself.
- Work with your teen to find a financially acceptable way of meeting their entertainment needs. For example, Amazon offers unlimited music streaming to Prime members, Pandora and Spotify offer subscription music services, and Netflix subscriptions allow for unlimited online streaming of TV and movies.

Dealing with Hacking

- Explain that *hacking isn't a victimless crime* that's just about the thrill of overcoming a difficult challenge. Very few hacking attempts can be masked when going up against internet security firms. Your teen should be aware of the financial and legal ramifications of tampering with someone else's accounts or with school, corporate, or government sites.

Dealing with Oversharing

- A McAfee study showed that 45% of all teens will change their behavior if they know you are watching, so talk to them about what your family values are around privacy. Explain the difference between sharing their personal information versus hitting the "Like" button on a friend's post.
- Make a list of *personally identifiable information (PII)* that your teen should never post on any site whatsoever. The PII list should include things like **birthdays, social security numbers, phone numbers, addresses (home, school, or elsewhere), their current location, or their family's full names.**

- **Turn off location tracking** on your child's social media apps so that their whereabouts aren't automatically shared.

Dealing with Cheating

- **Have a talk with your teen about the definition of cheating** -- sometimes kids just aren't aware that their behavior is wrong. Be crystal clear about which acts constitute cheating -- e.g., copying from others, giving answers to others, using the internet to look up test answers, taking photos of tests (even blank ones) to share with others, etc. Also, help your child understand what plagiarism is and why it's wrong.
- **Check your teen's phone if you suspect cheating:**

- ☐ Oftentimes evidence shows up in the form of text messages to or from other students containing answers to test or homework questions.
- ☐ In addition to checking SMS text messages, also check messaging apps like WhatsApp, Facebook chats, Google Hangouts, Viber, Skype chats, or WeChat.
- ☐ Check the phone's photo gallery for photos of tests or homework.
- ☐ If your kid's phone has note-taking apps, be sure to check them too -- e.g., the iPhone Notes app, Evernote, Google Docs, Google Keep, Papyrus, and OneNote.
- ☐ Ask your child to show you any locked apps on their phone. (Locking apps like Smart AppLock allow your child to create passwords for each app on the phone.)
- ☐ Lastly, check your teen's phone, laptop, computer, or cloud drives for suspicious file names. The most popular cloud storage apps include: Dropbox, Google Drive, OneDrive, Box, Copy, iDrive, and Amazon Cloud Drive.

Dealing with Cyberbullying

- As a parent, arm yourself with information now. You should know the signs of cyberbullying and have a strategy for stopping it well before (or if) it's ever a problem. Consult a trusted online source like the [Connect Safely Cyberbullying Resource Center](#)
- Tell kids it's ***not their fault*** and instruct them not to respond, but to ***save any evidence in the form of screenshots, text, email or voicemail messages***.
- You should take your child's story quite seriously and respond appropriately.

Dealing with Pornography

- If you find out your teen has accessed online pornography, ***make sure you understand what happened before reacting***. In some cases, a teen might have accidentally wound up on a pornography site with a mistyped Google search or curiosity about a spam email resulted in a one-time click. Assess if the situation is a habit or an obsession by observing behavior changes. Then, have an open talk about the topic with your kid at a time and place where they feel safe discussing it.
- Talk with your kids about the risks of sexting. Not only could their pictures end up in the hands of people they don't know, but in some cases they could also ***face legal ramifications related to underage pornography***.

How To Protect Your Teen On Specific Apps

The best way to know what your teen may be doing on their phone is to pay attention to the apps and sites they use -- and what they use them for. Make sure that you keep up-to-date on the new features of each of these apps since they may affect how your teen uses the site. Here are some of the most popular apps with teens and specific advice for dealing with each one.

The Big Four

Not only have you probably heard of these sites, you might use them yourself. Most teens also have accounts on these sites. Make sure you familiarize yourself with the Safety Center for each of these sites.



Facebook

 **Safety Center** <https://www.facebook.com/safety>

Not only have you probably heard of these sites, you might use them yourself. Most teens also have accounts on these sites. Make sure you familiarize yourself with the Safety Center for each of these sites.

 **Watch out for**

oversharing, cyberbullying, sexting, stalking, and identity theft.



