September 2019
Volume 14, Issue 9

Cybersecurity Tips for K-12 Kids, Family, and Friends

Every child should be taught how to be safe online. In the new digital world, there are technological wonders, which often introduce cyber threats of many kinds. The online world can be a place of inappropriate conduct and content, where kids may feel anonymous. There are bullies, predators, hackers, and scammers that may pose a threat to your children. These factors can make it challenging for parents to guide their children today on interacting with others through technology. Providing this important guidance on online safety and privacy begins with talking about it and encouraging safe and smart decisions about online activity. Let's explore some concepts and tips that apply to keeping everyone safe online, regardless of age!

What are the risks?

The online world has many cyber risks and concerning activities for kids and parents to recognize. The following are some of the cyber risks:

- **Cyberbullying** is bullying that happens online. It can happen in an email, a text message, an app, an online game, or on a social networking site.
- **Phishing/Identity Theft** is when a scam artist sends text, email, or pop-up messages in a browser to get people to share their personal information. They can then use that information to commit identity theft.
- **Sexting** is the sending or forwarding of sexually explicit photos, videos, or messages from a mobile phone. In addition to risking their reputations, friendships, and safety, this could be illegal activity.
- **Social Networking** can help kids connect with family and friends, but it can invite danger if not used appropriately. Sharing too much information, posting pictures, videos, or words can damage reputation, hurt someone else, or invite a predator to contact the user. Once something is online, it may not easily be removed. Oversharing may be leveraged by online criminals to facilitate identity theft.

What can you do?

- Start at an early age! As soon as children can use a computing device, it is time to talk to them about using it safely. Parents and family have the best opportunity to teach children!
- Know what your kids are doing. Consider having a common area in the house for the family to do online activity, where children can feel independent, but not alone.
- Keep an open and honest environment. Let your children know they can come to you with any concerns or questions about their online experience.

- Protect your children's information. Don't over-share information about your children, and teach them this principle. Set social media accounts so only approved friends can see their content.
- Respond appropriately to cyberbullying. Tell children to ignore or block bullies, unless it becomes threatening. Report abuse to the website where it is taking place, or if you fear for your child's safety, report it to the authorities.
- Configure the security and privacy features on devices. Change default settings on your devices and enable security features like strong passwords, auto-updates, etc.
- Keep all your computers and mobile computing devices up to date with the latest security patches and anti-malware software.
- Consider installing or enabling parental controls on devices.
- Teach kids to be cautious of suspicious messages. Forward phishing emails to spam@uce.gov and reportphishing@antiphishing.org.

Additional Resources:
https://staysafeonline.org/stay-safe-online/managing-your-privacy/tips-parents-raising-privacy-savvy-kids/

https://www.consumer.ftc.gov/features/feature-0038-onguardonline

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK
CONNECT