How to Monitor your Child's Social Media

PRESENTED BY

SHARPER TRAINING SOLUTIONS, INC

WWW.STSICO.COM

Agenda

- Why Monitor?
- Dos and Don’ts
- Parental Controls
- Tracking Apps and Software
- Helpful Tips

What Does Monitoring Mean?

The internet can be a fantastic tool for your child's education and entertainment, but it also presents numerous risks. More parents are recognizing the web's potential dangers—which is the first step toward averting them. According to a national poll, adults named cyber safety as one of the top health issues kids face today, ranking it just below drug abuse
www.safewise.com/blog/internet-safety-for-kids/

- Monitoring means establishing firm guidelines and limits for your child to keep track of what is going on in his or her social media world.

- Monitoring also means establishing clear expectations about what your child should always tell you AND that they can always talk to you about the things going on in their life.

- But now, the majority of browsing and online activity happens on smartphones and other mobile devices, which makes monitoring your kids' online presence much more complicated. May want to "track"

Why Monitor?

- Do you know where your kids are each day, whom they're with, and what they're doing?
- How about in the digital world? Do you know where your children are spending most of their time when online?
- The American Academy of Pediatrics (AAP) recently released findings from a comprehensive study on the impact social media has on kids and families. Although there are real benefits to kids using sites like Facebook, including increased communication, access to information and help in developing a sense of self, there can be serious downsides to all this online sharing too.
- In addition to stranger danger, Kids may say things to each other online that they'd never say in person. This can lead to toxic gossip, cyberbullying, and damaged reputations. Children may also think the words and images posted online are fleeting, but they can be saved and forwarded and seen by practically anyone, and can linger for years. Words typed in a text message that seem innocuous and impermanent can actually be life-changing.

Trust But Verify

- Yes, you want to trust your kids. But they're kids -- relying on their word may not be enough to keep them safe
- Your honesty has its perks: If they know you're watching, their self-monitoring instinct will likely kick in. One of the best things you can do: Put the computer in a central location. There's no better way to keep an eye on things than to be able to wander by and casually say, "Hey, what website is that?"
- If your kids don't know you'll be monitoring their online use and you find something and go "Gotcha!" they'll be shocked and probably resentful, and may start hiding things from you.
- So ask questions: Who are they communicating with? Which websites did they visit today? Try to keep your conversations positive -- or at least neutral! If your only message is "You're on the computer too much" or "Don't look at that website," it becomes a point of tension, and kids won't come to you when they see things online that upset or confuse them.
- Then do regular checks to be sure you get the whole truth: Learn to use your browser's history function (keep reading) to see which sites have been visited recently and what's been downloaded.

Dos and Don’ts For Your Children

- **Do** let your parents know right away if you receive a message from a stranger.
- **Do** keep your passwords a secret. Never give them to anyone other than your parents.
- **Do** ask your parents before creating a social media account or downloading an app.
- **Do** ask your parents before posting pictures of yourself or others online.

- **Don’t** give out personal information such as your birthday, school name, or address. Including sharing pictures with this information
- **Don’t** bully, and tell your parents if someone bullies you.
- **Don’t** meet someone in person who you “met” online.
- **Don’t** accept friend requests from people you don’t know.

PARENTAL CONTROLS

Parental controls are features which may be included in digital television services, computer and video games, mobile devices and software that allow parents to restrict the access of content to their children.

Content filters were the first popular type of **parental controls** to limit access to Internet content.

Setting up parental controls can be very beneficial for your family. It gives you the ability to manage how your children use the computer and their devices. This will give you a peace of mind that they're staying safe online.

Where can you find parental controls?

Computers

Smartphones

Tablets

E-readers

TVs

Video Games

Computer/Internet Safety & Browser History

- Talk to Your Child About Internet Safety -
  It's a good idea to speak to your children about the importance of protecting themselves online, letting them know why you don't want them visiting certain websites and explaining what kind of behavior is appropriate on social networks.
- You may need to check on what websites your child is visiting on the Internet. Monitoring your children's online activity is a great way to become aware of any dangers that they might be exposed to.
- However, the most basic way to find out what sites your child has been visiting is to check the browser history. All internet browsers save a record of the sites that have been visited.
- Go to your Internet browser's Settings, then History –will give you a chronological list of all sites visited.
- Warning: Kids can learn how to delete the history to cover their tracks, so ask questions if you discover that the history was cleared by someone other than you.
- *Checking Browser History can also be done on the Internet App on their mobile devices

Where to find Parental Controls

- Your Internet Browser – Google's Chrome etc
- Your Anti-Virus provider – Norton, etc
- Your cell phone company – Verizon, T-Mobile etc
- Apps for your device - App Store, Google Play , Windows Store

More than Browsing History

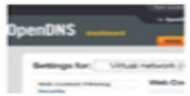
- You may need to do more than check the browser history

Options:

- Limit amount of time – most smart phones today have this feature
- Content filtering - most smart phones today have this feature
- Access site scheduling – Wifi router settings
- Monitor Social Media – need an app for this feature

