OUCH! September 2023

Online Security for Kids

Background

Our kids' lives are online today more than ever, from socializing with friends and gaming, to online learning and education. So how can we help our kids make the most of online technology, safely and securely?

Education and Communication

First and foremost, make sure that you foster good open communications with your children. Far too often, parents get caught up in the technology required to block content or determining which mobile apps are good or bad. Ultimately, keeping kids safe is less about technology and more about behavior and values. A good place to start is to create a list of expectations with your kids. Here are some factors to consider (Note that these rules should evolve as kids get older.):

- Decide on times when they can or cannot go online for fun, and for how long. For example, you may want to be sure children complete all homework or chores before gaming online or social networking with friends, and limit the amount of time they do spend online each day.
- Identify the types of websites, mobile apps, and games that they can access online and why they are appropriate or not.
- Determine what information they can share and with whom. Children often do not realize that what they post online is public, permanent, and accessible to anyone. In addition, anything they share privately with their friends can (and often is) shared with others without them knowing.
- Identify who they should report problems to, such as strange pop-ups, scary websites, or if someone online is being a bully or creepy. It's critical that children feel safe talking to a trusted adult.
- Just like in the real world, teach children to treat others online as they would want to be treated themselves, with respect and dignity.
- Ensure children understand that people online may not be who they claim to be, and that not all information is accurate or truthful.
- Define what can be purchased online and by whom, including in-game purchases.

Over time, the better they behave and the more trust they gain, the more flexibility you may want to give them. Once you decide on the rules, post them in the house. Even better, have your kids contribute to the rules and sign the document so that everyone is in full agreement.

The earlier you start talking to your kids about your expectations, the better. Not sure how to start the conversation? Ask them which apps they are using and how they work. Put your child in the role of teacher and have them show you what they are doing online. Consider giving them some "What if…" scenarios to reinforce the positive digital behaviors you've discussed or agreed upon. Keeping communication open and active is the best way to help kids stay safe in today's digital world.

For mobile devices, consider a central charging station somewhere in your house. Before your children go to bed at night, have a specific time when all mobile devices are placed at the charging station so your children are not tempted to use them when they should be sleeping.

Security Technologies and Parental Controls

There are security technologies and parental controls you can use to monitor and help enforce the rules you set. These solutions tend to work best for younger children. Older kids not only need more access to the internet but often use devices that you may not control or cannot monitor, such as school-issued devices, gaming consoles, or devices at a friend's or relative's house. In addition, older children can often circumvent purely technological attempts to control them. This is why, ultimately, communication, values, and trust with children are so important.

Leading by Example

Remember to set a good example as parents or guardians. When your kids talk to you, put your own digital device down and give them your full attention. Consider not using digital devices at the dinner table, and never text while driving. Finally, when kids make mistakes, treat each one as an experience to learn from instead of simply punishing them. Make sure they feel safe approaching you when they experience anything uncomfortable or realize they have made a mistake online.

Guest Editor

Diana Kelley is a Board member at WiCyS and the CISO at Protect AI. She is the instructor for the LinkedIn Learning Course: Security Risks in AI (Artificial Intelligence) and ML (Machine Learning) and co-author of the book Practical Cybersecurity Architecture.

Resources

Securely Gaming Online: https://www.sans.org/newsletters/ouch/securely-gaming-online/
Privacy: Protecting Your Digital Footprint: https://www.sans.org/newsletters/ouch/privacy/
Securing Your Mobile Device: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
Deep Fakes: https://www.sans.org/newsletters/ouch/learn-a-new-survival-skill-spotting-deepfakes/