Protecting Children's Privacy Online – A Guide for Parents, Carers and Educators

Published by **Paul Bischoff** on September 19, 2017 in **VPN & Privacy**

It's time to have the talk with your child. You peeked at their browser history and, well, it's time. It's going to be awkward and uncomfortable for both of you, and things have changed a lot since you were that age. But better to hear it from a parent than learn it from a stranger or God-knows-who online.

No, not *that* talk. It's time to discuss online privacy with your kids.

Won't the internet and government regulate this for me?

Haha. Good one.

Because we all know how honest people are when asked their age before entering a website. And everyone with the ability to make a website or app has a thorough

understanding of ethics and regulations when it comes to collecting data and serving advertisements to minors. With great power comes great responsibility, right?

At least, that's what the forward-thinking legislators that drew up the 1998 Children's Online Privacy Protection Act thought. The US law requires that websites directed at children under the age of 13 must get parental consent among other compliance standards. As if the average kid has a long enough attention span to wait around for their parent to read through a privacy policy.

COPPA has been heavily criticized for being ineffective and even counterproductive in protecting kids online. Children often resort to less age-appropriate content instead of waiting around for a parent's approval. It doesn't stop kids from accessing pornography or from being advertised to. Websites that might otherwise provide content that's appropriate for kids often ban children altogether because of the compliance burden and potential fines for violating COPPA.

The UK has been a bit more pro-active in spreading online privacy awareness among British youth through the UKCCIS and its "Click clever, click safe" mantra. However, this is the same organization that in 2013 attempted to filter websites deemed unsafe or inappropriate for children, but inadvertently blocked the websites of LGBT rights groups and charities meant to educate children about drugs, health, and sex.

So no, you can't depend on the internet self-regulating itself or on governments (which can only create regulations for their own country, anyway) to step in on your behalf.

Is children's privacy really an issue?

You bet it is!

Three out of four children have access to a smartphone in the US. In the UK, 43 percent of nine- to 12-year-olds have a social media profile, according to the Library of Congress. One in three are on Facebook despite the 13-year-old age limit. A quarter of those kids on Facebook never touch the privacy restrictions on their profile, and a fifth of them publicly display their address and/or phone number. Facebook claims it is powerless to stop children from lying about their age and creating accounts.

And that's just Facebook. It isn't even cool anymore. Snapchat, Tumblr, Vine, Instagram, and Kik are all popular among teens and pre-teens. Who knows what will come next?

Social media and games pose the biggest threat to children's privacy, because they request a significant amount of information upon registration. Profile info is used by the social network to serve targeted ads and recommend content. That info can also be used by scammers and predators to target kids. To be fair, it happens to adults, too. But kids are far more susceptible than adults.

Read more: [How your identity can be stolen using social media (and how to prevent it)]

The ramifications of ignoring a child's online activity can have both immediate and long-term effects. You've probably heard of horror stories where a kid unknowingly spends thousands of dollars on in-app purchases in a mobile game. Drug dealers and sex offenders target kids online, as do identity thieves. In fact, Carnegie Mellon CyLabs says children are over 50 times as likely to have their social security number used by another person.

One in 40 families has a child who is a victim of identity theft, according to the Identity Theft Assistance Center and the Javelin Strategy & Research Group, and that figure is on the rise. Kids make great targets for identity theft because they have clean slates with no blemishes on their credit report. Identity fraud can go on for years without notice, because kids have no need for credit until they are old enough to buy a car, rent an apartment, or take out loans for college. When that day comes, however, these young victims are in for a rude awakening.

Enough of your fear-mongering! What can I do about it?

As a parent, there's a fine line between protecting your kids' privacy and invading it yourself. But there are a few simple precautions to take that will allow them freedom while safeguarding their interests.

Follow and friend your kids

Worried about what your kid is posting on Snapchat? Well, that's easy. Install it, make an account, and follow them. Now you can safely monitor their public account activity from a reasonable distance, and they'll likewise be more conscious about what they post. You can view their friends list on Facebook to see if there's anyone shady. No, you won't be able to screen what's being said on private channels, but kids are allowed to have secrets.

Do the same for every social media account. Log into Minecraft to terrorize Junior's village. Not only will it help keep your child safe, you'll also get to know them and the world they live in better. It's a win-win for all parties.

Don't start making rules that seem arbitrary to your kid. Without being condescending, explain to them the risks and dangers of failing to protecting online privacy. Toss out some of those stats from above as proof.

Don't go behind their back and spy on your kids, either. This will only further distrust and could leave them more exposed. When you take a measure that requires some oversight, be transparent about it.

Don't use social logins on untrusted sites

Kids and adults alike get sucked into playing quizzes and taking surveys online, especially on Facebook. But many of these sites ask that the user log in with their

social media profile before the results can be posted for friends to see. Tell your kid to avoid those games and quizzes, as many of them mine data from your child's profile and their friends' profiles, which is used by the company and third parties to target advertisements and who knows what else. Unless you recognize and trust the company that owns the website, don't use your social media profiles to authenticate or authorize apps.

See also: Facebook, Twitter, Google+, or LinkedIn … Which should you log in with?

Adjusting kids' privacy settings

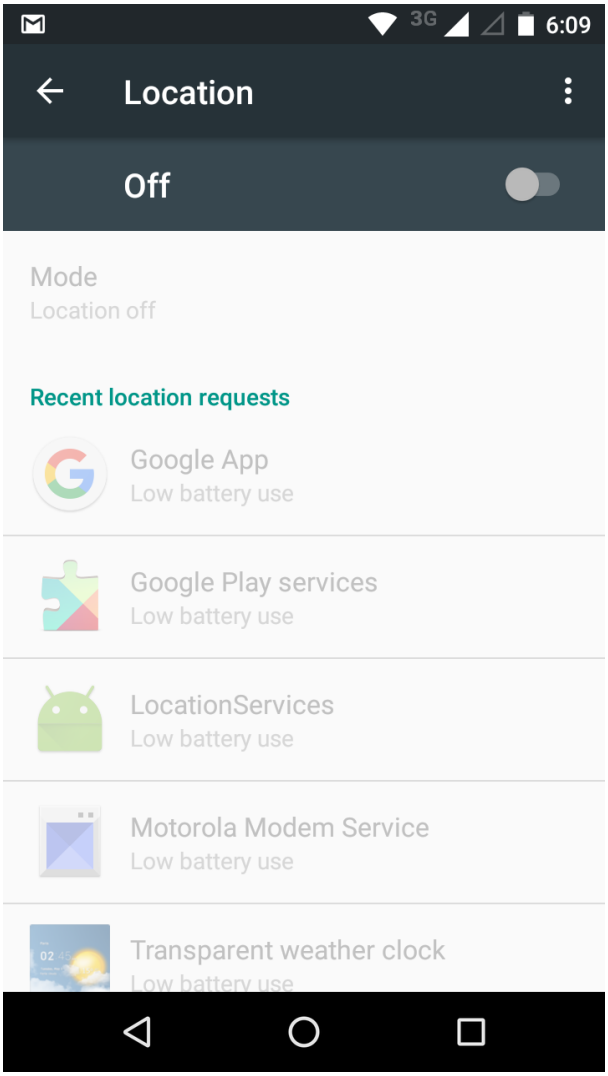
Almost every social media app will have a tab full of privacy settings. Learn them. Read the privacy policies. Now that you have the same apps as your kid, sit down with them and disable what needs to be disabled. Remove the accounts from search results so strangers can't send friend requests. Remove as much public profile info as possible–address, school, phone number, email address, etc. Tightening privacy settings for the most part won't affect how a social media app functions, so your child shouldn't put up much of a fight.