Twitter

 **Safety Center** <https://support.twitter.com/groups/57-safety-security>

Teens may think that since Twitter is limited to 140 characters that there's not much trouble they can get into. Unfortunately, they're wrong. Twitter posts can easily link out to dangerous sites and pictures can be shared for sexting. Instruct teens not to DM (direct message) people they don't know.

 **Watch out for**

sexting, identity theft, oversharing, cyberbullying, and stalking.



Instagram

 **Safety Center** <https://help.instagram.com/285881641526716/>

Instagram is equipped with good privacy settings for keeping out people your teen doesn't know -- make sure they take advantage of those strict privacy settings. Also, it's a good idea to turn off location tagging so that your teen's exact whereabouts aren't known. Instagram recently introduced a DM (direct messaging) feature so instruct your child not to accept messages from unknown Instagrammers.

Watch out for

Sexting, oversharing, low self-esteem issues from lack of "Likes", stalking, and cyberbullying



Pinterest

 **Cyberbullying Center**

<https://help.pinterest.com/en/articles/harassment-and-cyberbullying>

 **Pinterest Privacy Help**

<https://help.pinterest.com/en/articles/change-your-privacy-settings>

Pinterest allows pinners to block specific people from interacting with your teen or even seeing their pins, as well as a way to report harassers. Pinterest allows pinners to create "secret boards" so that only those you invite may see your pins.

Watch out for


pornography, oversharing, and self-esteem/body image issues.


Apps On The Rise With Teens

In a typically rebellious fashion, today's teens are leaving the "Big Four" sites in favor of newer sites that are less popular with their parents. Here are some of the most popular apps with today's teens.

Chatroulette

 **Safety Center** NONE

 **What it is** Chatroulette is a free online chat website that pairs random people from around the world together for webcam-based conversations. Visitors to the website begin an online chat (text, audio, and video) with another visitor.


 **Warning** As soon as you load the Chatroulette website, your "chats" will start which includes video from your webcam and a text chat box. No login is required and due to the anonymous nature of Chatroulette, exposure to live pornography is not only possible but highly likely.


 **Watch out for** oversharing, cyberbullying, sexting, stalking, and identity theft.

Other sites that match up anonymous strangers, similar to Chatroulette: Omegle, Zumbl, Tinchat, Whisper, PostSecret.

GroupMe

 **Safety Center** NONE

 **What it is** GroupMe is a private chat room for multiple people to share to several people at once, where everyone can see what others are typing. Pictures can also be shared.

 **Watch out for** sexual predators, oversharing, cyberbullying, sexting, stalking, low self-esteem issues (from not being invited to a group), and identity theft.

Kik



Safety Center

<https://kikinteractive.zendesk.com/entries/40268633-Safety-Tips-for-Kik-and-all-your-fave-apps->



What it is

An instant messaging client that allows users to send free text messages (using Wi-Fi instead of their SMS phone network) as well as photos and web pages. In addition to people they know, your teen could also communicate with strangers on Kik and even company brands.



Watch out for

sexual predators, oversharing, cyberbullying, sexting, pornography, stalking, and identity theft.

Pheed



Safety Center

NONE



What it is

Pheed is a way to share any type of content in one place: voice notes, text, photos, videos, music or even live broadcasts. Pheed users may rate their sites to conform to the movie rating system: G, PG, PG-13, or R, so that, in theory, parents can restrict a child's access to only suitably-rated channels. However, it's fairly easy for your teen to change the rating restriction whenever they like. Also, be aware that some Pheed channels cost money to view.



Watch out for

sexual predators, oversharing, cyberbullying, sexting, pornography, stalking, and identity theft.

Tinder -- and other location matching dating apps



Safety Center

<https://www.gotinder.com/safety>



What it is

Tinder uses your location (via GPS) to match you up with people located near you for dating opportunities. It scrapes information from your Facebook profile and attempts to find others near you with compatible Facebook interests. It offers a chat feature for matched users and lets them swap time-limited photos (similar to Snapchat). There are numerous perils involved with online dating apps like Tinder.

Watch out for

sexual predators, oversharing, sexting, pornography, and stalking.

