Cybersecurity for Families

As technology continues to evolve, the tools and toys available to your children increase in number and evolve in capabilities. Technology can be used to educate and inspire creativity in kids, but it also exposes them to a risky landscape most of us didn't have to worry about during childhood. Adults can discuss with children how the digital world is a great resource, but we must remain cyber aware. We all should be responsible with the information we share, and the ways we explore.

Here are a few things we should all do to protect our kids and our home networks.

Keep Software Updated:

Think of all the devices in your household that connect to the internet - phones, tablets, computers, gaming systems, smart appliances, even lightbulbs! One of the most important things you can do to keep your devices safe is to ensure your devices are up to date and using the latest software. When your devices notify you about a software update, install the update right away, or set them to automatically update. Those updates contain security patches that close loopholes that hackers can use to gain entry and access your data like your passwords, payment information, photos, and more.

Always make sure you know what apps are on your children's devices, know what those apps do, and what type of information they monitor or collect. This can be done easily by checking the app settings and privacy disclosures.

If you have children prone to installing anything that looks new and flashy, consider requiring a PIN or password you only know before allowing installation of new applications.

Implement Domain Name System (DNS) Filtering:

As we all know, surfing the web can be a risky business. While we can usually identify scams and malicious links, children may not catch on so quickly and see that the link their friend's hacked account just sent them for a free game is a malicious website in disguise.

Implementing DNS filtering, which prevents devices on your network from connecting to known bad websites, is a free and easy way to help prevent everything from phishing and ransomware, to spyware and viruses. It is so useful, some of largest IT companies in the world have joined forces to provide it for free to public users. This includes no sign ups, tracking, or personal information saved by those providers. DNS filtering can even be set up on your home router with very little effort, which will help protect anyone or device on your entire network. DNS filtering services can also be used to implement parental controls to deter kids to going to unwanted or inappropriate websites. You can additionally limit kids' screen time and monitor their online surfing activity if you choose to do so. By doing this, you can create a family-friendly online space in your home while also protecting your identity and blocking cyber-villains.

DNS filtering options for families –

- Quad 9: When your computer performs any Internet transaction that uses the DNS (and most transactions do), Quad9 blocks lookups of malicious host names from an up-to-the-minute list of threats. https://www.quad9.net/
- Cleanbrowsing: A free DNS system that focuses on privacy for households with children. It provides 3 free filter options and blocks most adult sites. https://cleanbrowsing.org/
- OpenDNS: Owned by Cisco, OpenDNS has two free options: Family Shield and Home. These are incredibly useful for monitoring and preventing adult site access as well as general internet safety and performance. https://www.opendns.com/

Talk to Your Kids:

Finally, make sure you talk to your kids about cybersecurity. Just like other issues that have the potential to harm our children, keeping an open line of communication regarding cybersecurity is vital to keeping them safe.

Outside of adjusting privacy settings and parental controls on devices your kids use, make sure they learn how to spot unusual behavior and encourage them to tell you about it. Teach your kids about proper online etiquette and encourage appropriate interactions.

Supervise their screen time and make sure you are in the know about who they talk to and interact with online. Talk to them about the importance of keeping some information private – such as your name, home address, and phone number.

Check their apps and devices frequently to make sure your kids haven't turned on location sharing or made their social media accounts public to anyone and everyone. As they get older, remind them that once information is online it can't be taken back – it's online forever.

Cybersecurity was not something past generations of parents had to worry about when raising their children but is a big part of all our lives now. And even though we may not like all that comes with these technologies, they're here to stay and it is imperative that we teach our children how to responsibly and safely use them. Let's give our children the foundation they need to be able to safely and securely engage in today's connected world.