Protecting your child's privacy is really just an extension of protecting your own privacy. You can perform many of these tasks together. We won't cover every single app that your child may or may not have installed in this article, but we'll touch on a few of the big ones.

See: 75+ free tools to protect your privacy online

Device settings

First off, on all devices, location services have become the norm. This allows Apple, Google, Microsoft, and app makers to monitor the location of the user. For obvious reasons, it's best to turn these off. Tell your kids not to geo-tag their photos on social networks–at least not until they've left that particular location and don't plan to return. In newer versions of iOS and Android, you can disable the location-tracking permission on an app by app basis, or disable it entirely in the settings.

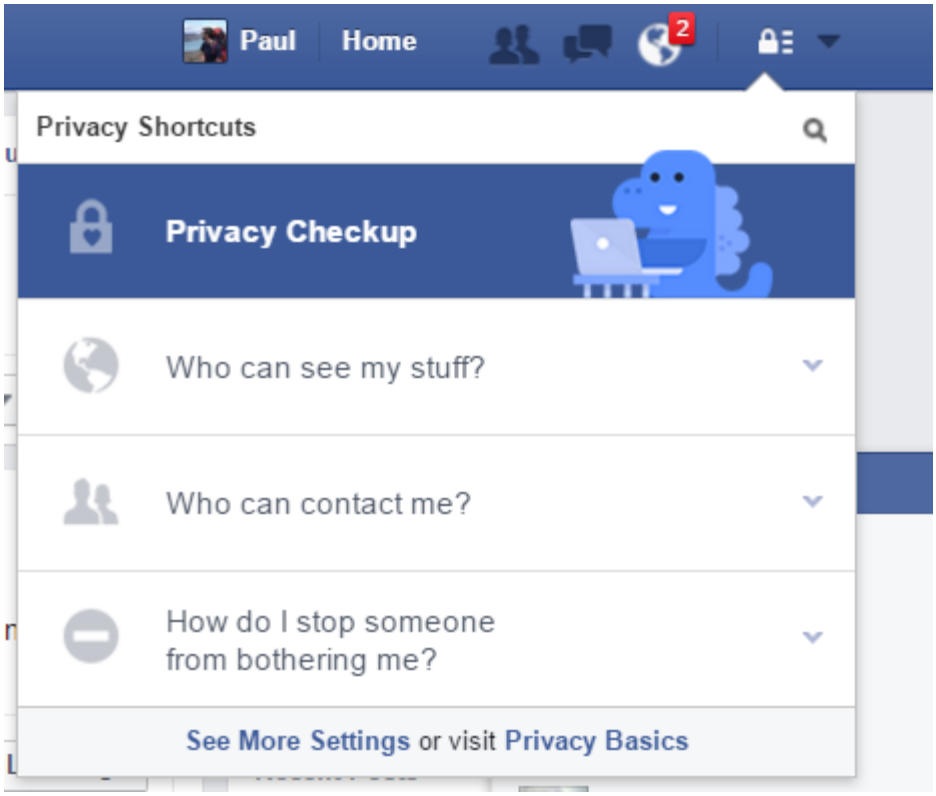


Front-facing cameras are also nearly universal on phones, tablets, and laptops nowadays. There's no shortage of news stories about both hackers and law enforcement remotely enabling cameras unbeknownst to the user, snapping photos and learning their whereabouts. Place a sticker or piece of electrical tape over these cameras.

Always set a swipe pattern, PIN number, or password on your devices to keep both strangers and ill-willed acquaintances out of your kid's business.

Facebook privacy settings

It's likely that no social network on the internet knows more about us than Facebook, and the privacy settings of the world's largest social network can unfortunately be a bit tricky to navigate. Start by going to the top-right corner of the home page and clicking the lock icon. Click to drop down "Who can see my stuff?" and switch it to "Just friends." This should keep your child out of view from passing strangers.



In the next drop-down, “Who can contact me?”, you can set who is allowed to send your child friend requests. There’s no longer an option to make a profile un-searchable. Instead, the most private option you get is to only allow Friends of Friends to send friend requests. Your kid can still send friend requests to whomever he or she pleases, so it won’t limit who they can be friends with.

On the last section, block scammers, cyber bullies, and anyone else you don’t want your kid communicating with.

We’re not done yet. On the very bottom of this tab, click “See more settings.” Here you can prevent people from searching for your kids’ account by their phone number or email address. Do so.

Click the “Timeline and Tagging” tab on the left sidebar of this page. Set all these settings to “Friends” when available to keep strangers at bay. Here you may also want to add the option to review photos and statuses in which your child is tagged. This prevents any inappropriate photos and cyber-bullying from showing up on their account, which could otherwise come back to haunt them later.

Facebook now lets users choose to share statuses and photos but exempt specific people from seeing them. Let your kid know that they shouldn’t block you in this way, as anything that they don’t feel comfortable sharing with you shouldn’t be shared with the rest of the world.

Next up is the Followers tab. A follower is basically someone who can view your profile and posts but isn’t personally friends with you. Switch this from Everybody to Friends as another barrier to strangers.

Now for the apps section. This is the most under-utilized part of Facebook's privacy protections, probably because Facebook financially benefits from third-party apps having access to users' personal data. Any time you log in with Facebook on another website or app, it shows up here. You and your son or daughter should both do this part. Go through each app individually (there may well be a lot of them) and give each the absolute minimum permissions. This means changing visibility to Only Me unless it won't otherwise function, and disabling other visibility permissions like friends list, timeline, email address, school, phone number, etc. Don't let apps post on your behalf or send you notifications unless you absolutely trust them. If you don't recognize an app or don't use it anymore, remove it altogether, as the privacy policy may have altered since first connecting it to your account.

