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.