PINNACLE BANK

Tips to Secure Your Mobile Devices

As consumer and business use of mobile devices continues to climb, cyber criminals are targeting those gadgets more frequently. Remember that your smart phone and tablets should be treated like a computer; and any device used to connect to the Internet needs to be protected.

The American Bankers Association and Pinnacle Bank advise using the following practices to protect your mobile device.

- ✓ **Use the passcode and/or biometrics lock on your devices.**
  This will make it more difficult for thieves to access your information if your device is lost or stolen. Ensure no additional users are added to your phone's biometric feature. *(e.g., storing a friend or family members face ID or Touch ID on your phone may allow them to override and access applications.)*

- ✓ **Log out completely when you finish a mobile banking session.**

- ✓ **Always backup your device's data.**
  Feel safe knowing your photos, apps and contacts are secure in case your device gets lost, stolen or destroyed. Make sure that you sync your phone, and that data is backed up to the cloud or a personal external drive.

- ✓ **Use caution when downloading apps and avoid downloading apps from third party sites.**
  Apps can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary "permissions."

- ✓ **Keep your operating systems and applications up to date with the latest versions.**

- ✓ **Avoid storing sensitive information on your device.**
  Such as passwords, social security number, photos of driver's license etc. in an unsecured location within your mobile device.

- ✓ **Tell your financial institution immediately if you change your phone number or lose your mobile device.**

- ✓ **Be aware of shoulder surfers.**
  The most basic form of information theft is observation; be aware of your surroundings especially when you're inputting sensitive information.

- ✓ **Wipe your mobile device before you donate, sell, or trade it.**
  You can reset your device using specialized software or using the manufacturer's recommended technique, some software allows you to wipe your device remotely if it is lost or stolen.

- ✓ **Beware of mobile phishing.**
  Avoid opening links and attachments in emails and texts, especially from senders you don't know, and be wary of ads *(not from your security provider)* claiming that your device is infected.

- ✓ **Watch out for public Wi-Fi & Turn off Wi-Fi & Bluetooth when not in use.**
  Public connections aren't very secure, so don't perform banking transactions on a public network. If you need to access your account, try disabling the Wi-Fi and switching to your mobile network.

- ✓ **Take advantage of multi-factor authentication methods when available.**
  This can include ensuring carrier security questions are up to date; and if applicable adding a PIN to your account.
  Pinnacle Bank will never contact you on an unsolicited basis and request customer provisions of electronic banking credentials.

- ✓ **Review your application and security settings regularly.**
  Ensure you can track and lock your device if lost or stolen, and that no suspicious settings are enabled for an application when not needed.