Mobile Banking Access

Download the official mobile application from the App Store or Google Play Store. Search for the following name:

TXN Bank Mobile

MOBILE APP NAME

The financial institution's public website contains direct links to the application. Visit our website at:

https://www.txn.bank/

PUBLIC WEBSITE ADDRESS

Do not download the organization's mobile app from other app stores, as those have not been authorized and the application may be compromised.

Learn More

To learn more about securing your mobile financial services, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- CISA.gov

CYBERSECURITY AWARENESS

Mobile Financial Services

Mobile Device Protection

PASSCODES

Create a complex passcode for your mobile devices. Avoid using personal information (e.g., names, dates, etc.) in your passcodes. Do not share your passcodes with anyone.

SECURITY FEATURES

Enable available security features, such as biometrics (e.g., fingerprint scanner, facial recognition, etc.), auto-wipe after a number of failed passcode attempts, and auto-lock after a certain amount of time.

UPDATES

Keep your device up to date. Install new updates as soon as you can to fix any identified security vulnerabilities.

AVOID COMPROMISE

Do not root, jailbreak, or otherwise circumvent security controls on your device. Install anti-malware, when possible.

SCREEN LOCK

Lock your device's screen anytime you are not using it, so it must require authentication before the device can be used again.

Mobile Applications

Download and install mobile apps only from trusted sources authorized by the device manufacturer, such as the App Store, Google Play Store, or Microsoft Store.

When possible, require authentication to download mobile apps to prevent unauthorized installation.

Protect yourself from fraudulent mobile apps by watching for these signs:

- Typos
- Poor image quality
- Formatting issues
- Low download number
- Negative user reviews

Review other mobile apps created by the app developer to validate the application's legitimacy.

If possible, create a passcode on mobile applications which can access your personal information (e.g., mobile banking services).

When finished with a mobile app, always "Sign Out" or "Log Off" rather than just closing it.

Be On Alert

People are trying to steal your personal information. Remember to be on alert for the following types of threats to your mobile financial services.

SOCIAL ENGINEERING

Phishing is a social engineering tactic used to obtain personal information by masquerading as a trustworthy person via electronic communications (e.g., email, text message, phone call, etc.).

UNSECURE NETWORKS

If you can connect your phone to a wifi network without entering a password, unauthorized individuals can, too. If you are on an unsecured wireless network, such as a mobile or wifi hotspot, do not use your mobile device to transmit sensitive data.

COMPROMISED WEBSITES

Watch for potentially compromised websites. If the website has a security error or your browser gives you a warning about the site, use caution. If you go to one web address and are redirected to another, close your mobile device's browser immediately and remember:

When in doubt, do not click.