Category type	Parental Control Device	Parental Control Device	Router	Router	DNS Service	DNS Service
Company name	**Circle with Disney**	**KoalaSafe**	**Luma**	**Torch**	**SafeDNS Safe@Home**	**OpenDNS Home**
View product	View on Amazon	View on Amazon	View on Amazon	View on Amazon	View on Amazon	View on Website
Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review
Equipment price	$99	$99	$149	$249.99	$0	$0
Recurring fee	$9.99/month for Circle Go	None	None	$9.99/month	$19.95/year	None
Daily time limit	✓	✗	✓	✗	✗	✗
Daily schedule	✓	✓	✓	✓	✓	✗
Content filtering	✓	✓	✓	✓	✓	✓
Internet pausing	✓	✓	✓	✓	✗	✗

Internet Parental Controls

Product	Qustodio	Net Nanny	Symantec Norton Family Premier	Kaspersky Safe Kids	Circle With Disney	Clean Router	Mobicip	SafeDNS	OpenDNS Home VIP	uKnowKids Premier
	Qustodio	Net Nanny	Norton by Symantec							
Lowest Price	$49.95 Qustodio	$39.99 ContentWatch	$49.99 Norton	$14.99 Kaspersky Lab	$78.99 Amazon	$29.99 Amazon	$39.99 Mobicip	$19.95 Amazon	$19.95 MSRP	$100.00 MSRP
	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT		
Editors' Rating	●●●●◐ EDITORS' CHOICE	●●●◐○	●●●◐○	●●●●○	●●●◐○	●●●◐○	●●●◐○	●●●○○	●●●◐○	●●●◐○
Limit on Children / Devices	5 / 5	1 / 1	None	None	None	None	5 / None	None	None	4 / 8
Per-User Settings	✓	✓	✓	✓	✓	—	✓	—	—	✓
Content Filtering	✓	✓	✓	✓	✓	✓	✓	✓	✓	—
Filter HTTPS Sites	✓	✓	—	✓	✓	✓	✓	—	—	—
Access Scheduling	✓	✓	✓	✓	—	✓	✓	✓	—	—
Social Network Monitoring	✓	✓	✓	✓	—	—	—	—	—	✓
Remote Management	✓	✓	✓	✓	—	—	✓	—	—	✓

FREE APPS FOR PARENTAL CONTROLS

- **Qustodio** - A full suite of parental control tools to keep your kids safe online. Their free version is one of the most comprehensive parental control apps around, enabling you to set rules and time schedules, block pornography and other unsuitable content. If you go for the paid-for version, you'll also get SMS (text) monitoring, social media features and per-app controls.
- FamilyShield is a free service from OpenDNS. Its parental control tools automatically block domains that OpenDNS has flagged under the headings "tasteless, proxy/anonymizer, sexuality, or pornography". One of the big pluses here is that while FamilyShield can run on PCs and mobile devices, you can also apply it to your network router and filter all the traffic that passes through the router – it's just a matter of changing the DNS server numbers in your control panel. This has the happy benefit of improving DNS lookup speeds on some ISPs. By filtering everything at the router level, every device on your network benefits from the filters. However, the router level will affect everyone in the home going online.

Continued

- KidLogger - This free parental control software not only tracks what your children type and which websites they visit – it also keeps a record of which programs they use and any screengrabs they take. If you're concerned about who your kids might be talking to online, there's even a voice-activated sound recorder. If your children are a little older and more responsible, you can pick and choose which options to monitor and give them a little privacy. The free software only covers one device and lacks some of the sneakier features of the premium editions (including silent monitoring of WhatsApp conversations and the ability to listen to Skype calls), but it's still a well-rounded tool if you're concerned about your kids' safety.
- Spyrix Keylogger - Keyloggers have something of a bad reputation online, as they're often used by crooks hoping to capture passwords and bank details, but they can be a force for good too, and Spyrix Free Keylogger enables you to see what your children have been up to. Although it's dubbed parental control software, the free version of Spyrix really a monitoring program; it doesn't stop the kids getting up to no good, but it does let you see exactly what they've done. The absence of filtering means Spyrix might not be the best choice for younger kids' computers, but it may be useful for older children if you suspect online bullying or other unpleasantness.

How to Monitor/Track

- **All-Seeing Software -** monitoring software falls into two categories:
- Blocking software lets parents create a list of approved websites and block all others. Attempts to visit unapproved sites are recorded, and some programs will message you if that happens. You can also restrict when and for how long the computer can be used.
  - Net Nanny (about $40) is a good place to start for parents of young kids.
- Recording software records all data that's sent, received, downloaded, and viewed. Also takes periodic snapshots of the screen. Don't have time to view all that data? You can flag keywords (like profanity or sex-related words) and get alerts if they're used.
  - eBlaster (about $100) is a popular choice.
  - An advanced program, such as WebWatcher (about $100), offers both blocking and recording, and lets you watch your kid's computer activity in real time from a remote computer.
- PLEASE NOTE – Some apps are free – Some apps may not be available in both iOS or Android devices.

