TRAVELING WITH SMARTPHONES

- **Do** enable password and fingerprint locks on your device. Also, protect "Settings" changes on your phone by requiring a password.
- **Do** assume that all information on your device can be accessed remotely. Don't store passwords and sensitive information on your phone.
- **Do** always use complex passwords. The stronger and longer the password, the more difficult it will be for someone to hack into your phone.
- **Do** delete emails that are old or no longer needed prior to travel. Remember that emails contain a lot of personal information. Think about what a hacker might gain if they were able to access your email.
- **Don't** become complacent upon returning from your travels. Examine your smartphone as soon as you return home. If it is acting up or repeatedly making you put your password in, there may be malware on your device. In that case, you may want to take it in or consider getting a new device.
- **Don't** link apps and social media accounts together (e.g., using one SM account to login to another). Remember, if someone hacks into one of your accounts, it is better if they only get access to that one. Linking accounts together makes all of them vulnerable.
- **Don't** leave GPS, Bluetooth, and wifi turned on when traveling. Leaving any of these on could allow a hacker to connect to your phone if able to get within a certain distance from you.

Wifi Safety Tip

Avoid Public wifi at all costs as hackers will often name a network the same thing as the hotel or other public network. Hackers in Europe have been caught making Public wifi networks to resemble public network names. Do not assume all networks are secure. Just because it says the name of a company does not mean it is a legitimate network. Check with the company to be sure. Also, be sure to turn your wifi off when you are not using it in order to prevent remote tracking or hacking of your phone.

Precautionary Tips

- Be aware that your phone may be forensically scanned when entering a foreign country.
- Set your phone to lock automatically and ensure you have a complex password or fingerprint enabled while traveling. This will help limit an intruder's ability to break into your phone if you happen to misplace it.
- Consider installing a VPN to ensure more secure online activity.
- Turn off wifi and Bluetooth when traveling. Only turn on these capabilities when absolutely necessary, then turn them off when done.
- Purchase SIM cards for international travel in the U.S. prior to departure. This will ensure not only your security, but functionality with your device. If you decide to use a SIM card, make sure to turn off "Auto Sync" to conserve your battery and data plan.
- Make sure all software is updated on your phone, as this will ensure the most up to date security patches are installed on your device.
- Make sure to backup all your data before traveling so that if your phone or data is lost, you can easily restore the information and won't be without important contacts and travel information.
- When feasible, it is recommended to purchase a pay-as-you-go phone for travel, especially for travel overseas. This is probably the single best way to prevent your personal information from getting into the wrong hands should you lose the phone.
- Make sure to use your own charger and cables. Try not to purchase them from your destination if possible.