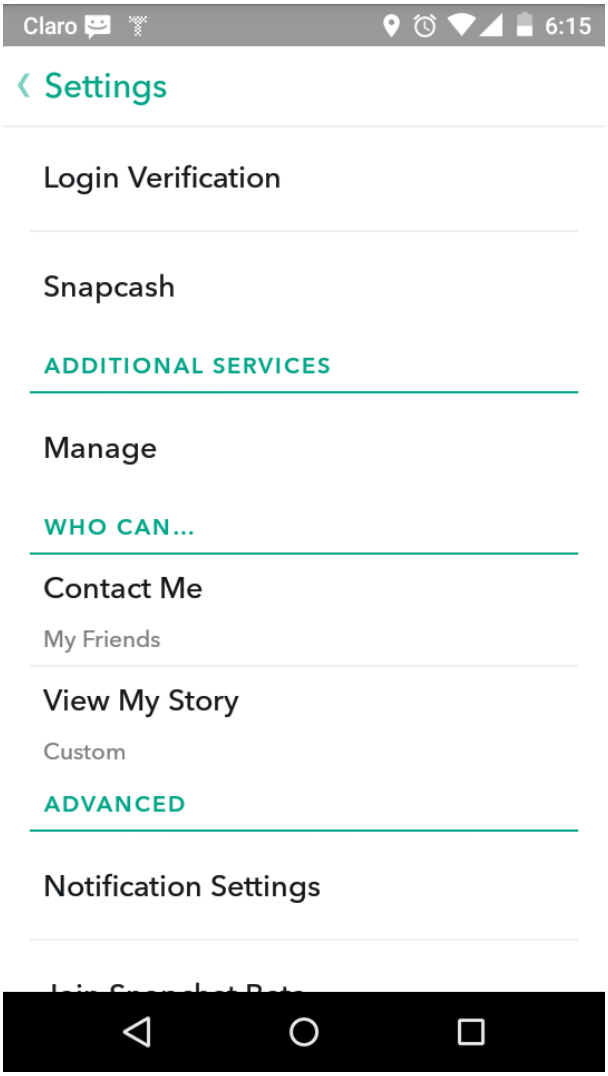
After you've removed all the unnecessary permissions from all these apps (make sure to click Show All at the bottom), scroll down a bit further to the three panels below the app list. Under Apps Others Use, click Edit. This is a list of information that apps used by your friends can see on your profile. Tricky, right? Even after disabling all those app permissions, the apps used by your friends can still access your information. Uncheck everything and stick it to Big Brother.

Okay, last step. Go to the Security tab at the top of the left sidebar. The privacy-related bits we're most concerned with here are Login Approvals, App Passwords, Your Browsers and Apps, and Where You're Logged In.

- Login Approvals is basically the same as two-step authentication. Whenever logging in from a new device, a code will be sent to your phone as an extra layer of security. You will have to add a phone number if you haven't already.
- App passwords lets you set a separate password for apps that support this function and allow you to log in with your Facebook account, such as Spotify and Skype. It's a good idea to have different passwords for each app when possible. Learn more about creating and memorizing strong passwords here.
- If your kid gets a new phone or logs in on someone else's device, the Your Browsers and Apps setting is important. It's a log of devices that don't require identity confirmations or send notifications when logged in. Remove any that aren't among your current devices or that you don't recognize.
- Where You're Logged In is similar to the above setting, but for active logins. Again, remove any you don't recognize or that aren't yours.

Snapchat privacy settings

If sifting through all of Facebook's privacy settings made you weary, you'll be happy to know Snapchat is much simpler. Launch the app and click the ghost icon at the top of the screen, then the settings cog at the top right. Scroll down to the "Who can…" section. Set both Contact Me and View My Story to My Friends. Who can view my story can also be customized to a specific list of people. This is also where to block certain individuals.

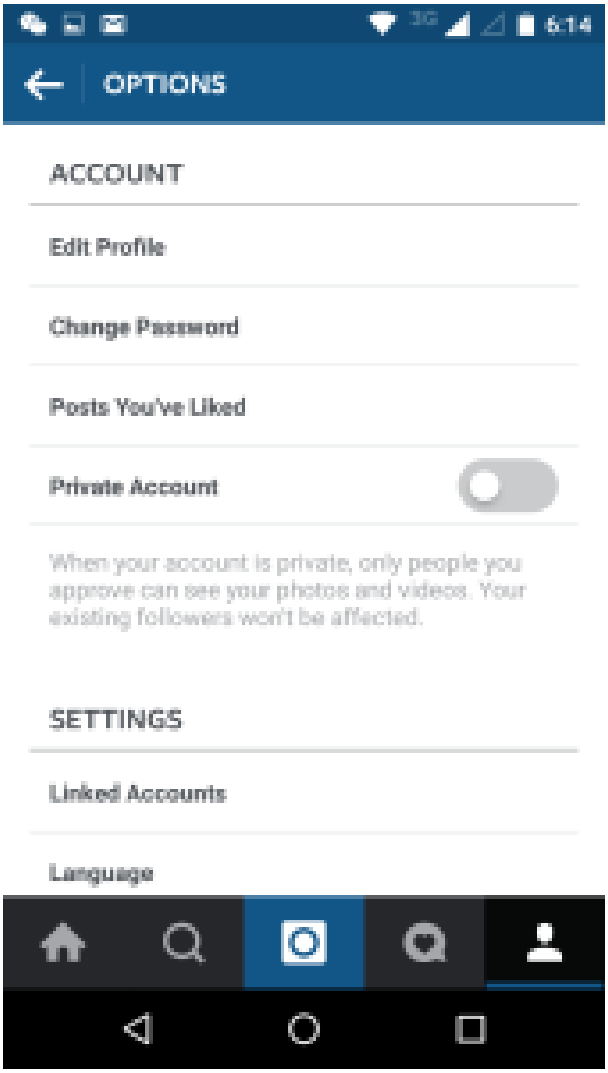


Back on the settings page, click Login Verification to set up two-step authentication. This can be done with a phone number and SMS or using an authentication app like Google Authenticator or Authy. Login verification makes logging into Snapchat from a new device a two-step process, which is more secure.

That's pretty much all that can be modified on Snapchat as far as privacy goes. You can navigate to Additional Services > Manage > Permissions to see what kinds of access Snapchat gets to your device, but these cannot be modified. You'll also find the privacy policy and terms of service on the main settings page.

Instagram privacy settings

Rounding out the top three most-used apps among teens is Instagram. To find Instagram's privacy settings, click the head and shoulders icon on the bottom right, then the three dots on the top right.



You can elect to switch to a Private Account, but most would agree this sort of defeats the point of Instagram. Other than that, there's not much to make private.

