# MOBILE BANKING SAFETY TIPS


WELCOME and CONGRATULATIONS on the activation of our mobile banking app, TouchBanking! We're certain you will enjoy the benefits and convenience of "banking" via your cell phone.

We would like to take this opportunity to share some basic mobile banking safety tips:

- Avoid storing sensitive information like passwords and social security numbers in your mobile device.
- Password protect your mobile device and lock it while not in use.
- Enable an automatic screen-locking mechanism to lock the device when it's not actively being used.
- Be aware of your surroundings when typing sensitive information.
- Download all updates for device software and mobile applications.
- If you change your phone number or lose your mobile device, log in to our Home Banking website and disable that device immediately. If you do not have access to a computer at the time, you may notify us and we will disable it for you.
- Monitor your accounts regularly and report suspicious activity.
- NEVER ATTEMPT TO USE THIS APP WHILE DRIVING.

**SMShing**

SMShing is phishing that happens via SMS text message. A criminal sends a text message tricking you into replying with financial or personal information or clicking on links that will sneak viruses onto your mobile device. To guard against these scams:

- Don't respond to a text message that requests personal or financial information. NASCOGA Federal Credit Union will **never** ask you to respond in this way.