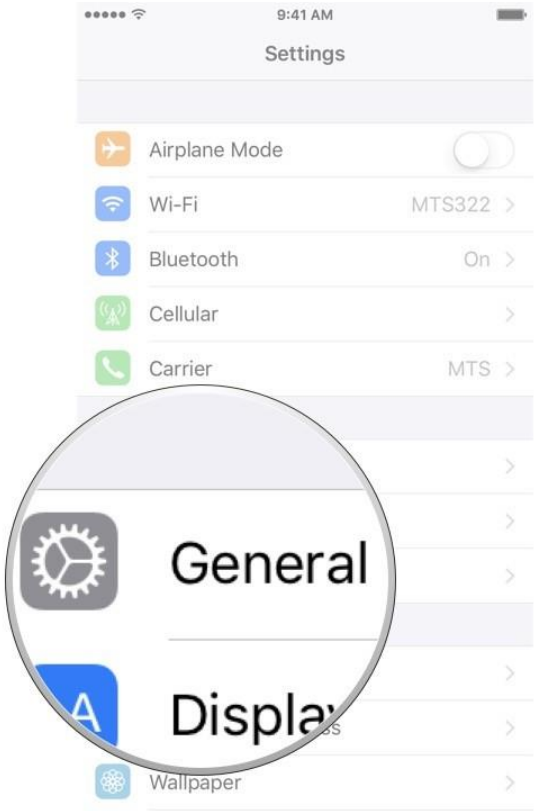
Parental Controls on Devices Younger Children

- iPad/iPhone - how to set up parental controls on your child's iPhone, iPod Touch, or iPad”
  - For Older Devices: To enable restrictions tap the settings app on your iOS device, choose "General", and then touch "Restrictions“. On the "Restrictions" page, choose "Enable Restrictions". You will now be prompted to set a PIN number that you will need to remember and keep from your kids. This PIN number will be used for any future changes you want to make to the restrictions that you have set.
  - For iOS 12: Go to Settings, then *Screen Time* - The first time you open Screen Time, you’ll see a splash screen with the option to ***Set up as a Parent***, tap that and follow the prompts to add restrictions by customizing Downtime, App Limits, Content & Privacy, and creating your Parent Passcode.

    If you’d like to make any adjustments, you can always return to ***Settings*** → ***Screen Time***

- Android – this link will provide several options for setting up parent controls for Android Devices https://www.lifewire.com/childproof-android-4137048

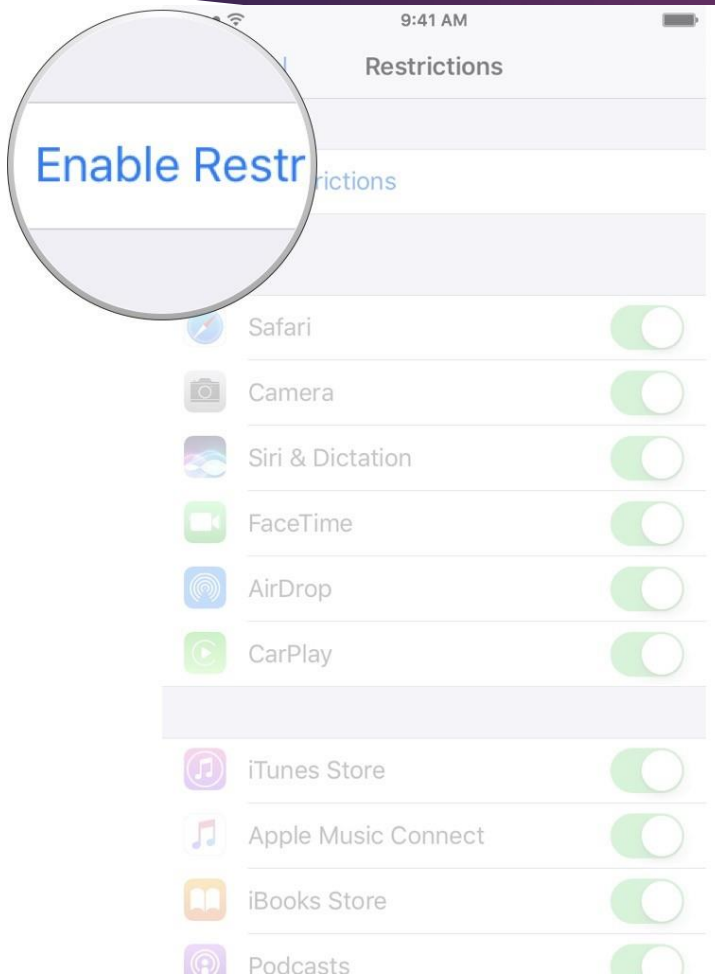
Parental Controls – iPhone/iPad (older iOS)

