# Best Practices for Business Mobile Banking

FIRST BANK
*The **one** who's here.*

As the use of mobile devices increases for banking, First Bank wants our business customers to know that we take security very seriously. The widespread use of mobile and text banking with mobile devices means much more convenience for customers and better ways to monitor account activity. Unfortunately, it also means there are more opportunities for fraud. First Bank provides a secure environment for Mobile Banking keeping our Online Banking services up to date to help protect our customers from fraudulent activity. As our customer, there are several things that you can also do to significantly reduce the risk of fraud and identity theft while using our mobile banking services.

1. **Password protect your mobile device** changing password frequently and lock it when you aren't using it. Never use passwords that include birthdays, names, pet names, social security numbers or that repeat numbers or letters. Do not configure your mobile applications for auto-login capability. Keep your device in a safe location and don't leave your mobile device unattended in public places. Consider using a Pattern, Fingerprint, Face ID or other authentication methods offered by your mobile device.

2. **Frequently delete text messages received from us on your mobile device**, even though they don't contain sensitive information. Never disclose personal information about your accounts via a text or Email message. For example: account numbers, passwords or any combination of personal information.

3. When you log into mobile banking, **be aware of the people around you.** Even if you are speaking on your phone, be careful not to give account numbers or other personal information within earshot of others.

4. **If you change your mobile number or lose your mobile device,** immediately log onto online banking to disable mobile and text banking changing your sign on information to online banking, and call us to report a lost or stolen device.

5. **Do not modify your device.** This could leave it susceptible to infection from a virus. Don't modify the mobile device to: give yourself more control, enable features that void warranties, change the root file systems or allow modifications to install third-party software or hardware components.

6. If possible, **install reputable mobile security software on your device** such as an anti-virus and anti-malware. Consider using tools that allow you to remotely wipe your mobile device if it is lost or stolen.

7. **Only download applications from reputable stores** after reviewing feedback from other users and closely review application permission requests. Always start with contacting First Bank to verify what the apps or mobile banking products are called and where to sign up.

8. **Monitor your accounts.** Check balances and items that are presented on a regular basis. This will help to spot any suspicious activity.

9. **Set up transaction Email alerts** so that you can be notified for if your balance drops below a certain level and other transaction information so you will be better aware of your transactions and balances.

10. **Online Banking Administrators should not share their sign on information with others.** Their sign on was created specifically for them to manage the organization's Online and Mobile Banking. An Online Banking administrator can add services and accounts and manage the organization's funds as well as creating access for others to the organization's online banking. Sharing the administrator sign on gives powers to others that was not intended increasing risk.

11. **Don't access banking or shopping applications** using your private sign on credentials while connected **through public Wi-Fi connections.** Ensure your home wireless network is configured to use Wi-Fi Protected Access II (WPA2) Wireless Security Technology. Disable discoverable mode after enabling Bluetooth® devices, if your Smartphone does not automatically default to off after adding a device.

12. **Ensure your Sign On and Password are hidden** when interacting with First Bank's web site and Mobile Banking App.

13. **Delete any confidential information from the device** prior to any third party servicing.

14. **Don't store financial information** in your mobile device.

15. **Keep your mobile device** operating system and applications up to date with the latest patches.

16. **Be cautious of opening unsolicited files**, text messages, or applications, especially if they are received from unknown sources.

17. **Never respond to a "phishing" text or email** that requests your PIN, account number, or any card, and please remember that First Bank will never request this information in this manner.

Thank you for your support of First Bank. First Bank has provided the above Best Practices to assist you to protect your confidential and financial information. Please be sure to implement these practices to help reduce your risk. First Bank is not responsible for losses related to security weaknesses within your personal online banking access devices such as your home computer and mobile devices.

DISCLAIMER: *First Bank does not provide any express or implied warranty, guarantee or promise concerning the content, completeness, accuracy or value of the above information. All persons or entities should confirm the accuracy as it applies to them specifically or their business or system. These "mobile banking best practices" are provided as information only and First Bank will have no liability to a client or any other person or entity, for any direct, indirect, incidental, special or consequential damages arising out of the information above.*