Extension Education
Tasha Killian News Column
October 3, 2018

Online Safety
By Tasha Killian

In a similar way that we teach our children to look both ways before cars because the road can be dangerous, we need to teach our children how to avoid dangers in the online world. Below is a simple list to help you keep your children out of certain danger. This list is taken and adapted from a list provided by Common Sense Media. Common Sense Media is a great resource for parents, educators and community members.

Use strict privacy settings in apps and on websites – Most websites and apps allow you to customize your privacy and preference settings. When you sign up for a new website, or download a new app, go through the settings and find what data the app collects, if any, and how to turn off information you'd like to be hidden.

Enable two-factor authentication – Two-factor authentication means that you use two different methods to get into a site or app. Many sites like Gmail or Facebook have the option to set up two-factor authentication, making it harder for hackers to get into your accounts and steal your information.

Beware of phishing scams – A phishing scam is a scam meant to get you to click on or open an email, text, ad, etc. Once you click on it, it can allow for hackers to have access to your devices or give you a virus. Phishing scams can be hard to detect because they usually contain very authentic looking logos and information. The best way to avoid them is to not click on any links or unusual offers from unknown numbers.

Use antivirus protection – Downloading and using antivirus protection from a reputable source can help you avoid unnecessary viruses. Just like a person's immune system is better protected with shots, your devices are better protected when they have antivirus protection downloaded on them.

Don't use unsecure Wi-Fi networks – Imagine you have all the most important things to you in your car. When you stopped somewhere, you'd definitely want to make sure your car doors are locked, right? We need to make sure the Wi-Fi networks we use are locked for the same reason. When we use unsecure Wi-Fi networks, we are allowing hackers and anyone else who can get access to our personal information including our bank account numbers, social media logins, photos, etc. To make sure you are using a secure network, double-check that there is a lock symbol next to the network's name in your settings.

Fine-tune your browser settings – We don't often think about how our activities can be tracked online, they are. Have you ever googled something, or tried to shop online and then been surprised to see ads for that exact same thing all over your devices? That's because of something called cookies. Although cookies sound like they would be a good thing, they aren't always. You can edit your browser settings to limit how websites track and use your online activity.

Turn off location services – Location services can be a great thing if you are looking for a restaurant or store nearby, or need a map to help you find your destination. However, for some apps and websites it isn't necessary and you are voluntarily giving them your location and the ability to track that location. To prevent this, you can go into your browser settings and turn off location services and then turn them back on again only when you need to search for a place. You can also turn them off in your settings on your phone.

Don't let apps share data – Certain apps ask for permission to have your information when you download them. For example, many social media sites will ask to access your contacts, photos, etc. It is okay to say no. If the app won't work without your personal information or access to your phone, it may not be worth downloading.

Be careful with social logins – Although it is fun to find out what dog we would be, or where we should take our dream vacation based on our personality, it can be dangerous to allow apps and websites to connect to your social networking accounts to access your data. Be sure to read through what the app is asking and avoid apps that ask to share your data. Sharing data puts you at risk of having your profiles hacked.

Do regular privacy checks – We use check-ups as a way to do just that, check-up on what we have going on. It is best practice to do a privacy check-up every so often. Sometimes our privacy settings might have changed. Doing a check-up allows you the opportunity to go back in and change settings to your preferences, not what the app or website has decided they be for you.

Use tough passwords and change them frequently – Passwords are fun to set. You have the unique dilemma of deciding what to use that is both secure and easy to remember. According to Common Sense Media, the best passwords to use are those with normal phrases that are easy to remember, but substituting out characters for letters, like this one: B@tm@nR0ck$.

Although it may seem like a big task, being vigilant about privacy online can help you protect yourself and your family. It is important to discuss with your children the practices listed above so that you call all be on the same page regarding privacy procedures for your household.