



# TIPS FOR SAFE MOBILE BANKING

When using a mobile device to manage your finances, it's important to take steps to protect your accounts. Key tips to keep in mind:

- **Never give out Personal Information to strangers**

This includes your debit card number, PIN, bank account number and any online or mobile banking login information.

- **Treat your cell phone like your wallet or purse.**

- **Be cautious of who you let use or borrow your device - they could quickly download fraudulent apps.**

- **Keep your device up to date with software releases and update and protect it with AVS and personal firewall.**

- **Texts from First Bank & Trust will never ask for account numbers, user name, passwords. Never send this secure information to anyone.**

- **Avoid public Wi-Fi connections as these are unsecured.**

- **Most mobile devices offer a feature allowing you to select a PIN or pattern recognition to unlock the device. This feature should be turned on and used anytime you turn your screen on.**

- **Do not store user name or password in your device's notebook, contacts or any other apps for easy retrieval.**

- **Don't be tricked into downloading anything**

The highest risk in a mobile banking setting is from downloading rogue apps or clicking links contained within certain websites and/or text messages.

STRONG PASSWORDS

SOFTWARE UPDATES

TEXT MESSAGE LINKS

AVOID WI-FI CONNECTIONS