Instead, privacy and safety on Instagram is more about how the app is used. When you post a photo, don't add a location until after your child has left said location, and only if they don't plan to return anytime soon. Otherwise, strangers can determine where your kid hangs out or where they are as soon as the photo is posted. Not only could this mean a predator could find your kid, it also means a burglar could figure out if a family is home or not.

Twitter privacy settings

Similar to Instagram, there's not much to hide on Twitter. Don't add any personal details to tweets or the profile blurb, and you'll be fine.

Tumblr privacy settings

Tumblr isn't quite as popular among teens as other apps, but among the art and poetry lies a haven for porn, smut, and vulgarity. Tumblr doesn't require a real name

upon registration, so there's no need to use one. Privacy settings can be accessed through the app or on the website.

Here you can disable messaging so strangers can't contact children. If your child has his or her own Tumblr blog, it's probably a good idea to disable comments and replies to posts. Blogs can be made private, but this makes them password protected. It's between you and your child if you think this is best.

As with everything else, don't post personal details and be smart about geo-tagging photos.

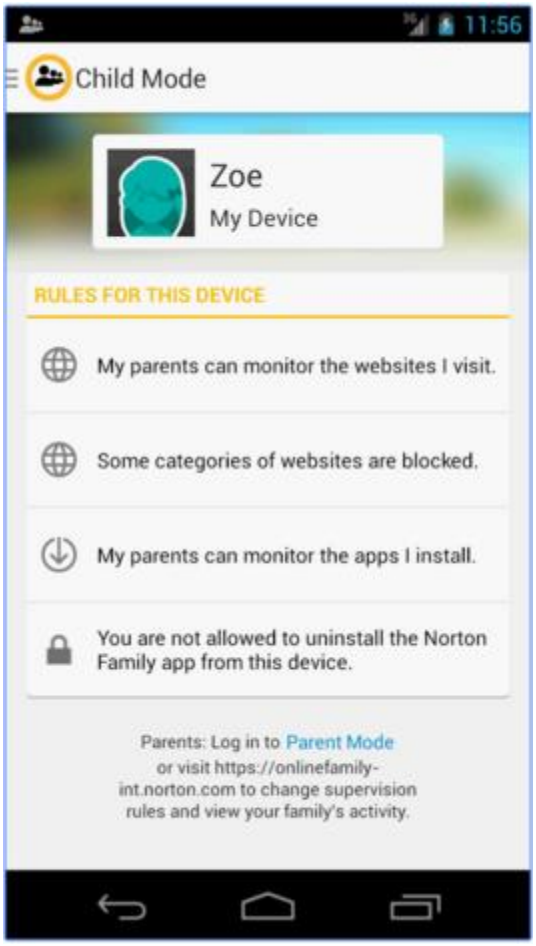
Parental controls

Parental controls can be enabled by either a built-in mechanism or by a third-party tool on Android, iOS, and most modern web browsers. These controls not only protect your child from inappropriate content, but can also prevent them from inadvertently divulging personal details about themselves or your family. These are mainly aimed at younger children; your 16-year-old won't appreciate the level of micromanagement that these tools offer.

Android

Android lacks dedicated parental control, but some phones come with the ability to create multiple user accounts. In the settings, check for for a "Users" section, where you can add a restricted profile. A restricted profile allows you to toggle which apps the user can access. This is especially useful if you allow a young child without a phone of his or her own to play with your tablet or phone. The account switches depending on the PIN or password entered on the lock screen.

If you're worried about invasive apps or games that are likely to run up a bill, parents can require that their Google account password be entered before downloading an app or making in-app purchases. Apps can be filtered by low, medium, or high maturity levels.

