



Parents: Cybersecurity Tips to Teach Your Kids



KIDS ALSO NEED TO UNDERSTAND THE BASICS OF STAYING SAFE ONLINE

October is Cybersecurity Awareness Month — but not just for adults. Kids also need to understand the basics of staying safe online for many reasons, including:

- Since most kids don't have credit reports, cyber criminals are stealing their identities and establishing entire credit histories before their parents even know that fraud is happening.
- There is a disturbing trend involving hackers targeting online video games and encouraging kids to self-harm (e.g. the ["Momo Challenge"](#)).
- Like many adults, kids tend to reuse the same password on multiple accounts and/or use easy-to-crack passwords. Once these accounts have been compromised, hackers can infect PCs or devices and steal confidential information about family members and friends.
- Hackers are posing as friends and relatives in chat rooms in order to get confidential data like passwords, credit card numbers, and so on.

In light of these (and other) serious threats, and the fact that most kids are naturally trusting and don't quite understand the risks, threats and dangers — basically, they just want to have fun online, which is what kids do! — here are some cybersecurity tips to help keep your kids out of harm's way:

Social Media

The first contact of children with social medias these days is at the age of [11.4 years old](#). With this in mind, set the privacy level to maximum for all of your child's social media accounts, turn off location finding, and teach them not to accept requests from people they don't know. Also, if they are not 13, it's not the best idea for them to be on social medias. It's also important for you to keep an eye on what they're doing. No, they aren't going to like this (in fact, they're going to hate it). But your goal isn't to snoop on them. It's to keep them safe!

Phishing

Kids love email links that look interesting and exciting (e.g. "Be the first of all your friends to play this AMAZING new game!"), which means they're happy to "click first and ask questions later". Unfortunately, this is exactly what hackers are counting on.

To avoid this trap, you can dial up the security on your child's email account, so that links are inactive and attachments cannot be downloaded. If your kids are a bit older — or if there are legitimate reasons why they need to click links, like they're working on a school assignment with a classmate — then teach them not to click on suspicious-looking email links (or better yet, have them check with you or another adult before clicking anything). If they're old enough to have a more sophisticated understanding, you can also show them how to check a link's real URL by hovering their mouse over it.

Private Information

Understandably, many kids — especially younger ones — don't know what "[private information](#)" means. Basically, to them, everything is available to anyone who wants to know: from what they had to eat last night, to what they think of the latest Justin Bieber song, to whether they finished their homework assignment (of course they didn't!).

So, it's important to help kids understand the difference between information they should keep to themselves and information they can share with others. For example, it's OK to talk about how great or awful the new Justin Bieber song is, but it's not OK to share passwords — even with their BFF 4EVR.

Devices

If you go to the lost and found in a store, stadium, restaurant or anywhere else, you'll probably find a line-up of parents hoping to [recover the device their child has left behind](#). To avoid this risk — and the replacement cost — teach your kids to keep track of their devices at all times, wherever they go. Consider rewarding them for their good behavior. For example, each month they go without losing their device means a new video game or some other desirable treat.

Avoid Public Wi-Fi

Last but not least, teach your kids not to use public Wi-Fi — which is asking a lot, because Wi-Fi is available everywhere these days: in malls, libraries, stores, and so on. If your kids are old enough and insist on using public Wi-Fi, install a good VPN on their device(s) and teach them how to use it (some are more user-friendly than others).

And while we're on the subject of insecure Wi-Fi networks: contrary to what most adults believe, home networks are usually quite vulnerable as well and need to be secured. Otherwise, hackers can easily breach them.

Make Cybersecurity a Concept — not an Action

Overall, the goal is to help kids understand the importance of cybersecurity. This will keep them and your family safe, and it will further serve them as they get older. Platforms like [Interland](#), an online game that makes learning about cybersecurity fun and interactive, will help them understand the importance of cybersecurity and how to stay safe online. This platform is completely free and you can access it [here](#).

Heck, they might even become cybersecurity professionals, which is a very [smart and lucrative career path](#)!

Your Turn

If you have any kid-focused cybersecurity tips, please share them with the community. What has worked/not worked in your house?