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**.**
- Be aware of your surroundings when typing sensitive information.
- Log out when you complete a mobile banking session.
- Protect your device from viruses and malware by installing mobile security software.
- Download all updates for device software and mobile applications.
- If you change your phone number or lose your mobile device, let us know immediately.
- Monitor your accounts regularly and report suspicious activity.

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. Petefish, Skiles & Co. Bank will never ask you to respond in this way.
- Verify the phone numbers that appear in a text message. Store Petefish, Skiles & Co. Bank phone numbers in your mobile contacts for a quick crosscheck. Or, you can go to the Contact Us page.

Stolen Devices

Mobile phones and tablets offer convenience, but they're also easy to lose or steal, which can put you personal information at risk.

- Password-protect your device so it can't be accessed unless the password is entered.
- Enable an automatic screen-locking mechanism to lock the device when it's not actively being used.
- Consider using a remote wipe program. This will give you the ability to send a command to your device that will delete any data.

Keep a record of the device's name, model and serial number in case it's stolen.