First Choice Bank™

MOBILE BANKING SECURITY TIPS

We're dedicated to providing the highest level of security. When using our mobile banking app, keep these tips in mind to ensure your experience is as secure as possible.

- Protect your personal information by ensuring your mobile device maintains a PIN, fingerprint authentication or strong password. When your device is not in use, enable automatic screen lock.
- Once your session is complete, log out of mobile banking before closing the app.
- Do not share personal and financial information via email, text or phone. Social Security number, birthdate, passwords and account numbers should be kept private and never stored on your mobile device.
- Delete security codes and message alerts you may receive via text from your financial institution. If you change your mobile phone number, be sure to update your online banking profile to protect sensitive message alerts.
- Report a lost or stolen device. Contact your financial institution immediately to update your information. You can also log in and remove the old device from your online banking profile.
- Use caution when downloading banking apps. Only install apps from reputable sources such as Apple® App Store, Google™ Play or a direct link from your financial institution's website.
- Keep your mobile operating system up-to-date by installing the latest updates as prompted by your device to ensure maximum security.
- Access mobile banking on a secure wireless network. Do not use public Wi-Fi hotspots. Unsecure networks can expose sensitive data, making it vulnerable to hackers.
- Do not root or jailbreak your device. This practice weakens device security.
- When depositing a check through our mobile banking app, wait until the funds are available and then destroy the check.