Mobile Device Security Tips:

- **Keep your device locked –** In the event that your device is lost or stolen having a lock on your phone whether it is a passcode, pattern, fingerprint etc. will prevent others from being able to use your device without your permission.
- **Use secure passwords –** Using secure strong passwords will help make it harder for a hacker to guess them.
- **Keep your devices operating system updated –** Updating your device's operating system when notified to do so helps patch security gaps and improve your device's overall performance.
- **Connect via secure Wi-Fi –** A Public WiFi network is less secure than your personal, private one, because you don't know who set it up or who else is connecting to it.
- **Only download apps from trusted sources –** Download apps only from trusted sources such as the Google Play store or App store. It is also suggested to check the privacy policy, ratings, and reviews of an app before downloading.
- **Encrypt your data –** Encryption is defined as the process of converting information or data into a code, especially to prevent unauthorized access. Encrypting the data on your device makes the information on your device unreadable.
- **Don't jailbreak or root your phone –** Jailbreaking/Rooting is the process of removing the limitations put in place by a device's manufacturer. Jailbreaking/Rooting is generally done to allow the installation of third party apps outside the app store. Jailbreaking/Rooting can create large security gaps that allow malware to infect your device, leaving your personal information at risk.
- **Enable two-factor authentication –** Two factor authentication is basically adding a second layer of protection to your account, app or service to go alongside your regular method of logging in. An example of two-factor authentication would be receiving a code SMS/text and having to enter that in addition to your password.
- **Audit your apps to see what information they are accessing –** Apps require permissions. App permissions are the privileges an app has like being able to access your device's camera or contact list. Generally trusted developers wont request anything that they don't need for the app to function but that's not always the case-a good rule of thumb is that if you don't plan on using a feature offered by the app that you might as well disallow it. Example: Facebook Messenger asks for access to your microphone not because it's eavesdropping on you but because it does have a voice-memo function if you do not plan to use this function then you could disallow it.
- **Always backup your data –** The main reason for a data backup is to have a secure archive of your important information, so that you can restore your device quickly and seamlessly in the event of data loss.