CYBER SECURITY AWARENESS TIPS - November 2017

Guarding Against Online Predators

In this age of social media, at some point every parent worries about the possibility that their child my encounter an online predator. While it's smart to be cautious, instead of acting out of fear, parents should arm themselves with information so that they can help their kids be smart, cautious, and savvy online. Use some of the following strategies to be proactive in protecting your kids.

Help your kids set the privacy controls on their social media accounts

If your children share messages, pictures or videos on Facebook, Instagram and other platforms, they might not be aware of who can see their posts. Most apps do have privacy settings that let your children control who they let into their lives. Here are links to information about the privacy settings on a few of the most popular apps:

- Facebook
- Instagram
- Snapchat

Set up separate accounts for your kids on your computers and mobile devices

If you share a device with your children, set up separate user accounts for them. Each account will have its own home screen and, depending on the device and platform, a different selection of features, apps, and permissions. This helps you to protect your own data or video and it also allows you to set up customized security and privacy settings for each child. Use the **Settings** app on individual devices to enable restrictions.

Secure your gaming systems

Don't forget that your gaming console is also an Internet device these days. Children can download games and make in-game purchases, and even surf the Web. Most devices have features that allow you to restrict the kind of content your children can get, limit their purchasing capabilities and restrict or turn off their Web browsing.

Consider using kid-safe browsers and search engines

For added control, you can install a kid-safe web browser for your children to use. There's a free version for Windows PCs and Macs, and for Android and iOS tablets and smartphones. These typically include ad blocking, time limits, and other features.

Most commonly used browsers have the capabilities to set up a "supervised profile." This will block explicit search results, show you what websites your children visited, and even restrict what websites they can go to. The restrictions work in two ways: You can have a list of approved websites and your children can visit those sites only or, you can pre-ban a list of websites that your children are not allowed to visit. For example, here's Google Chrome's supervised profile information.

There are several kid-safe search engines that provide a way for kids at home and in schools to research the internet more safely using strict filtered results. These search engines help to block content that may not be appropriate for children. Safe Search Kids is powered by Google to deliver filtered search results.

Use an app that limits the time your child spends online

According to the Pew Research Institute, 50 percent of parents have used parental control tools to block, monitor, or filter their child's online activities.

For information on parental control apps, visit the tom's guide website, which offers comparisons of a wide variety of technology products based on research, tests and reviews to provide recommendations to consumers. The site also provides product tutorials and tech-related community forums for knowledge sharing.

Make sure your kids are only using safe chat rooms

Some kid-friendly platforms offer chat rooms where kids can talk to other kids. If you allow your child to visit online chat rooms, vet the sites first to make sure that someone monitors the chat rooms. And teach your kids not to share their real identities on such platforms but to use anonymous screen names instead.

Teach your children not to respond to messages from strangers

Teach your children to delete any text messages, instant messages, emails or social media messages from people they don't know. Make sure they know not to open it, not to respond to it, and, of course, not to click on any links or attachments.

Educate your children about the risks of texting inappropriate pictures of themselves or others

Besides the psychological damage, children who both send and receive these types of pictures are breaking the law and it could result in criminal prosecution.

Warn your kids about online polls and surveys

There are lots of fun, harmless polls out there, like the one that tells you what kind of poodle you are. But many ask for too much personal information, and could land your kids on spammers' email lists, or open them up to identity theft. If your child has a legitimate reason to fill in questionnaires needing an email address, consider helping them set up a second email account of their own.

Know your children's online friends

As with their off-line friends, confirm their identities, and talk to those kids' parents. Be sure that those "kids" are, in fact, kids.

Set a good example

Before lecturing your kids about staying safe, make sure that you yourself are a good model. Learn about the privacy settings in the social media apps you use most, then check that you aren't sharing private, personal moments with the whole Internet.

Set rules about what your kids can share online

Make sure your kids know the rules about what information you allow them to post online and that they understand the reasons behind them. Even seemingly innocuous information, like vacation pictures, can let criminals know when your house is empty. Some things are best not shared online at all.

The Family Online Safety Institute (FOSI) is an international, non-profit organization which works to make the online world safer for kids and their families. It is also a respected resource for information and guidelines on internet use.

The FOSI also has a sample Online Safety Contract that can be used to set up ground rules with your children for safer and more responsible use of technology.

Add your kids as a "Friend"

If your children have their own accounts on Twitter, Facebook, Google Plus, Instagram, Snapchat or other social media sites, follow or friend them. You'll be able to see if they're posting inappropriate things online and can step in before problems escalate. Don't let your kids tell you that "other parents don't do this." According to the Pew Research Center:

- 61% of parents say they have ever checked which websites their teen visits
- 60% have ever checked their teen's social media profiles
- 56% have ever friended or followed their teen on Facebook, Twitter or some other social media platform
- 48% have ever looked through their teen's phone call records or text messages