Mobile Banking Security Best Practices

Merchants Bank of Commerce, a division of Columbia Bank would like to encourage our customers who utilize Mobile Banking products to use the following security features.

Mobile Banking

- Touch ID or Face Recognition
  - By enabling Touch ID, every person with a saved fingerprint on your device will have access to your account. For your security, review the fingerprints to make sure that each person is authorized to access the personal and financial information available in this app.
    i. **We don't recommend using Touch ID if you share your device.**
- Do not store your passwords on your phone unencrypted.
- Do not store unencrypted personal information on your cell phone or any other unsecure application.
- Critical data should be stored in a digital wallet or password manager with strong encryption, such as 256 bit AES to keep the data safe, secure and accessible.
- When finished using mobile banking remember to sign off before accessing another application.
- Don't use unsecured WiFi networks, such as those found at coffee shops because fraudsters may be able to access the information you are transmitting or viewing.
- If you lose your phone, call your cell phone provider immediately so they can deactivate your phone.
- **If you lose your phone it is also imperative that you call us at 1-800-421-2575 to disable your Login ID and remove your cell phone number as a secure access code delivery method.**
  - If after hours or on a weekend, you can disable access to your mobile banking by attempting to log in with an invalid password 3 or more times.
- Utilize the "passcode" or auto-lock options available on your particular device.
- If available, use the option that will erase or "wipe" your phone after too many unsuccessful passcode attempts.
- If available, turn on the option to track and remotely erase your device if lost.

Virus Protection

You may consider installing virus protection on your mobile phone. Please research carefully the best practices for your particular device. Currently virus protection for smart phones has limited and debated effectiveness.

- Virus Protection should be installed with automatic updates, scanning, as well as malware detection software.
- Never click on a text message or email to install free software.

Jail Breaking or "Rooting" your mobile device

- Jail breaking and rooting are methods of "self-hacking" your smart phone in order to gain full access to all features of the technologies of smart phones. However, this makes the smart phone extremely susceptible to malware, viruses and other malicious programs. We will never recommend you to jail break or "root" your smart phone. If you have done this please contact your smart phone service provider.

Downloading Apps

- We recommend that you download Apps from trusted and approved App stores endorsed by the particular technology provider (iPhone, Droid, Blackberry etc.) and service carrier. Certain smart phones can be configured to block Apps installed outside of trusted and approved App stores.

Sensitive Information

- When you're using our mobile products for your online banking **we will never ask you for any sensitive information via a SMS text message**. If, while on our mobile products you are being asked for any of the following information, STOP and do not enter your login information. Some examples of sensitive information include:
  a. Your name
  b. Your date of birth
  c. Social Security number
  d. Account number
  e. ATM or PIN number
  f. Passwords
  g. Any other personal identifying information

Bluesnarfing

- Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a short range high speed wireless technology used for sharing information between devices. Devices with Bluetooth enabled by default and "always on" may present a target for exploitation and interception of data which can be done undetected
- Keep Bluetooth turned off by default and use only when necessary. Make sure that Bluetooth is turned off when conducting any mobile banking transactions or inquiries.

On a *daily basis*, all customers should be verifying their online activity and contact us immediately at 1-800-421-2575 if unauthorized transactions appear.