Other sites that match up anonymous strangers, similar to Tinder: Scout, Cuddlr, Grindr.

Snapchat

Safety Center

<https://www.snapchat.com/safety>

What it is

Snapchat is a photo/video sharing site which claims that shared pictures “disappear” after a time limit that the user sets between 1-10 seconds. Users take “Snaps” (photos, record videos, add text and drawings), and send them to a controlled list of recipients. Users set a time limit for how long recipients can view their Snaps, after which they will be hidden from the recipient’s device and deleted from Snapchat’s servers. However, there are many ways to capture the images permanently -- the easiest of which is to take a screenshot of the image. Additionally, there are third-party apps for Snapchat that can enable recipients to save Snaps on their device. Snapchat includes functionality that will warn the sender if the receiver is using any of these unsanctioned apps and says it will block repeated offenders of this policy.

Watch out for

sexual predators, oversharing, cyberbullying, sexting, pornography, and stalking.

Tumblr

Safety Center

NONE. However they have a list of Community Guidelines.

What it is

Tumblr is a microblogging site -- which means it’s like a blog but posts are usually much shorter. You can make your Tumblr private or public. Treat Tumblr like you’d treat any blogging platform like Wordpress or Blogger.

Watch out for

oversharing, cyberbullying, sexting, pornography, stalking, and identity theft.

Vine

Safety Center

<https://support.twitter.com/groups/57-safety-security>

What it is

Vine allows users to share 6 seconds of looping video clips. Instruct teens not to DM (direct message) Vines with people they don't know. It will block repeated offenders of this policy.

Watch out for

sexual predators, sexting, identity theft, oversharing, cyberbullying, and stalking.

YikYak

Safety Center

NONE

What it is

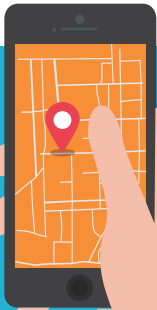
YikYak is similar to Chatroulette in that it pairs random people together -- except that YikYak is only for messages, not video. However, one significant difference with YikYak is that it pairs people based on their proximity to each other, usually within a 10-mile radius. This location matching makes YikYak an especially dangerous site for children.

Watch out for

sexual predators, oversharing, cyberbullying, sexting, pornography, stalking, and identity theft.

Should You Monitor Your Teen's Online Activity?

It's tempting to believe that you can protect your teen from harm by monitoring everything they do online. Tech-savvy parents can have a false sense of security thinking they can spot all the digital footprints of a kid's activity. Unfortunately, even the most informed parents can be fooled. According to [McAfee's Digital Divide Study](#), kids are adept at developing workarounds like clearing their browser history, deleting IMs, lying about online activities, private browsing modes, and even creating email addresses and social network profiles their parents don't know about.



Are Monitoring Or Geolocation Apps A Good Idea?

[Experts are divided](#) on the answer to this question. On the one hand, teens are at the age where they are eager to prove they are trustworthy and to get rewarded with independence. Installing monitoring software can send a message to your kid that you don't trust them, which can inhibit them from communicating with you if they ever do need your help.

On the other hand, it's possible that well-timed parental intervention can protect teens from potentially life-threatening situations, such as the case with cyberbullying, predators, or suicide.

To make matters even more complicated, third-party monitoring apps can collect a large amount of private information on your child that you are entrusting them (and their employees) to handle properly. If you do go with a monitoring app, make sure you are completely satisfied with its privacy policy and methods of handling personally identifiable information.

Examples of Monitoring Apps

Moment [iOS only]

Moment tracks minutes used for iPhones and iPads for each family member. Parents can set time limits for screen time and even lock out devices for certain time periods so you can be with each other instead of your phones, for example, at dinner time.

My Mobile Watchdog [iOS and Android]

My Mobile Watchdog allows you to monitor your teen's text messages, block apps (of your choosing), set time limitations on when and how long an app can be used, and it also tracks your child's location by GPS. It can inform you when inappropriate content is received or sent from your teen's phone.

TeenSafe [iOS and Android]

TeenSafe allows you to see your teen's activity on Facebook and Instagram. You can also see text messages, location information, phone logs, and web browsing history. The monitoring dashboard is only available to you. (Your teen can't access the TeenSafe dashboard.) On iPhones the app is undetectable to your child.

