# Safety Tips to Remember When Using Mobile Banking

Let's talk about mobile banking safety. By now, mobile banking is a pretty common term that most of us hear on a day to day basis. But, how safe is it to use? In general mobile banking is safe. In today's world nothing can be 100% secure from some type of compromise, but the banking industry has taken major steps to make sure that mobile banking apps are secure. The problem often lies with the mobile device and how it connects to internet.

Our mobile devices are convenient and are a big part of how we keep in touch with the world. It makes sense that we now have banking information at our finger tips, 24/7. As a financial institution, we work hard to make sure that your banking information stays secure, and we want to provide you with several tips to help prevent someone from gaining access to your personal information.

The most important step in keeping mobile devices such as phones and tablets secure is realizing that mobile devices are portable computers and treating them as such. Using these common-sense precautions can help protect your personal information:

**1.** Set the device to require a strong password to power on or awake it from sleep mode. If it is lost or stolen, this will make it more difficult to access any personal information stored on the device.

**2.** Whether you're using the mobile Web or a mobile app, don't let your device automatically log you in or remain connected to financial or sensitive apps or websites. Otherwise, if your phone is lost or stolen, someone will have easier access to your information.

**3.**Don't save your password, account number, PIN, answers to secret questions or other such information in an unprotected manner on the mobile device. Consider using a secure password keeper app for this purpose.

**4.** If you lose your mobile device, IMMEDIATELY tell your bank or mobile operator. The sooner your report the loss, the better protected you are from fraudulent transactions.

**5.** Treat your mobile device as securely as you would your wallet, cash, and credit cards.

**6.** Download and install new software updates. This includes operating system updates for your mobile device as well as new app versions. These updates often incorporate security patches to help better protect your device.

**7.** Say NO to public WIFI! Only use WIFI on your device when connected to password protected hotspots that you know and trust. Turn-off auto-connect features. They might cause your device to log into insecure wireless networks without your knowledge. Consider using a reliable Virtual Private Network (VPN) to increase security when using public WIFI.

**8.** Keep track of account transactions. Review your bank statements regularly to identify unknown or fraudulent transactions. If you notice discrepancies, contact your bank immediately.

**9.** Be cautious of e-mails or text messages from unknown sources asking you to update, validate, or confirm your personal details including password and account information. If you are not 100% sure of the source,

don’t disclose any information.

**10.** Be aware of your surroundings if you check your financial information when you are in a public place. Some people may try to “shoulder surf” which is stealing your information by observing your activity.

**11.** Before you upgrade, dispose of, or recycle your device, delete all personal/business details. Perform a “factory reset” if possible to delete all personal information from the device.

We hope these tips will help you to keep you mobile devices and personal information protected. You may view our recent and past educational articles on our “Tips and Advice” page by clicking here or by clicking the “Tips and Advice” link from the bottom menu of any page on our site. And, as always, if you have questions about privacy or data security, or if you think your information may have been compromised, please call us at (580) 661-3541.