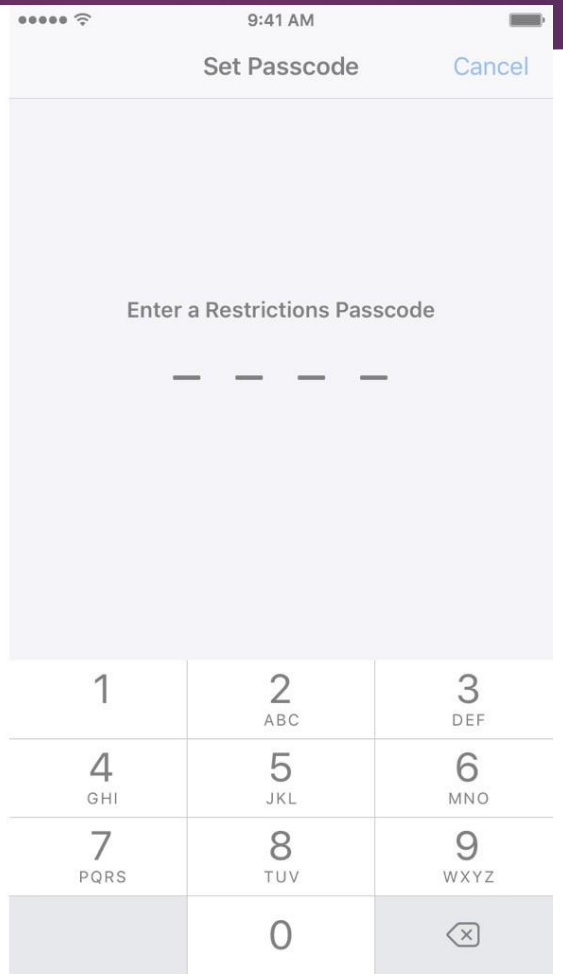


1.Launch the **Settings app** on your iPhone or iPad.

2.Tap on **General**.

3.Tap on **Restrictions**.