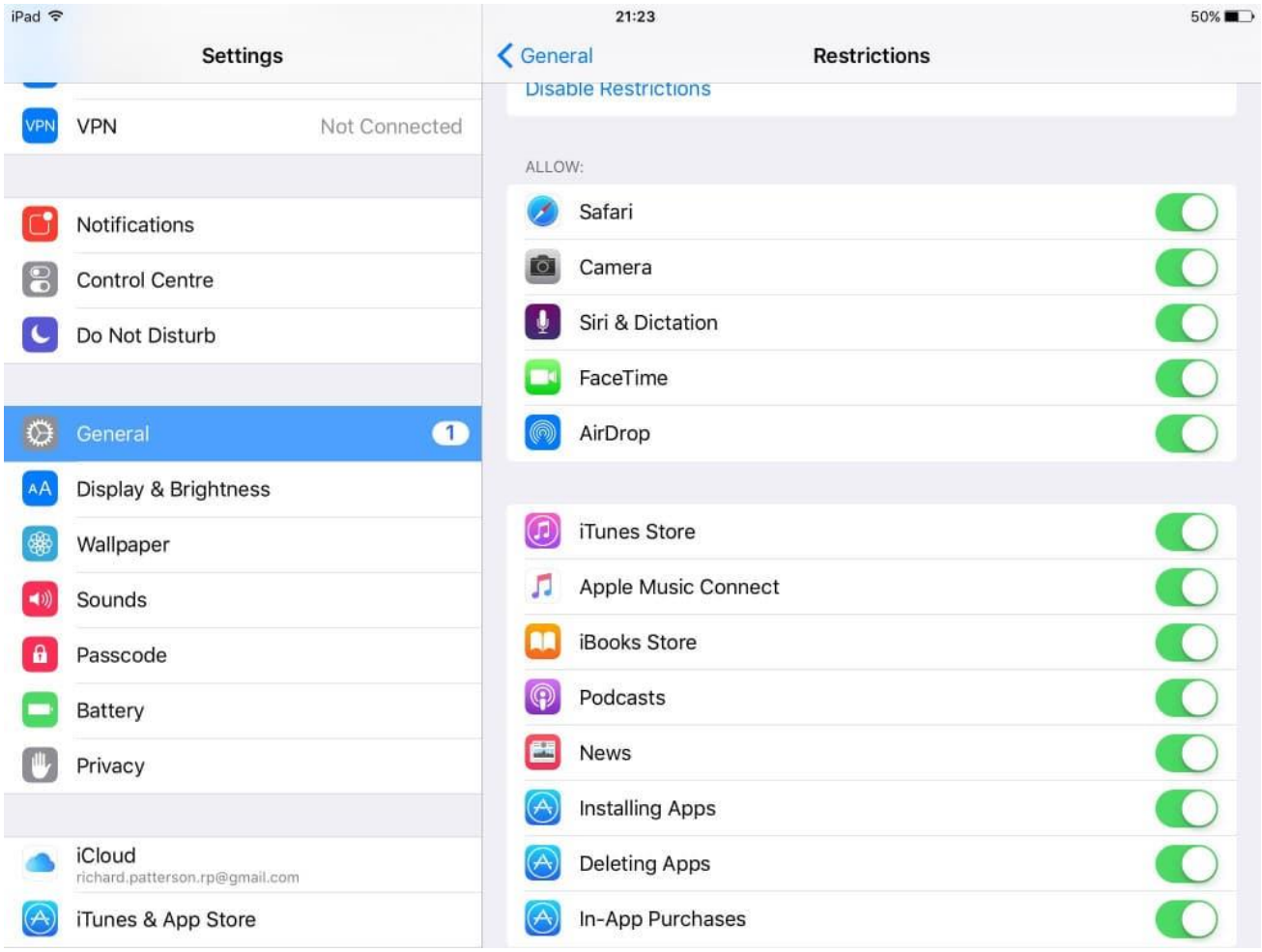


Several apps out there make it easy to monitor and manage what children do with their phones. Norton Family Premier costs a whopping $49.99, but it comes with a slew of useful features including location tracking, the ability to block individual apps, and web filtering. Parents can see and limit when and how much screen time their kids get. It also works on multiple devices for families with multiple smartphone-touting rascals. Qustodio, Net Nanny, and PhoneSherriff are other solid premium options.

For free alternatives, check out Funamo, Lock2Learn, MM Guardian, and AppLock.

iOS

iPhones and iPads, unlike Android, have some parental controls built in. In the General settings of iOS, just click on Restrictions and create a passcode. Here you can disable installed apps and certain features. Safari, the App Store, FaceTime, music apps, Siri, and in-app purchases can all be turned off or filtered.

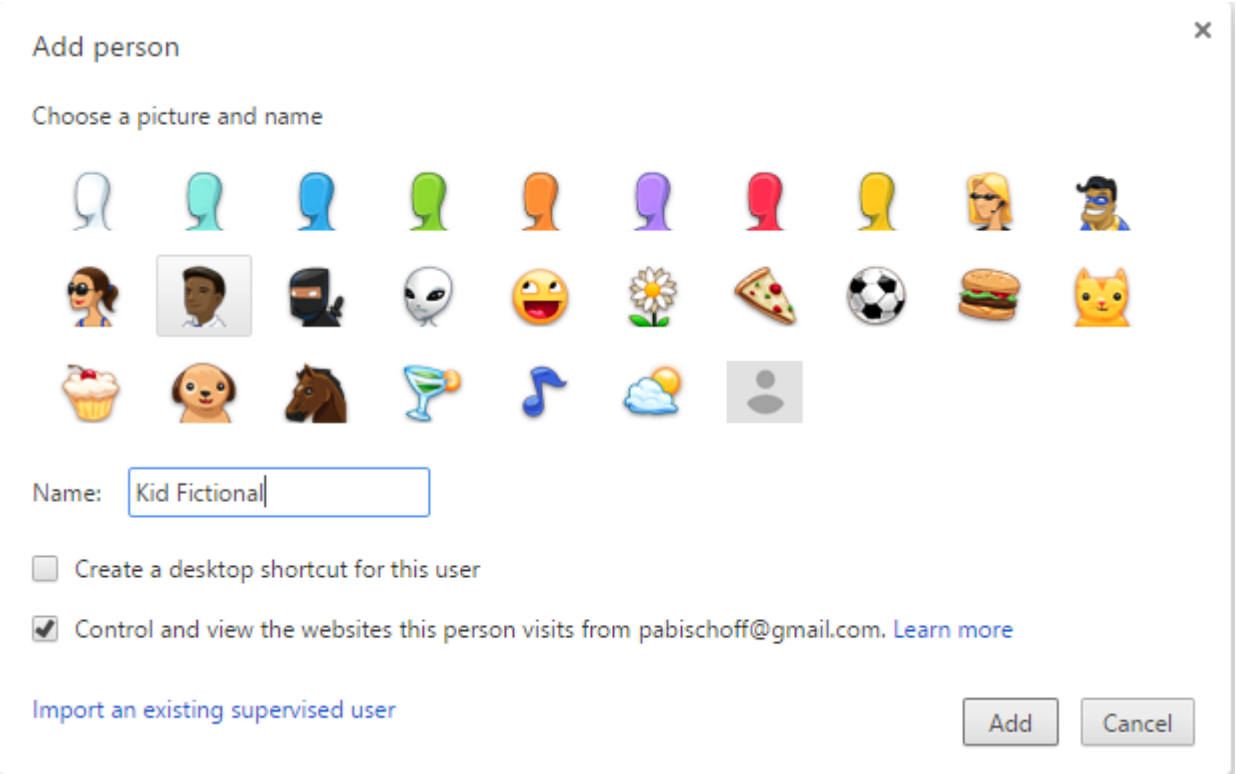


Social media and location services can be restricted as well.

If parents want to be able to monitor and manage iPhone use with more granularity, there's an app for that. Netsanity, Qustodio, OurPact, and Kidslox all include features like curfews, timers, site blockers, and app hiders.

Browsers

In **Chrome** settings on the desktop browser, scroll down to the People section. Uncheck "Let anyone add a person" so your child can't easily circumvent it, then click "Add person." You can choose to create a desktop shortcut especially for them. Select an icon for them and check "Control and view the websites this person visits from ." Navigate to the supervised users dashboard at https://chrome.google.com/manage. Choose your new profile, then click Manage on the top right of the Permissions frame. Here you can enter specific websites to block, or only allow certain websites to be accessed. Remember to enable SafeSearch as a general filter for kids. If you block a site that your tiny surfer wants access to, he or she can request it without even having to ask you face to face.

