The Bare Minimum You Should Do to Protect Your Family's Data

If you're not ready to #deletefacebook, here are 13 simple things you and your kids can do on your social accounts, phones, and devices to keep data safe. By Caroline Knorr 3/28/2018
Common Sense Media

For a lot of families, technology is maybe not a way of life but the glue that holds everything together. There's your kid's Instagram feed you follow to see what they're up to. There's your school's online network you check for homework and grades. There's the mapping app that gets you to your kids' playdates. And then there are the regular old texts from your kids that say "hi Mom" and let you know all is well. But this connection and convenience comes at a price -- and that's your data. With increasing frequency, we're seeing large privacy violations -- when hackers get access to people's online data or companies misuse it or fail to protect it -- and we all realize how vulnerable we are to identity theft, the publication of sensitive information, and stolen credit card numbers. Technology use comes with privacy risks, but don't worry -- the answer isn't living the life of a Luddite.

The thing is, most of us are far too reliant on technology to stop using it now. You may delete Facebook for a while … but you always go back, because how else are you going to see your cousin's new baby? And how can you tell your kid's teacher your kid can't sign up for Google Classroom when that's how the students work on group projects? It may be a stretch to say we need technology, but we sure don't want to live without it. Fortunately, there are some simple things you can do to reach a higher level of safety and security. It's important that the whole family is on board with these privacy best practices, because your data is only as strong as the weakest link. Do these now:

Use strict privacy settings in apps and on websites. When you or your kid signs up for a new website or app, establish your privacy preferences immediately. The default settings on most apps usually aren't super private, but on popular social media such as Instagram, Musical.ly, and Snapchat, you can control things like who can see what you post, who can contact you, and whose posts you can see.

Enable two-factor authentication. For an added layer of protection, enable two-factor authentication on apps and sites (like Gmail or Facebook) when available. This will help protect your accounts from hackers by sending a code to your phone when you log in from an unfamiliar device.

Beware of phishing scams. Don't open emails, texts, online "security" alerts, text notifications, or other things from anyone you don't know, don't recognize, or weren't expecting. Often this is "phishing" -- companies sending out enticements hoping someone will click on them, thereby allowing entry to your device. Phishers can make their messages look authentic by copying logos from companies such as

Amazon, Google, or even the IRS. But they often make mistakes such as using unusual grammar, weird punctuation, or threatening language.

Use antivirus protection. Buy and download antivirus software from a reputable source such as McAfee, Norton, or Symantec. Beware of free antivirus software, as it can contain malware. The iOS operating system has antivirus software built in, but it can still be vulnerable, so make sure you update your OS when prompted, as the updates can fix security holes.

Don't use unsecure Wi-Fi networks. Make sure any Wi-Fi you connect to has the little lock sign next to it and requires a password. Hackers are notorious for sneaking into unsecured Wi-Fi. Even better, get a VPN (virtual private network) -- but, just like with antivirus software, don't use a free VPN.

Fine-tune your browser settings. Take a look at the privacy settings offered in your browser (usually in the Tools or Settings menus.) Most browsers let you turn off certain features -- for example, the "cookies" that websites install on your computer that track your movements. Some cookies, such as those that remember your login names or items in your online shopping cart, can be beneficial. But some cookies are designed to remember everything you do online, build a profile of your personal information and habits, and sell that information to advertisers and other companies. Consider using plug-ins like Privacy Badger or HTTPS Everywhere to block tracking or keep your activity safer from snoops.

Turn off location services. Unless you use an app that lets you track your kid's location for safety reasons, turn off location services on your phone and your kid's phone. You can turn them on again if you want to find local businesses or use your mapping program.

Don't let apps share data. When you download a social app, it will ask if it can access information stored on your phone, such as your contacts, photos, music, and calendar. Say no. If the app won't work without this data, consider whether you can share some of what it's requesting but not all. Or find a similar app that doesn't overreach.

Be careful with social logins. When you log onto a site or app with your Facebook or Google username and password, you may be agreeing to share certain information from your profile. Read the fine print to know what you're sharing, and edit if possible. Even if you limit what's shared with the third party, your social network will continue to track your behavior.

Do regular privacy checks. Get in the habit of regularly checking your privacy settings on all social apps you use. Do this in front of your kids and narrate the experience to demonstrate how important keeping track of your information is.

Use tough passwords and change them frequently. The best practice for passwords is to use real words or phrases you can remember easily -- but spell them incorrectly. They should be at least eight characters and have a combination of letters, numbers, and special characters, such as 5pEAzhawh$ for "five pizzas." Even better, use a password manager like Lastpass. Get more password tips.

Tweak your home assistants. Keep Alexa and Google Home's microphones off if you're not using them. Also, periodically comb through the settings either on the apps or in your online profile to see what you've shared and whether you need to delete recordings or make other privacy changes.

Cover your cameras. Whether it's with a Post-it or a cute customized cover, block your webcam from potential spies. It might seem paranoid, but even Mark Zuckerberg does it.