Mobile Device Security Best Practices

- **Lock your device with a Personal Identification Number (PIN).**
  Activating the PIN option on your device, as well as utilizing the auto-lock timer feature will help secure the information on your device, especially if the device is lost or stolen.

- **Turn off Wi-Fi and Bluetooth services when they are not in use.**
  Unsecured Wi-Fi connections and Bluetooth signals can be used by criminals to gain access to information on your mobile device. Banking or shopping using a mobile device should only be done when using a secure Wi-Fi connection. Disabling these connections when they are not in use provides another layer of protection that can prevent criminals from gaining access to your device.

- **Avoid sending personal information via Text or Email.**
  As a general rule, never reply to a text or email with any personal information such as account numbers, passwords, or any other sensitive information. It is recommended to contact the business directly to confirm the legitimacy of the request.

- **Keep your device updated.**
  Software updates for your device often include security updates. Be sure to install software updates as they become available.

- **Do not “Jail-Break” your mobile device.**
  Hacking or “jail-breaking” a device creates security vulnerabilities. A hacked device may allow a user more control over what kinds of apps can be installed, but it also makes a device more vulnerable to exploits by criminals.

- **Only install Apps from trusted sources**
  Be sure to only download apps from reputable sources such as the Google Play store or Apple App Store. Be sure to read the app's privacy policy regarding what data the app will need access to on your device. Some apps may request access to data on your device that you may not be comfortable sharing.