Strategies to secure your mobile devices

1. **Create a PIN or passcode for your device.** You can still answer incoming calls without entering PIN/passcode. Set it to automatically timeout and request PIN re-entry (shorter the better). Most importantly, enable the option to “erase data” after certain number of failed attempts.

2. **Keep your firmware and apps updated.** Whenever you see updates available on your phone operating system or apps, update them.

3. **Turn off services when not in use.** Wi-Fi, Bluetooth, and other virtual private networks are handy to have when you’re using them but when you’re not; they can expose your device to unwelcome remote connections. Not only will this prolong your battery life, but also it will help secure your device.

4. **Encrypt sensitive data.** With iOS devices, once you enable PIN/Passcode, it enables encryption. With android or other devices, you have to enable encryption manually or use third-party app from reputable vendor.

5. **Backup your data.** Having your data available to you if your mobile device is lost or stolen is key in being able to recover sensitive data. Remote erase your data in case of lost or stolen is needed but with backup you don’t lose the data.

6. **Be selective.** The more information you put on your smart device, the more you are opening yourself up to security issues. Store as little personally identifiable information on your smart device as possible. Even reputable companies can make mistakes and leave security loopholes wide open for hackers. Many apps may not be reputable and will steal data and many do not use encryption properly (or at all) so passwords and other data may be exposed, especially when using wireless. It can be safer to use a browser and access a secure web site than use a dedicated app.

7. **Have a plan if your device is lost/stolen.** Consider installing an app that allow you to find, lock, or wipe your phone remotely if lost or stolen such as Find my iPhone, Lookout, Lost Phone, or Autowipe. Label your device with minimal information. Put an email address or an office phone number on the device so if it is found it can be identified and returned to you. If your device is lost/stolen:
   a. Immediately change all passwords for accounts accessed on the smart device, especially e-mail accounts.

8. **Clear web browser cache on mobile devices.** This will make sure there is not traces left on mobile devices of your website and data access.