Action for Children

Talking to Teens about Cybersecurity

FIRST THINGS FIRST

Take your passwords very seriously. You ARE NOT more clever than professional hackers. Use password management tools.

PASSWORD MANAGEMENT

https://www.pcmag.com/picks/the-best-password-managers

CYBERSECURITY BASICS[1]

According to the Federal Trade Commission, it's a good idea to check your child's credit report near the age of 16 so you'll have time to fix any errors before they take out that first loan or apply for their first job. Learn more about child identity protection here: https://www.consumer.ftc.gov/articles/0040-child-identity-theft

PRIVACY AND SECURITY SETTINGS EXIST FOR A REASON

Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.

ONCE POSTED, ALWAYS POSTED

Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70 percent of job recruiters rejected candidates based on information they found online.

KEEP PERSONAL INFO PERSONAL

Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data or commit other crimes such as stalking.

[1] https://staysafeonline.org/wp-content/uploads/2020/04/Talking-to-Teens-About-Cybersecurity-.pdf

KNOW AND MANAGE YOUR FRIENDS

Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know and trust) up to date with your daily life. Also, you don't have to accept friend requests from everyone. If you don't know someone, it's perfectly fine not to accept their request to connect.

KNOW WHAT ACTION TO TAKE

If someone is harassing or threatening you, remove them from your friends list, block them and report them to the site administrator.

KEEP YOUR SECURITY SOFTWARE CURRENT

Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats. Don't click postpone. A cyber criminal gaining access to your information will be way more inconvenient than updating your software.

MAKE YOUR PASSPHRASES A SENTENCE

A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces.

WHEN IN DOUBT, THROW IT OUT

Links in email, tweets, texts, posts, social media messages and online advertising are an easy way for cyber criminals to get to you. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. Essentially, just don't trust links.