How to Secure Your Mobile Device

- Always use a passcode lock to secure your mobile phone and other devices.
- Always log out completely on your mobile banking session.
- You can install mobile security software to protect your device from malware.
- Keep your phone and apps updated.
- Do not store sensitive information on your mobile phone. (e.g. passwords, social security numbers)
- Contact your financial institution if your phone is lost/stolen.
- Be careful when entering in sensitive information on your device; you never know who is watching.
- Avoid opening suspicious attachments in emails and texts (AKA Smishing), especially when it's someone you do not know.
- Contact your service provider if you receive an email saying your device is infected; this is a common attack method.
- Do NOT perform banking transactions over a public Wi-Fi. They are not very secure. Use your mobile network instead, when conducting these transactions.
- Report any suspected fraud to your financial institution immediately.