# MOBILE BANKING SAFETY & SECURITY TIPS

While technology continues to provide opportunities for consumers with the convenience of banking when and where you want; along with this convenience come some added security risks. You can help protect yourself from these risks by following a few best practices.

**Be proactive in securing your mobile device**

- Set up a unique Username and a "strong" Password for Mobile Banking. Don't give this information to anyone.
- Password Protect your mobile device. Set your device to require an access password and enable your screen to auto-lock to keep your information private.
- Keep all mobile software, antivirus and malware programs up-to-date.
- Don't save or store login credentials on your mobile device. While this may provide you easy access, storing login information could be more easily accessible to others, including fraudsters.
- Be sure to log out of each application immediately after use, including your Mobile Banking session. Before exiting or navigating away from Mobile Banking, be sure to log out of your banking session to ensure your account information is not easily accessed if your phone is compromised.
- Create nicknames for your bank accounts. (For example, My Checking or Joe Savings). A nickname helps to ensure that your account numbers aren't visible when you are accessing your account from your mobile device.

**Be careful about where and how you conduct transactions**

- Before downloading applications, know if the application (app) you are downloading will access, store, or even share your data.
- Don't use an unsecured Wi-Fi network, such as those found at coffee shops, because fraudsters might be able to access the information you are transmitting or viewing.
- Trust your browser. Your web browser wants to help you stay safe. If you get any warnings (such as untrusted certificates or similar), especially unexpected warnings while using Wi-Fi away from home, wait until you're on a secure network to access bank accounts.
- Prior to making a purchase or conducting a transaction on a mobile device, review the web address for security. Websites that contain "https:" in the web address indicates that site has taken measures to secure your personal information.
- Delete Mobile Banking text messages after viewing. Once you've received and reviewed the account information you requested via text message, delete the message to ensure the information is not found by others if your phone is lost or stolen.
- Be on guard against unsolicited emails or text messages appearing to link to a financial institution's website. Make it a practice not to respond to any emails, text messages, or calls that request your personal information or demand you take immediate action.

**Take additional precautions in case your device is lost or stolen**

- Check with your wireless provider in advance to find out about features that enable you to remotely turn off access to or remotely wipe your device in case of loss or theft.
- Promptly notify the bank if your device is lost or stolen.