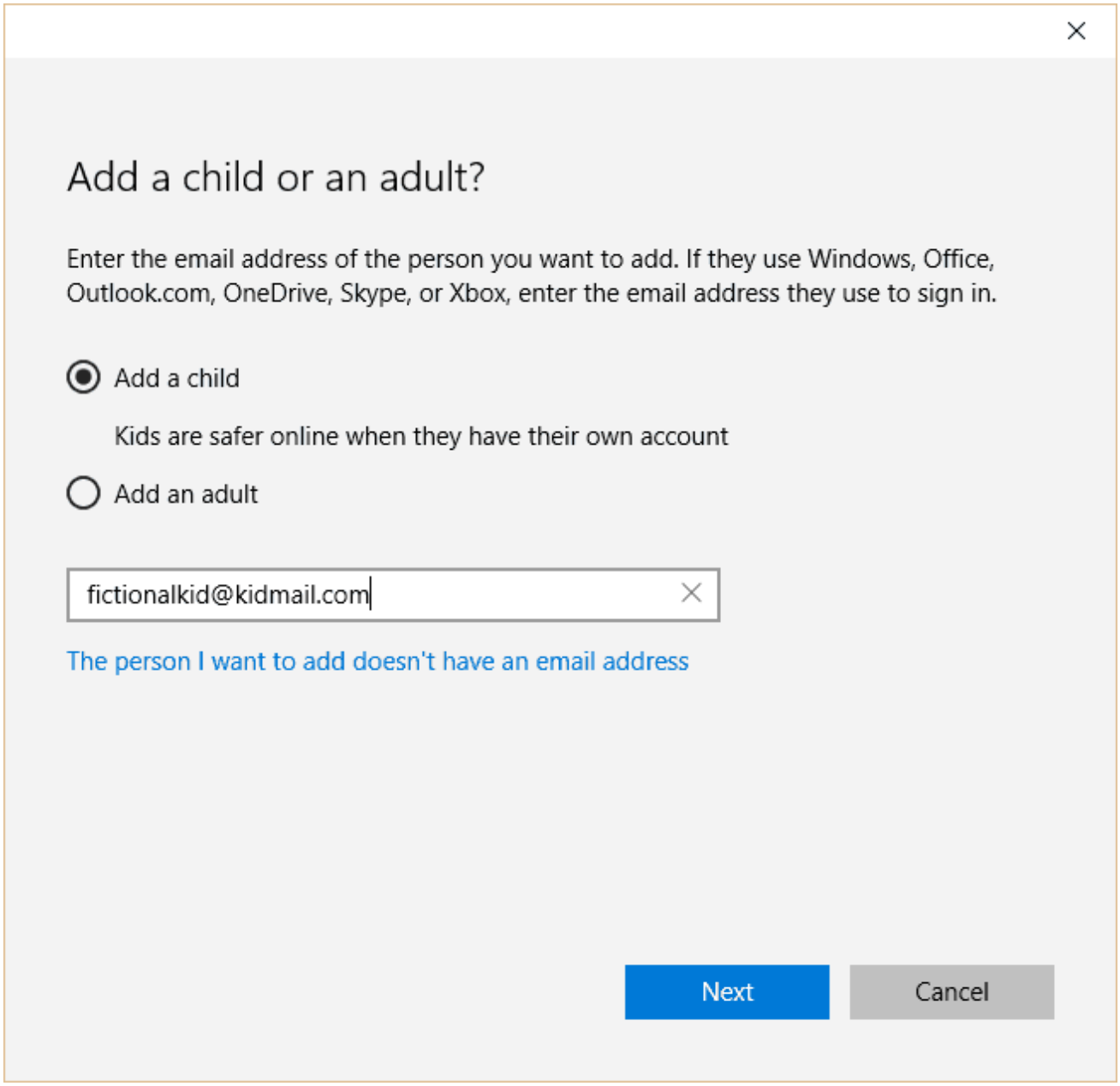


For more granular controls, a handful of extensions in the Chrome store should fulfill your needs. WebFilter Pro and Blocksi Web Filter offer features like time management, Youtube filtering, web filtering, whitelists, and blacklists.

Firefox doesn't come with any built-in parental control measures, so you'll have to rely on third-party plug-ins. FoxFilter is probably the most widely used. The sensitivity can be set to block keywords in the body text or just in the metadata, such as page title and URL. Specific keywords and websites can be blacklisted and whitelisted, and many keywords are included upon installation.

Windows

Microsoft introduced dedicated children's accounts starting with Windows 8.
On **Windows 10**, click on the start menu and go to Settings. Head to the Accounts > Family and Other Users, and hit "Add a family member." On the following screen, choose "Add a child." You may need to create an email account for them. Enter a phone number used to reset the password. Windows will then ask you if you want to let Microsoft target your kids with ads or send them promotional offers. Turn these off, as they are counterproductive to the whole privacy stance we're trying to take.