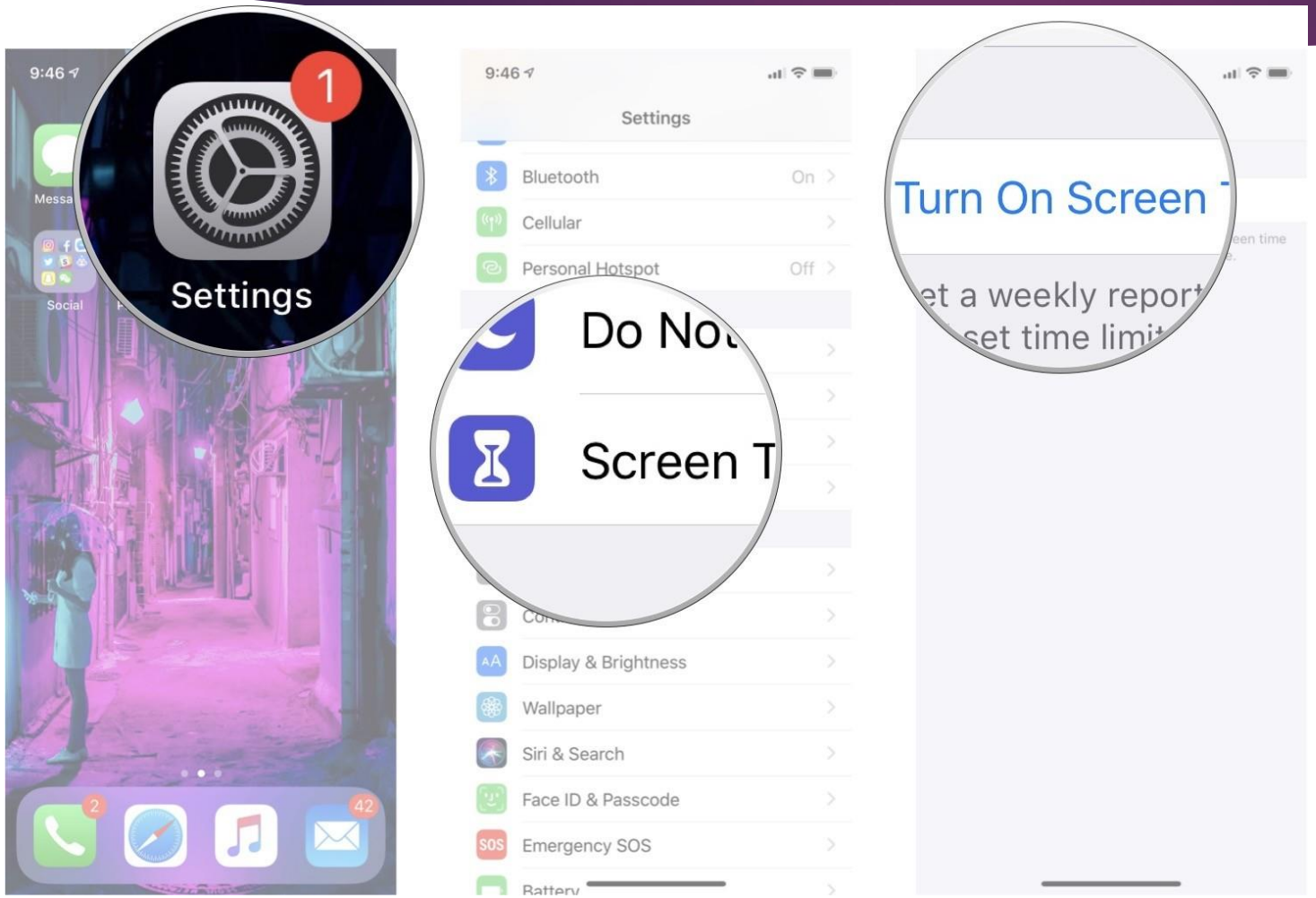




4. Tap on **Enable Restrictions**.

5. Type in a **passcode**. You'll remember for when you need to disable restrictions again. (This can and should be completely different from your Lock screen passcode.) Make sure you note it down somewhere — if you forget the passcode, you'll have to erase your device and set it up from scratch.

Parental Controls – iPhone/iPad NEW iOS12

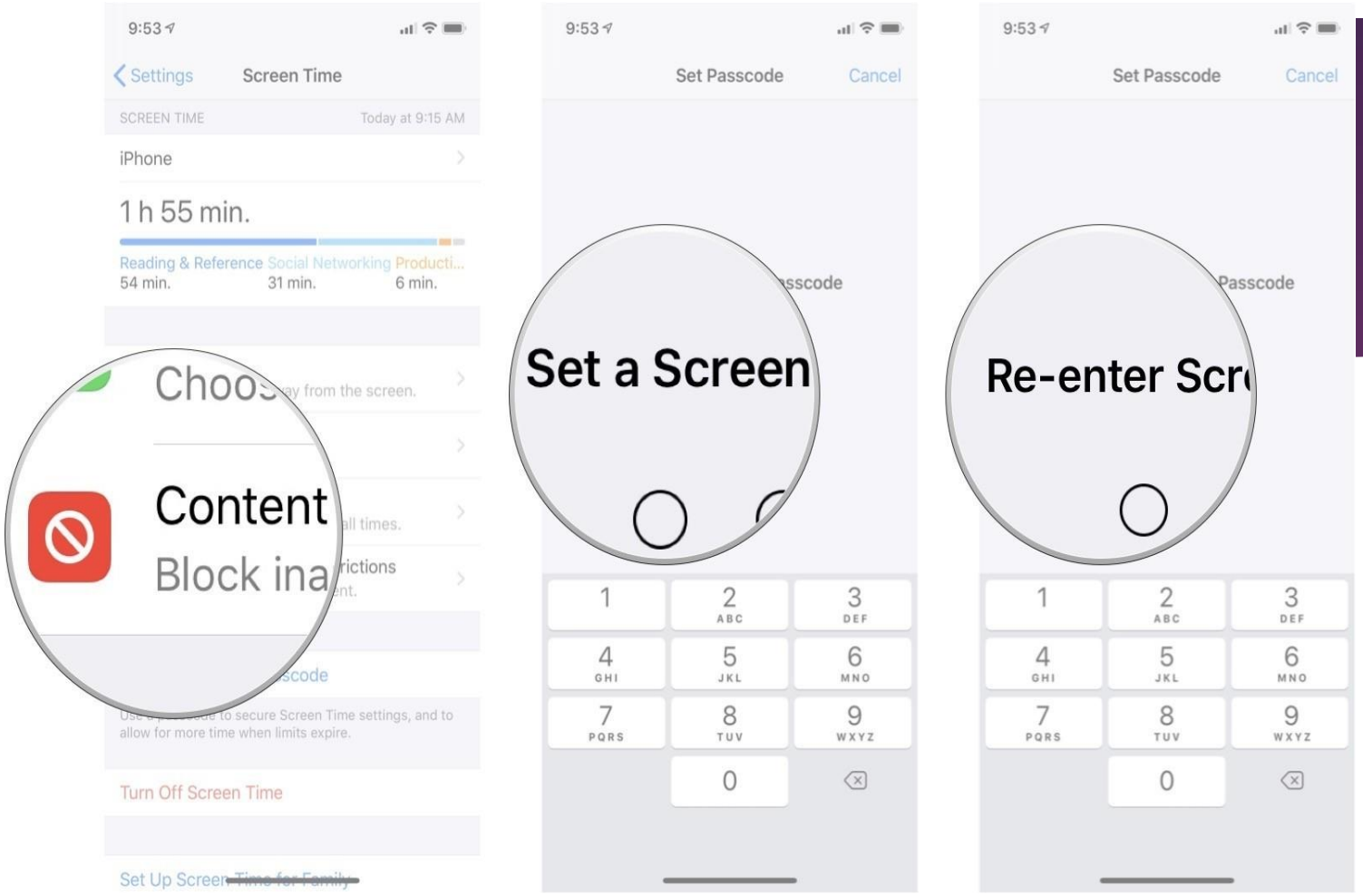


In iOS 12, restricting access to any content falls under the new Screen Time feature.

1.Launch **Settings** from your Home screen.

2.Tap **Screen Time**.

3.Tap **Turn On Screen Time**.



