

## Mobile Security

The most important step in Mobile Banking security is treating your mobile device like a portable computer. A few common-sense precautions will help protect you from fraud and I.D. Theft:

1. **Set the phone to require a password to power on the handset or awake it from sleep mode.** If it's lost or stolen any personal information stored on the device will be more difficult to access. Whether you're using the mobile Web or a mobile client, don't let it automatically log you in to your bank account. Otherwise, if your phone is lost or stolen, someone will have free access to your money.
2. **Don't save your password, account number, PIN, answers to secret questions or other such information on the mobile device.**
3. **Immediately tell your bank or mobile operator if you lose your phone.** The sooner you report the loss, the better protected you are from fraudulent transactions.
4. **Download and install antivirus software for your mobile device, according to the manufacturer's recommendations.**
5. **Be careful when downloading Apps.** Downloads should always be from a trusted and approved source, and endorsed by your mobile device provider.
6. **Avoid "free offers" and "free ringtones."** An email or instant message that offers free software downloads, such as ringtones, may contain viruses or malware.
7. **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.** Don't reply to text messages from people or places that you do not know.
8. **Treat your mobile device as carefully you would your wallet, cash or credit cards.**
9. **Keep track of account transactions.** Review your bank statements as regularly as possible to rule out the chances of fraudulent transactions. If you notice discrepancies, contact your bank immediately.
10. **Only use Wi-Fi on your device when connected to password protected hotspots.** Turn-off any auto-connect features. They might cause your phone to log into insecure wireless networks without your knowledge.
11. **Make sure you log out of social networking sites and online banking when you've finished using them.**
12. **Install operating system updates for your device as they become available - they often include security updates.**
13. **Before you upgrade or recycle your device, delete all personal/business details.**

Mobile Banking is a useful tool that can simplify your life and make managing your money incredibly convenient. By using common sense, it can also be a safe and secure part of your daily life.