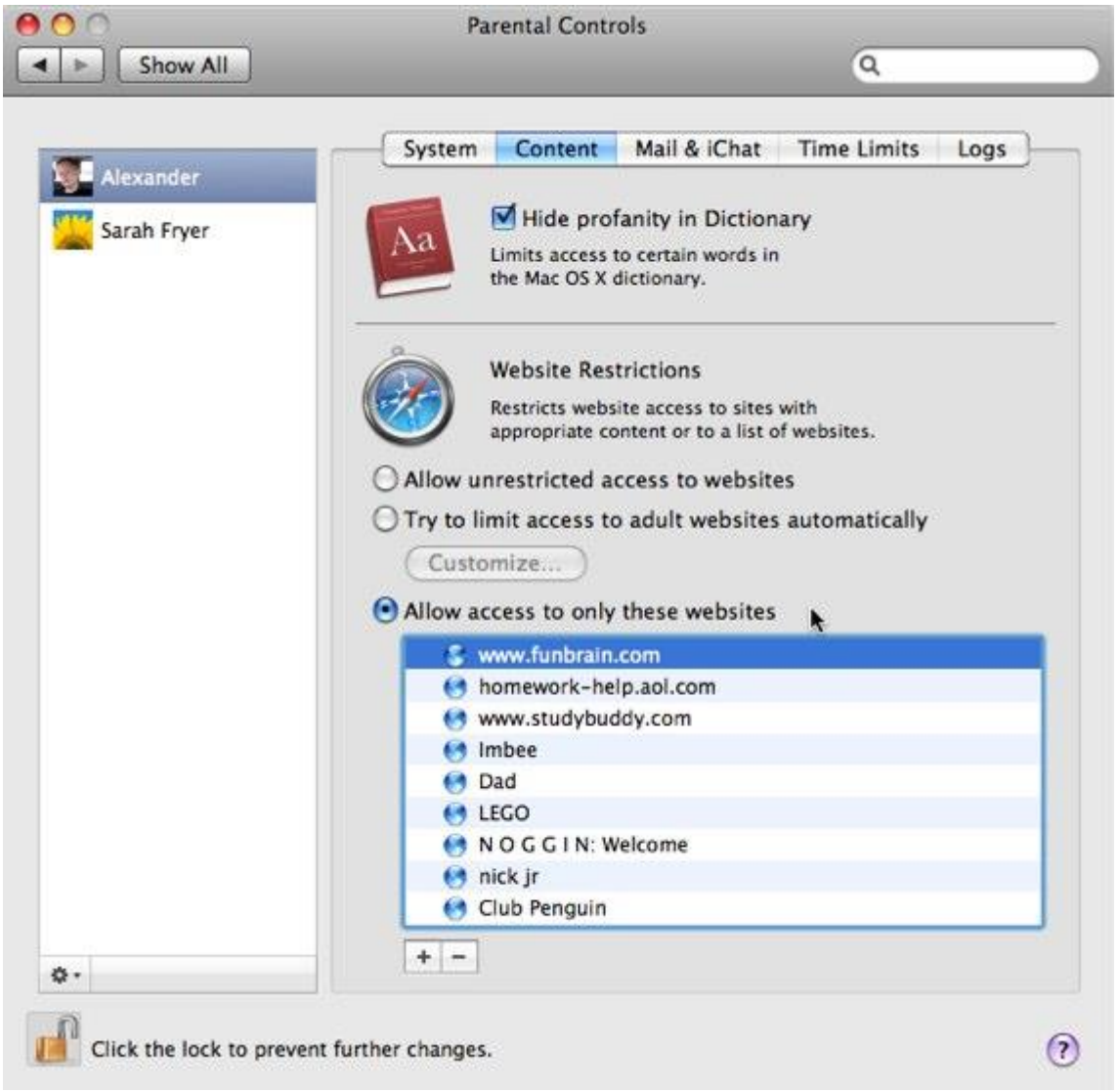


Now that you have a child account set up, you can receive weekly reports on their activity and manage the settings online. You can choose to block inappropriate websites, add your own sites to the whitelist and blacklist, limit apps and games by rating, and set when and how long the computer can be used.

You might find this process a bit off-putting since your child has to register with an email address. If that's the case, third-party applications are also available. You might recognize the names from our Android and iOS lists: Qustodio, Norton Family, and SocialShield are all solid options. SocialShield is particularly useful for monitoring social media, alerting parents to posts containing content about sex and drugs, suspicious friend requests, and messages that could lead to a real-world interaction.

Mac OSX

To turn on parental controls in **OSX**, head to the System Preferences in the Apple Menu. Click Parental Controls, and add a new user with parental controls enabled. Now back on your administrator account, enable parental controls for the new user. If you spoiled your kid with his or her own Macbook, you can also manage parental controls from another computer.



To set restrictions, click through the tabs on the top. Apps lets you specify a permitted rating and what apps your kid can access. Web lets you filter access to websites. People restricts a child's interaction with others through the Mail, iMessage, and Game Center apps. Time limits is for time management. Other can be used to censor language, block the built-in camera, and prevent password changes.

Qustodio and Norton Family are also available as third-party parental control software for Macs.

ID theft protection

ID theft can happen to anyone, and children are often targeted because few people think to check their kids' credit reports. Be one of the few who do. In the US, all citizens are granted one free credit report from each of the three national credit reporting bureaus per year, which you can get from AnnualCreditReport.com. Order a copy and check it for any unauthorized or suspicious activity.

UK citizens don't get the same courtesy, but a few credit reporting agencies offer free trials from which you may obtain your kids' credit reports.

Credit reporting begins as soon as a child has an account opened in their name for which a credit check is required. From that point on, they have a credit score.

Teach your kids good habits early on, such as thoroughly checking each purchase on a credit card statement if they have one, and regularly monitoring bank accounts for any activity they didn't authorize. Let them know the importance of safeguarding their social security numbers (national insurance numbers if you're in the UK), as well as other ID numbers on driver's licenses and medical insurance cards. These can all be used to commit fraud under your kid's name and damage their credit for years to come.

As an added layer of protection, you might consider investing in an identity theft protection service. These agencies monitor your personal information, bank accounts credit cards, and public records for misuse. They offer assistance should discrepancies or fraud crop up, along with large insurance plans to compensate for any losses that occur as a result of identity theft. If your child has previously been a victim of identity theft, then they are more at risk, so these services are especially useful.

TrustedID is the only ID theft protection service that we've reviewed with a true family plan, but other agencies usually have options to enroll kids. Check out all of our ID theft protection reviews to find which one best suits your family.

Parental control software

Parental control software can give parents broader and more granular tools to manage their kids online behavior. Many programs allow you to monitor what websites your kids visit and which apps they use. You can block specific sites or apps or enable blocking on websites that contain certain keywords or fall under a

certain category. You can even specify when kids can use their devices and for how long.

Dozens of parental control software are available, so finding the best fit at the right price can be a challenge. Fortunately, we've taken care of that for you by extensively testing several of the top parental control software on the market. Check out our parental control software reviews here.

