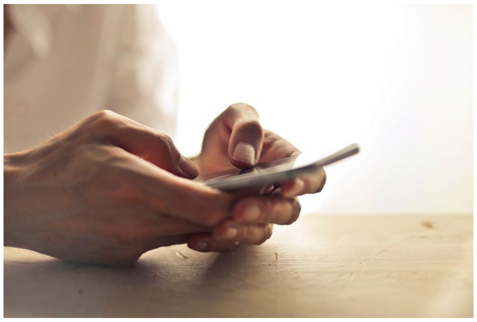
School Sisters of Notre Dame
Central Pacific Province

National Cybersecurity Awareness Month

MISSION STATEMENT

As Information Technology professionals for the School Sisters of Notre Dame, we believe it is essential to our plan that all technologies implemented be effective, functional, secure and driven by the mission. We commit ourselves to being good stewards of the Information Technology department by developing and making our sisters, personnel, resources, and finances a priority in moving forward.



SEVEN WAYS TO SAFEGUARDING YOUR MOBILE PHONE

By Patrick Conley, IT

Your mobile phone goes with you everywhere. Not only is it a telephone for making and receiving calls from just about anywhere, but it's also a powerful computer that can store and access your private and work data.

We can argue the usefulness of mobile phones beyond our basic need to communicate with each other. The truth of the matter is that mobile devices over the past two decades have permeated our daily lives and have changed the way we spend our personal time and conduct business. There are a plethora of mobile "apps" at our fingertips now that supplement our social lives, allow us to play games, shop and bank online, and give us instant access to business (work) systems.

We leave our personal lives and employers at risk when our mobile devices are not protected properly. So beyond never forgetting to leave your phone at the restaurant table, in the Uber drivers' car, or at the wedding reception, what do we need to do to make sure that cybercriminals or someone in the booth next to us doesn't lift our mobile device?

Rule #1: Use a passcode

Yes, we know it's a hassle. Yet it's the easiest way to prevent Joe Schmo from grabbing your phone and gaining instant access to every aspect of your life and job. Most employers won't let you use your personal mobile phone for business use without a passcode or passphrase. Do it! You'll get used to unlocking your phone. 😊 Steps on setting up a passcode for an iPhone and on an Android (Galaxy, etc).

Rule #2: Update your phone software and apps

There is a reason behind the regular updates to your phone's operating system and apps. The developers are staying one step ahead of hackers and ensuring your phone is as secure as possible. Don't delay! Install those updates – steps for Apple iPhones and Android phones.

Rule #3: Back up your data

For iPhone users, back up your phone data to iCloud. Android phone users can back up data with syncing to Google. Your phone settings, photos, and documents can be easily restored if your phone is lost.

Rule #4: Stick to your phone app store

The iPhone App Store and Android Google Play are certified locations for developers to place their apps. Both Apple and Google scan apps in their store for malware. Your phone will update apps with newer versions from the app store. This will ensure your phone is secure as possible. Downloading apps from other locations may not be as secure.

Rule #5: Set up Find My Phone and Find My Mobile

Apple iPhones have an app called Find My iPhone and Android has Find My Mobile. Enabling these apps will allow you to find your mobile phone if it is lost. If you can't find your phone, you can remotely wipe the data on it. That way a stranger can't use your mobile phone or access your private data.

Rule #6: Ignore suspicious emails

The easiest way for hackers to gain access to your data is through email. Avoid opening email links, attachments, or downloads. If you do not know the email sender, question it and contact the IT department.

Rule #7: Use secure WiFi

When you connect to a public WiFi network you open your phone to anyone else on that network. Hackers will use an unsecured WiFi network to spy on your mobile phone. General web browsing is fine but ordering that favorite pair of socks online or doing banking should be done on your mobile phone providers network rather than unsecured WiFi.

We are here to help! Contact Help Desk at 1-800-373-7521 or via email helpdesk@ssndcp.org. You can continue to follow us online during the month of October for our weekly security articles!