

Young social media users may be naïve to potential internet dangers. They may:

- Use their full name for their Instagram or Twitter handles.
- Keep their location services on while using apps like Snapchat, Tik Tok or Instagram that could disclose the users' GPS locations.
- Add their phone number and email address to Facebook profiles.

Disclosing this type of information can pose a serious threat to your child and could possibly put the whole family in danger.

As a parent, there is a balance between monitoring your child's online activity and giving him or her the space to be independent and have his or her privacy. The best way to set them up for online safety success is to start having conversations about this important topic at a young age.

The parental speech that warns against talking to strangers and disclosing where you live to strangers is not any different now than it was before the internet became part of how we conduct business and foster friendships.

The conversation you have with your children should be simple and consistent. Tell them do not:

- Speak to an online person or profile with which they are unfamiliar.
- Disclose personal and identifiable information, such as addresses and phone numbers.
- Accept friend requests from people whom they don't know.

Talk to your children, pre-teens, and teenagers about the content of their posts. For example:

- Make sure they understand the consequences of posting certain ideas, articles, or commentaries, such as ones that promote violence or hate.
- Help them be mindful when posting pictures to their profiles. For instance, posting pictures of real or simulated violence or criminal activity is inappropriate and illegal. In addition, remind your children to gain permission from anyone else in the photo before posting it.
- Explain that tagging locations on social media can also be problematic as it exposes the user's location to online predators.
- Log out of profiles on the computer when you are finished using them. By doing this, you can ensure others cannot immediately access your social media accounts while using the same computer.



All social media accounts have a privacy setting available to the user. The settings are customizable. On Facebook, the user can make his or her content, profile pictures, and photo albums available only to his or her friends. Similarly, on Instagram, users can make the profiles private and friend requests have to be sent and approved for the profile to be viewable.

You can protect yourself with these STOP. THINK. CONNECT. tips:

Keep security software current: Having the latest security software and up-to-date web browser can protect against online threats.

Own your online presence: Set your privacy and security settings on your profiles to your comfort level. You can limit as much, or as little, as you'd like, even to your friends.

Make a strong password or passphrase: It should be at least 12 characters with uppercase and lowercase letters, spaces, and special characters. It can even be a phrase or a sentence! Make sure it is something unique and something you can remember. Also – do not have the same password or passphrase for all of your accounts. Mix it up!

When in doubt, throw it out: Phishing is what hackers do to try and see your personal information. Phishing can come in the form of emailed links, tweets, messages, or online advertising that may look suspicious to you. If you are unsure, delete it. Clicking on phishing links can leave you exposed to online hackers.

Use the Golden Rule: Post about others as you would have them post about you. If you don't have anything nice or helpful to say, don't say it at all.

Reference

Womens Law.org. (2018). Safety while using social media. [Safety Tips]. <https://www.womenslaw.org/about-abuse/safety-tips/safety-social-media/basic-information>

Passwords

Using strong passwords is vital to online safety. Here are some basic rules for creating protective passwords.

- Use a mix of uppercase and lowercase letters, special characters, numbers, and symbols.
- You can also make your password something most people wouldn't think of or know about you, like your favorite food.
- Do not use the same password for all of your accounts.

