http://www.cybersecdaily.com Mobile Device Tips:

NOTE: The following best practices are listed in order of priority.

1. **Passcode**

   Setting up and using a passcode on your mobile device is the first and foremost thing you should do.

2. **Tracking and Wiping Tool**

   Install a remote tracking and wiping tool to track a lost device and, if necessary, to delete private information remotely.

3. **Public Wi-Fi Hotspots**

   Do not allow a device to automatically connect to insecure public Wi-Fi hotspots like those in coffee shops or airports.

   Never pay bills or do banking on devices using public Wi-Fi, because it makes you a prime target for cybercrime.

4. **Mobile Payments**

   At businesses that accept mobile payments, never allow a clerk to take the mobile device out of sight.

5. **Important Documents**

   Never put scanned digital copies of important documents, such as a driver's license or passport, on a mobile device.

6. **Vishing (Voice Phishing)**

   Be on alert for "vishing," or voice phishing. Criminals call masquerading as bank or credit card employees, saying they need a bank account or Social Security number. Never share those details over your mobile device. Call the company's customer service department on a main number. Calls can come from anywhere in the world, but look as though they are from the United States.

7. **Browsing Mobile Sites**

   Beware of browsing mobile sites. Criminals are setting up fake websites to resemble real ones of trusted entities. Since mobile views of websites often look different from regular company websites, many people do not suspect a problem.