4. Tap **Content & Privacy Restrictions**.
5. Enter a **four-digit passcode**.
6. Re-enter the **four-digit passcode**.

Now you can choose what type of content to block, including in-app purchases, adult websites, location sharing, and a lot more!

More information from Apple: https://support.apple.com/en-us/HT201304

Android Parental Controls

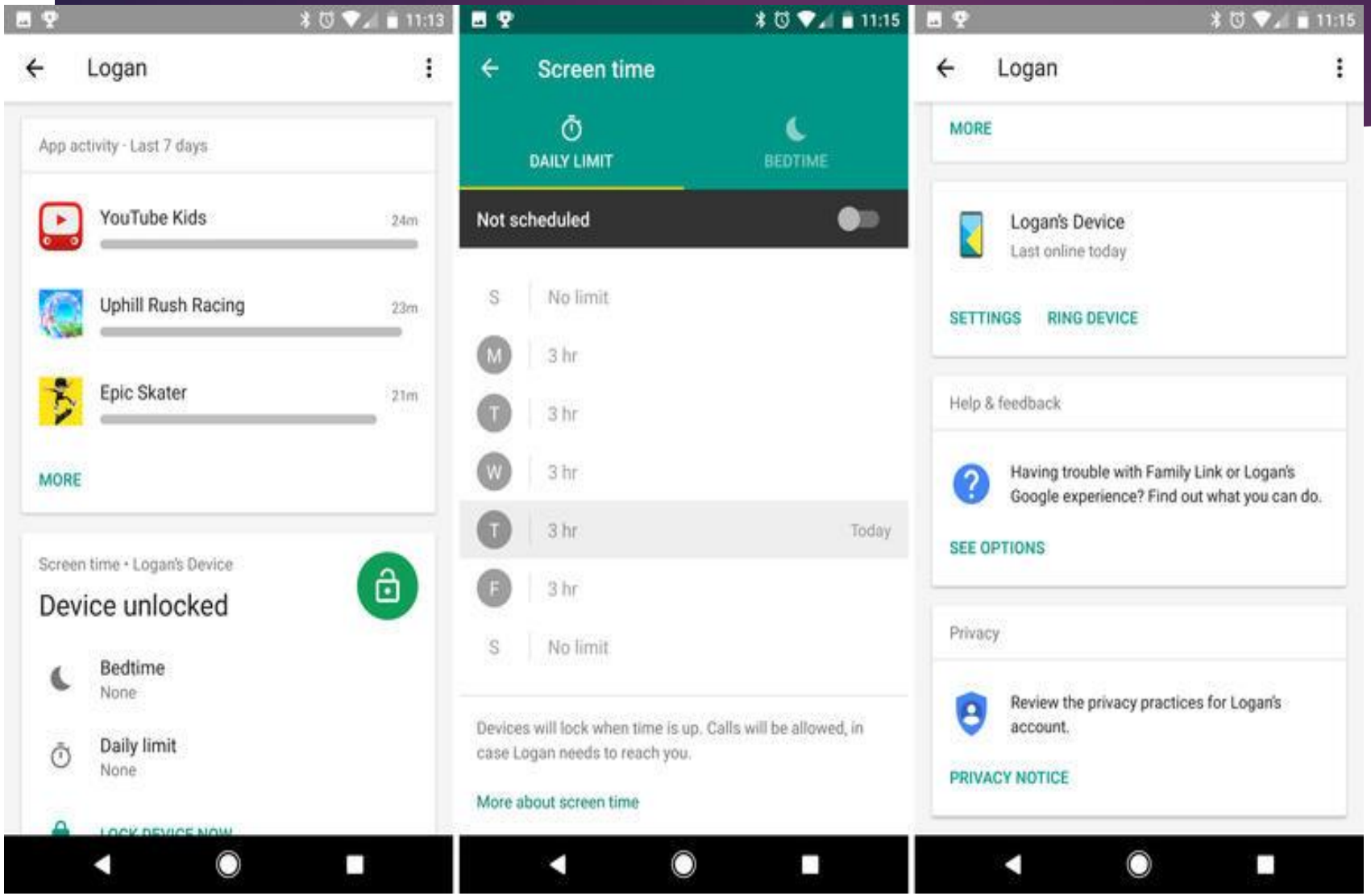
When you turn on parental controls, you can restrict what content can be downloaded or purchased from Google Play based on maturity level.

To Set up parental controls -

- On the device you want parental controls on, open the Play Store
- In the top left corner , tap Menu lines, Settings, Parental Controls.
- Turn "Parental controls" On.
- Create a PIN. This prevents people who don't know the PIN from changing your parental control settings. If you're setting up parental controls on your child's device, choose a PIN they don't already know.
- Tap the type of content you want to filter.
- Choose how to filter or restrict access.

Once you set up parental controls, you can turn them on or off. When you turn them back on and create a new PIN, your old settings will come back. This helps you share a device with people who don’t need parental controls.

