Mobile Banking Best Practices

Protecting the security of your money and identity is our priority.

Let's work together to protect it.

Your mobile device is a GPS device, MP3 player, gaming device, video player, web browser and more. Your mobile phone is a computer in your pocket. Because it stores your personal information, contact lists, photos, videos and more, it's crucial that you protect it. Use mobile device security software (eg. Antivirus) and keep smart-phone software/firmware, system patches and upgrades up-to-date to protect yourself against viruses, Trojans, hackers, thieves and other threats just as you do on your other computers. There are several additional precautions you should take to ensure your data is safe. The following list includes a few of these:

- **Secure Your Passwords and Devices**
  Creating secure passwords is something you hear about all the time, and it is one of the easiest ways to keep your information safe. Having a strong password with symbols, numbers, upper and lowercase letters should be a priority. Having a simple password makes it easy for hackers to quickly access and steal your information. Change your password often. Also use a password on your SIM card (subscriber identity module) if your mobile phone uses a SIM card. Use biometrics if available on your mobile device (fingerprint, face ID). Use passcodes and screen lock timers to protect your mobile devices.
  In addition, some smartphone users make it simple for thieves by staying signed in to social networks and other applications that store personal data. When you are finished accessing your personal accounts online, make sure to log out. This is particularly important when you are using Online and Mobile Banking.

- **Research Apps Before You Download Them**
  If you find an app that sounds fun and exciting in a mobile marketplace or store, that alone, does not guarantee the app is safe to download. Do a little research on your own and find out if other users have had problems with the app. Compare similar apps and see which one seems the most trustworthy. Apps are one of the main ways viruses and other malicious threats enter a mobile device, so take extra precautions when it comes to what you download onto your mobile device, just as you would with your other computers. Review and understand the permissions required when downloading/installing applications.

- **Be Cautious on Public Wi-Fi Networks**
  We have all experienced the benefits of free, public Wi-Fi, but unfortunately there are several drawbacks that come along with this convenience. On a public Wi-Fi connection, it is easier for someone to hack into your data. Many public Wi-Fi areas are not encrypted and are prime targets for hackers to access information on your mobile device or computer. If you are accessing any type of personal information, be cautious. If possible, avoid any type of webpage or application that can identify you.

- **Don't Jailbreak Your Phone**
  When you jailbreak your mobile phone, you are making it possible for an "unapproved" app to be downloaded onto your device. In addition, you may be removing needed security features. Although not foolproof, Apple Android and Blackberry all have inspection processes they put apps through before they are approved to be put into the marketplace or store. This helps to ensure that an app is safe and doesn't contain malicious or destructive code. When you jailbreak your mobile device and download an unapproved app, you are taking away that security precaution.

- **Be Mindful with Mobile Banking**
  Mobile Banking uses encryption technology to ensure that all the data you are using is safe. But there are still ways hackers and thieves can access your information. Sending text messages with banking information, even a username to your account, can be an aid in accessing your information. If emails or text messages from the bank come to your mobile phone, look at them and immediately delete them. In addition, if you use your smartphone for mobile banking and your phone is lost or stolen, notify us immediately. We can then more actively monitor your account.

- **Document and Register Your Mobile Phone**
  Fortunately, there are numerous ways you can locate a lost mobile phone. Almost all require that you sign up for something beforehand, so prepare now. First, write down somewhere safe your phone's IMEI, MEID or ESN number (it's on the sticker under the battery). That's a unique identifier you can give to the police or your wireless carrier if your mobile phone gets lost.

  All the carrier-based services need to be activated before you lose the phone, because you either need to reply to a text message or change some settings on your phone to accept tracking. Android phone owners can load a third-party program which offers phone-tracking, remote lock, backup and wipe services. Apple iPhone owners can subscribe to MobileMe and use its Find My iPhone feature. You can also use third-party tracking apps. BlackBerry users can try the third-party Berry Locator which will send a message to your lost BlackBerry and show you where it is on a Web-based map from any PC or use third-party tracking apps.

- **Phishing, Vishing and Social Engineering** attacks are used by bad actors as part of an elaborate scheme intended to trick victims into taking specific action to defraud them. These types of attacks can come through any communication channel including telephone/voice, SMS, Chat, Email, Postal Mail, Internet/Web/Social Media and others. The following best practices can be implemented to mitigate against these methods.

    - Do not respond to any unsolicited Multi-factor authentication (MFA) requests
    - Do not divulge your credentials or MFA code to anyone
    - If you suspect you've been part of a Phishing, Vishing or Social engineering attack, notify your financial institution
    - Change your username & password periodically and use strong passwords
    - Use complex and unique passwords for all types of online accounts consisting of at least 12+ characters, including special characters and numbers

REV 06/26/2020