NetSanity [iOS only]

NetSanity can block out specific times for app usage (e.g., lock down everything at bedtime), block specific websites and apps, and can even block content types across all apps. You can control the app's dashboard from any browser -- mobile or desktop.



How To Set Security Settings On Your Child's Mobile Device

Most phones come equipped with a few ways to set up restrictions for your teens and their phone usage.

iOS for iPhone & iPad Parental Restriction Settings

- 1 Settings > General
- 2 Restrictions > Enable Restrictions
- 3 Create a parental passcode
- 4 Go through each setting type to enable the type of restrictions you'd like to put on your child's phone. The settings allow you to customize which apps and content types the phone is allowed to access. You can also prevent your teen from changing the privacy settings on specific apps (e.g., Facebook) after you've set them up.

Android Tablet Parental Controls

[For Android 4.3 Jelly Bean or later.]
For Android phones, skip to the next set of instructions.

- 1 Pull down the top menu and tap Settings
- 2 Users
- 3 Add user or profile
- 4 Create a restricted profile

[Next page >>](#)

- 5 Enter a parental PIN (If you already have a PIN you won't see this step.)
- 6 Tap the Settings icon next to New Profile and give it a name (e.g., Teen)
- 7 Go through the list of apps and toggle off the apps you'd like to restrict.
- 8 Location sharing defaults to "OFF" unless it's been turned on by your child.
- 9 You can also restrict access to the Google Play Store to prevent unauthorized purchases from your child's phone.
 - a Launch the Play Store
 - b Tap the menu and select Settings
 - c Enable the feature called "Password – Use password to restrict purchases"
 - d Enter the password for your Google account

Android Phone Parental Controls

[For Android 5.0 Lollipop you have the options of limiting SMS & voice calls only. Additionally, earlier versions of Android don't have parental controls. In addition, some phones running Android 5.0 or newer still do not have the ability to create multiple users]

For Android tablets, see the previous set of instructions.

- 1 Tap the Profile icon (a white circle) in the notification bar
- 2 The Users menu appears
- 3 Tap Add User > OK
- 4 Tap Set Up Now
- 5 Tap the gear icon next to the User Name you just created
- 6 Slide the selector to the right to disallow SMS and phone calls

[Next page >>](#)

- 7 You can also restrict access to the Google Play Store to prevent unauthorized purchases from your child's phone.
 - a Launch the Play Store
 - b Tap the menu and select Settings
 - c Enable the feature called "Password – Use password to restrict purchases"
 - d Enter the password for your Google account

Amazon Fire Phone Parental Controls

[For Amazon Fire tablets see below.]

- 1 From Settings > Applications & Parental Controls.
- 2 Enable Parental Controls.
- 3 Toggle the parental controls ON.
- 4 Enter a password, confirm your password again, and then tap Submit.
- 5 From here you can restrict almost anything about your child's phone, including: browsing, email, social sharing, the camera, and purchases.

Amazon Fire Tablet Parental Controls

[For Amazon Fire phones, see above.]

- 1 Swipe down from the top of the screen to show Quick Settings, and then tap More.
- 2 Toggle the parental controls ON.
- 3 Enter a password, confirm your password, and then tap Finish.
- 4 From here you can restrict almost anything about the tablet, including: browsing, email, social sharing, the camera, and purchases.

More Resources For Parents

Child Safety On The Internet

- [FBI Publications: A Parent's Guide to Internet Safety](#)
- [Common Sense Media](#)
- [UKnowKids](#)
- [Connect Safely](#)
- [Cyberbullying Research Center](#)
- [NetSmartz Workshop](#)
- [ProtectKids](#)
- [Family Online Safety Institute](#)
- [YourSphere](#)

Studies About Teens & The Internet

- [McAfee's Digital Divide Study](#)
- [GWI Audience Report: Teens Q1 2015](#)
- [Global Ranking Of Social Networks](#)

Talking To Your Kids About The Internet

- [American Academy of Pediatrics](#)
- [Parent/Teen Phone Rights Agreement](#)
- [Information about parental monitoring apps](#)
- [Dealing With Sexting](#)



HELPHYOURTEENNOW