Family Link App for Android



- Google has a New Feature called Family Link
- Family link allows parents to create a Google Account for your child, manage the apps they use, keep tabs on their screen time, and set a bedtime after which they are unable to use the device.
- Family Link does not block all offensive content; it is merely another tool you can use in your attempts to keep your kids safe online.

Family Link Details

- Download the Family Link app on your own device
- Launch the app and click Get Started - Click Start on the 'Set up Family Link' screen, then follow the prompts to progress through the setup
- You'll need to answer a few questions about whether your child has a compatible device, and that you want to create a child's account and to start a family group
- Enter your child's first and last names and press Next, Enter their birthday and gender, then press Next
- Choose a Gmail.com username and press next
- Enter a password and press Next, Agree to the T&Cs
- Now it's time to add the account on your child's device. Turn on the phone and sign in using their account details
- Now enter your own Google password and press Next
- Family Link will now be installed on your child's device
- You can review any apps preinstalled on the phone as to whether your child should be allowed to use them.
- Now back on your phone you should find controls for your child's phone. These include content filters, location tracking, app activity and screen time

Parents Can Check Devices

- **We highly recommend checking your child's devices regularly**

- **Know your Child's device Passcodes –**

  1. **Check Cell Phone Calls/Text :** If you're unfamiliar with the phone, ask the salesperson to show you how to check for recent calls and texts. These histories can be cleared, so if there's a need, you can cross-reference with the phone bill. Bills usually itemize each text sent and received -- you won't see the body of the text, but you'll know when it was sent and to what number.
  2. Check Apps – click on apps that don't look familiar – they can be masking a different type of app behind the
     app image"
  3. Check Browser History (previously covered)

What Happens If….

- **1. Cyberbullying** is a frighteningly common occurrence. The Cyberbullying Research Center reports more than 27% of children surveyed say they've been bullied.

Report Harassment - Remind your child to tell you about any hurtful or offensive messages they encounter, and let them know they're not alone. Keep a record of the harassment and report the problem to your local law enforcement agency if necessary.

Block Bullies - If your child is harassed through instant messaging, social media, or email, block the cyberbully immediately and strengthen the account's privacy settings.

- **2. Identity Theft -** Children are prime targets because they have clean credit records and tend to post a lot of personal identifying information online. Plus, most parents don't check their kid's credit report, which means criminals may be able to use the child's identity for years unnoticed.

Keep Information Private - Don't allow your child to post things like their full name, complete address, date of birth. Remind your child never to give out personal information without checking with you first and caution them against taking online surveys or quizzes, as criminals can use information submitted through these formats to steal identities.

Check Credit Reports - Learn the warning signs of identity theft and check your child's credit report at least once per year. Identity theft and cyber scams often go hand in hand. If your child falls victim to a cyber scam, file a complaint with the IC3 www.ic3.gov/complaint/default.aspx

Continued

- **3. Online Sexual Predators -** Sexual predators often use social media to learn about their victim's likes and dislikes, find out where their victim lives and attends school, and even discover where their victim is at any given time.

Talk About the Issue - Reassure your child it's not their fault if someone they don't know initiates inappropriate contact with them, and tell them they must make you aware of the situation immediately. Show your child how to set privacy controls on their social media accounts to help avoid dangerous contact.

Follow Their Online Activity - Another way to help your child stay safe online is periodically checking their social media accounts and other online activity and talking to them about anything that concerns you. We recommend telling your child that you will monitor their activity and talking about your expectations.

- **4. Password Sharing and Hacking -** Sometimes kids share their passwords with friends. Unfortunately, this can result in the child's account being hacked. The hacker may pose as your child to post embarrassing or hurtful content on social media or to send disturbing emails—all of which appear to come from your young one.

