



Mobile Banking Best Practices

Merchants Bank is proud to provide Mobile Banking to its retail and small business customers. We provide Text Message Banking, and Mobile Web Banking. Text Message Banking enables customers to access their account information and receive account notifications on their text-enabled mobile phone or wireless device. Customers can receive balance information, their last five transactions, or make a transfer. Mobile Web Banking enables customers to access their accounts and other financial information from anywhere using a web-enabled mobile phone or wireless device. Customers can see their balances, transactions, conduct transfers and manage bill payments from any mobile device that has web browsing capabilities and a data plan.

As the use of mobile devices increases for banking, Merchants Bank wants all of our customers to know that we take security very seriously. The widespread use of mobile phones and mobile banking means much more convenience for customers and better ways to monitor account activity. Unfortunately, it also means there are more opportunities for fraud. Merchants Bank provides a secure environment for Mobile Banking. All communication between the mobile device, mobile carrier gateway and the mobile application server uses SSL/TLS encryption for secure communication with the customer's mobile device. Multi Factor Authentication is always used for every session. User IDs, passwords, the device itself and challenge questions are all used to authenticate the user. Passwords, answers to challenge questions, and account information are never stored on your device.

There are several things that you as our customer can also do to significantly reduce the risk of fraud and identity theft while using our mobile banking services. Please also be sure to check our Retail Online Banking Best Practices as well.

- 1. Password protect your mobile device and lock it when you aren't using it. Keep your device in a safe location.**
- 2. Never use passwords that include birthdays, names, pet names, social security numbers or that repeat numbers or letters.**
- 3. Never store your sign on, password, and answers to your challenge questions on your phone. Frequently delete text messages received from us on your mobile device, even though they don't contain sensitive information.**
- 4. Never disclose personal information about your accounts via a text message. For example: account numbers, passwords or any combination of personal information.**

5. **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.**
6. **If you change your mobile number or lose your mobile device, immediately log onto online banking to disable mobile text banking and change your sign on information to online banking, and call us to report the loss.**
7. **Do not modify your device. This could leave it susceptible to infection from a virus.**
8. **If possible, install reputable mobile security software on your device.**
9. **Don't download banking apps onto your phone without checking them out first. Always start with your financial institution to verify what their apps, or mobile banking products are called and where to sign up.**
10. **Monitor your accounts. Check balances and items that are presented on a regular basis. This will help to spot any suspicious activity.**
11. **Set up text alerts so that you can be notified if your balance drops below a certain level, a certain check has cleared or if a large check has cleared so you will be better aware of your transactions and balances.**

Merchants Bank has provided the above Mobile Banking Best Practices to assist you to protect your confidential and financial information. Please be sure to implement these practices to mitigate your risk of loss. Merchants Bank is not responsible for losses related to security weaknesses within your personal online banking access devices such as your home computer, cell phone, mobile device, etc.