Be Thankful for Good Cybersecurity Habits!

Last month the Law Enforcement Volunteers of California (LEVOC) hosted their 20th annual conference in Lodi. Over 500 volunteers attended the LEVOC annual awards for excellence and for professional learning. This year, two detectives demonstrated some of the current techniques in high tech crime investigations. Detective Daniel Garcia of the Tracy Police Department, a cyber investigation expert, uses technology to gather evidence to prosecute child predators. He talked about how information technology (IT) provides these predators unsupervised access to children. He emphasized the need for parents to make sure that their children are aware of internet and mobile device safety guidelines. Both social media sites and mobile devices offer many free, easy to install apps which can be given access to location services and private information which can be used to compromise our safety.

Every child should be taught how to be safe when using IT, whether they are online, using a mobile device, or any of the many internet of things (IOT) devices commonly found in the home. These technological wonders often introduce cyber threats of many kinds. There are bullies, predators, hackers, and scammers that may pose a threat to your children. According to Detective Garcia, providing guidance to 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 keep everyone safe online, regardless of age!

In 2019, the Department of Homeland Security cybersecurity theme is: "Own IT. Secure IT. Protect IT." Each of us plays a role in online safety and must take proactive steps to enhance cybersecurity at home, at school, in the workplace, and any public setting where IOT devices are available.

"Own IT:" Understand your digital profile and the devices and applications you use every day to help keep you and your information safe and secure.

- Stay safe on social media. Sharing too much information, posting pictures, or videos can damage the 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. Parents should help their children to use available privacy settings.
- Make sure that you and your kids know how to restrict cell phone apps from accessing certain features, such as location services.

"Secure IT:" Secure your digital profile. Cybercriminals are very good at getting personal information from unsuspecting victims, and the methods are getting more sophisticated as technology evolves. Protect against cyber threats by learning about security features available

on the equipment and software you use. Apply additional layers of security to your devices – like Multi-Factor Authentication (MFA), to better protect your personal information.

- Customize your standard password for different sites, which can prevent cybercriminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts.
- Enable MFA to ensure that the only person who has access to your account is you. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone.

“Protect IT:” Maintain your digital profile. Every click, share, send, and post you make creates a digital trail that can be exploited by cybercriminals. To protect yourself from becoming a cybercrime victim you must understand, secure, and maintain your digital profile. Be familiar with and routinely check privacy settings to help protect your privacy and limit cybercrimes.

- Whether it’s your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with antivirus software.
- Before you connect to any public wireless hotspot, be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities, such as banking, that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi.

This November, as you prepare your list for Black Friday shopping, keep these safety tips in mind and you will be thankful that you used good cybersecurity habits!