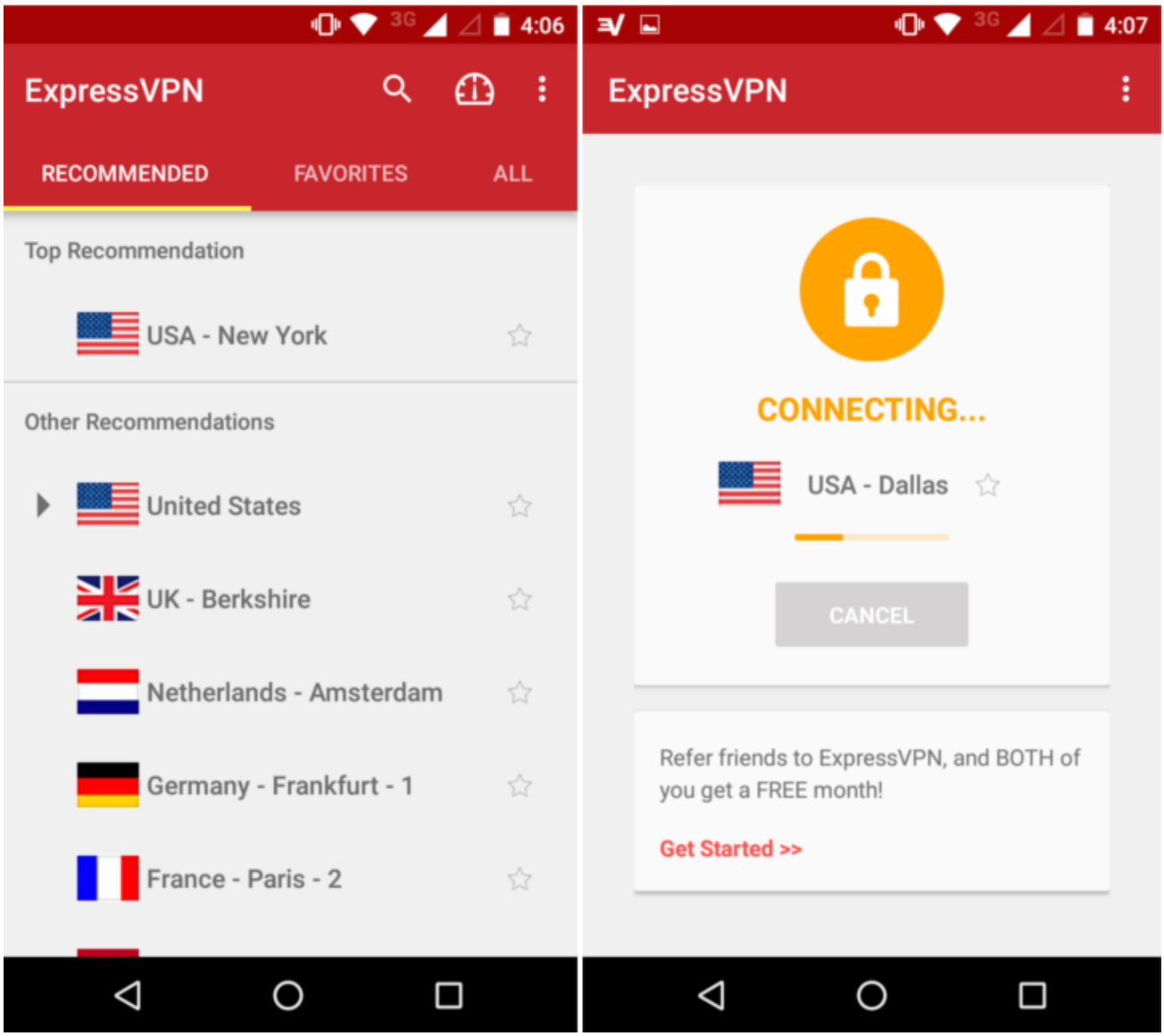
Use a VPN

When inputting private information on registration pages and online shopping sites, make sure the site uses a verified SSL certificate. This is usually indicated by a lock icon and a URL prepended with HTTPS. This encrypts communication between the browser and the server. Install the HTTPS Everywhere extension on your browser to use HTTPS by default when available.

HTTPS isn't available for most websites, however, so whatever information transmitted from your computer to the web is unencrypted and viewable by anyone who wants to see it. To better protect yourself and your children, invest in a VPN service. A VPN encrypts all your incoming and outgoing traffic, and it also routes that traffic through a server in a location of your choosing. This has the effect of making all your internet activity anonymous while hiding both the content of your connection and masking your IP address and true location.

Switching on the VPN before surfing the web or doing anything else online is a good habit to get into for both parents and kids.

When it comes to ease of use–even something a young child could learn to use–it's tough to beat ExpressVPN. It's one of the fastest VPNs we've tested and is designed with novices in mind. On the downside, it doesn't offer family plans, and the individual plans are relatively expensive. Read our review of ExpressVPN.



For a cheaper option that works for an entire household of devices, we recommend PureVPN or Private Internet Access. Read our reviews of PureVPN and PIA.

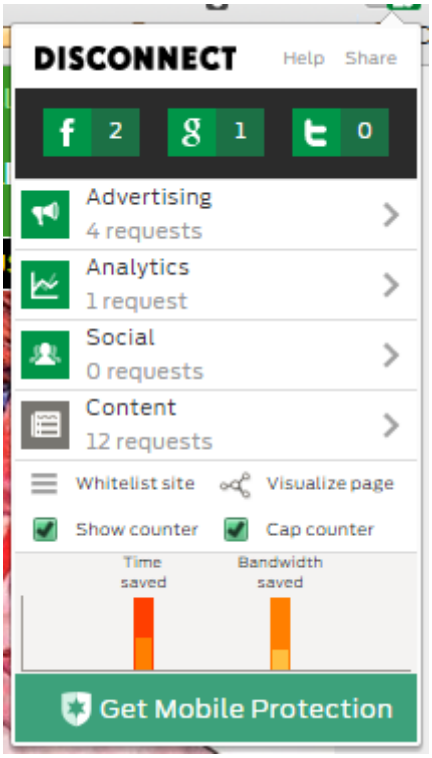
Making your child anonymous

In combination with a VPN, the following list of precautions can make your child invisible or at least more of an enigma to the internet at large.

Fake personal information

You probably spent a fair amount of time teaching your kids how to spell their names, when their birthday is, and the address where they live. Now teach them to lie about it to strangers, when asked. Use a fake birthday on Facebook, if you use one at all. A first and middle name is preferable to a first and last. If you're not expecting mail, use a phony address.

Enable ad blockers



Online advertisements aren't just for advertising, they are also used to mine data from the person viewing them. Some are harmless, but others are downright malicious. Ad blockers and anti-tracking extensions can prevent ad companies from snooping on your kids. We recommend Ad Block Plus and Disconnect. Disconnect even offers an educational kids version, Disconnect Kids.

Search anonymously

Whether for homework or curiosity, children will need to use search engines. Google and others will collect information on every user to create a profile around them, which is used to make recommendations and target ads. On both mobile devices and desktop browsers, you can set the default search engine to something more anonymous.

DuckDuckGo, StartPage, and ixquick don't log IP addresses, use tracking cookies, or monitor what results you click on. StartPage and ixquick actually scrub your personal details before submitting the search query to Google or another major search engine on your behalf, so you get the same results without giving up any information.

Police photos

This can be more difficult than it sounds. Depending on your child's age, you may want to untag all photos of your kid that appear online. On Facebook, as mentioned above, you can opt to review any photo that your child is tagged in before the tag is made public to friends. But not all social networks have such granular controls.

If your child is on a sports team or club, this can get tricky. Discuss the issues with adult leaders and coaches about tagging kids in photos and making web pages and Facebook groups private. Lay ground rules with babysitters and fellow parents about posting photos online.

Likewise, tell your child to be respectful and not tag anyone in a status or photo without their permission.

Collecting kids' info

If you run a website, app, or even just a Facebook group that involves kids, it's important to know what information to gather, how to collect and secure it, and who to share it with. We've got a separate guide just for that: Fair practices for collecting information from children.

Beyond safety

Kid's privacy isn't just about protecting them from predators and fraudsters, although that's certainly reason enough. But there's a societal impact on kids who are bombarded by algorithm-triggered advertising and marketing. Kids are impressionable, and their minds can be shaped by what they see online. What they see on the internet is defined by what Google, Facebook, Microsoft, and other corporations that rely on advertising and mass dragnet data collection want them to see.

Likewise, in an age when nothing is forgotten, children are also shaped by what they leave behind. In a Wall Street Journal article, Julia Angwen sums it up best:

"They won't have the freedom I had as a child to transform myself. In junior high school, for example, I wore only pink and turquoise. But when I moved across town for high school, I changed my wardrobe entirely and wore only preppy clothes with penny loafers. Nobody knew about my transformation because I left no trail, except a few dusty photographs in a shoebox in my parents' closet. Try that in the age of Facebook."

The internet can open up more of the world to your child than any generation before them. But we shouldn't allow faceless for-profit corporations to mould them into a class of consumers limited to the online personas that they unknowingly helped to create.