fmbnc.com

Mobile Banking: Security Tips

F&M Bank protects your personal information anytime and anywhere that you use mobile banking technology. We use advanced encryption technology and a multi-layered approach to authenticating our customers before allowing access to our mobile banking platforms. We will never ask for your account number, Social Security number, card number or PIN to be entered within our mobile banking apps.

Your mobile devices need to be protected just like your PC. You can never be too safe. Here is a list of mobile device security tips to help you protect your valuable private information.

Manage Your Security Settings

- Always use a screen lock on your mobile device with a password or PIN feature. Many mobile phones offer this option, as well as other customizable security settings, which can help you keep your phone and information secure.
- Never lower your security settings for convenience. This only makes it easier for thieves to get into your device.
- Do not store your PIN or personal data on your mobile device.
- Don't click suspicious links and attachments. It is important to be cautious about all communications you receive, including those thought to be from "trusted entities."
- Back up all your personal data, such as your contacts, documents and photos so that they may be restored if your device is lost or stolen.

Mind Your Neighbors

- Prevent anyone from looking over your shoulder while you are accessing mobile banking.
- Never leave your mobile device idle while your banking session is still active.
- Do not use free public Wi-Fi connections for banking transactions. We recommend using your phone carrier's internet connections for enhanced security.
- Never respond to urgent email or text messages claiming to be from a bank or any company that requests your account information or personal details. Fraudsters may use the request to "phish" for your personal information.
- Frequently delete text messages from F&M Bank, especially before loaning out, discarding or selling your mobile device.

Keep a Close Eye on the Software You Install

- Only download apps from your mobile service provider or mobile device manufacturer's marketplace. Download the F&M Bank app by searching "F&M Bank – NC."
- Be cautious about granting applications access to your personal information or letting the app perform functions on your device.
- Disable Bluetooth when not in use. In public areas, others can detect your phone and access it through Bluetooth. Disconnecting Bluetooth, a non-secure connection, helps prevent attackers from obtaining information or sending malicious code into your device.
- Always accept updates and patches to your device's software as soon as it's available. Just like your desktop or laptop, mobile devices need updates to patch vulnerabilities and fix software issues.
- Install security apps that enable you to find your mobile device and to delete all of its memory if necessary.
- Always wipe data on your old phone before donating, reselling or recycling it.

Get Help

Should your device become lost or stolen, you should contact your wireless provider immediately. They may be able to locate or disable the device. You should also call F&M Bank at 704-279-7291 to alert the bank of the lost or stolen device. For added protection, log onto online banking from your computer, change your password and disable your alerts.