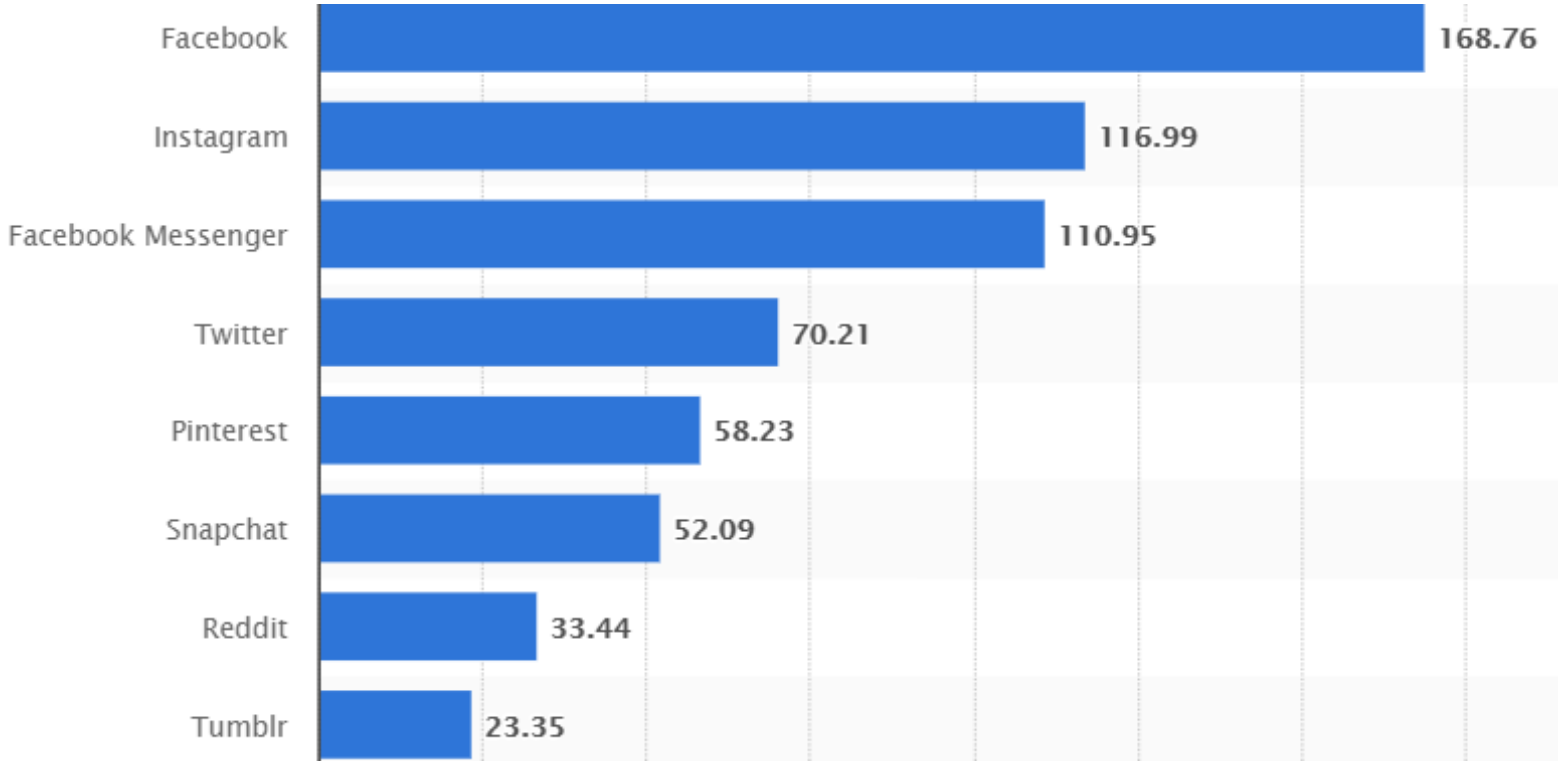
Use Strong Passwords - Help your child create hard-to-crack passwords and keep track of them. Remind your child not to share their passwords with anyone but you, and make sure their usernames aren't easy to guess. For example, a combination of their name and birth year would be easy for hackers to surmise.

Keep Antivirus Protection Up to date - It's important that your child not share their passwords, but it's also just as vital to install antivirus software and keep it up to date. Doing so is one of the best ways to help secure your family's smartphones, laptops, and other devices against hackers and many other cyber threats.

SOCIAL MEDIA

- FACEBOOK
- TWITTER
- INSTAGRAM
- SNAPCHAT
- FINSTA
- VISCO
- TUMBLR
- REDDIT
- YOUTUBE

Most popular mobile social networking apps in the United States as of July 2018 (monthly users in millions)



HELPFUL LINKS

- https://www.familyeducation.com/fun/mobile-apps/10-apps-parents-monitor-kids-mobile-use
- https://www.tomsguide.com/us/best-parental-control-apps,review-2258.html
- https://www.lifewire.com/smartphone-apps-for-monitoring-kids-online-4143301
- https://tech-vise.com/best-apps-and-devices-to-monitor-your-kids-online-activity/
- https://www.spyzie.com/parental-controls/parental-monitoring-app.html
- https://www.jcfs.org/response/blog/what-can-parents-do-make-social-network-safer-place-their-children

Text Abbreviations

ADIH: Another day in hell
A/S/L: Age, sex, location
BTDT: Been there done that
CULTR: See you later
GTFO: Get the f-ck out (expression of surprise)
H8: Hate
ILY or 143 or <3: I love you
JK or J/K: Just kidding
KWIM: Know what I mean?
LLS: Laughing like sh-t
LMIRL: Let's meet in real life
LYLAS (B): Love you like a sister (brother)
NIFOC: Naked in front of computer
PAW or PIR or P911: Parents are watching or Parent in room (drop the subject)
POS: Parent over shoulder (can also mean "piece of sh-t," used as insult)
Pr0n: Intentional misspelling of "porn"
STFU: Shut the f-ck up (expression of surprise rather than reprimand)
TMI: Too much information
TTFN: Ta ta, for now (goodbye)
WTF: What the f-ck?

AND MANY MANY MORE

SUMMARY:

- Keep the Computer in a open area of the home
- Limit child's time "online"
- Limit access to certain types of sites
- Check browser history on all devices
- May need to Monitor or Track your child's online presence using additional programs
- Stay informed – Parents need to stay up-to-date on what's new in social media – join a blog, or a newsletter