# Best Practices for Safe Mobile Device Usage

Online security is a top priority at Commercial Bank & Trust of PA. We want to provide crucial information, tips, and tricks to help protect your secure information.

Mobile Banking is constantly changing, making it difficult to identify all possible risks, but this comprehensive set of guidelines will give you knowledge to protect yourself and utilize mobile banking with confidence.

If you are using a mobile banking application, such as Commercial Bank & Trust of PA's Mobile Banking App, your smartphone could be a target for malicious individuals who want to steal your identity or those you lend your device to.

## What is a Smartphone?

A smartphone is a cellular phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded applications, more commonly known as apps.

**On which smartphones can I install the Commercial Bank & Trust of PA's Mobile Banking App?**

The Commercial Bank & Trust of PA Mobile Banking Application is currently available for download on Apple® & Android™ devices including tablets with Apple & Android operating systems.

If you have a smartphone with a different operating system such as Windows or Blackberry, you can still utilize Commercial Bank & Trust of PA's mobile banking through our website at http://www.cbthebank.com

## Key items to keep in mind

- Always treat your cell phone like your wallet or purse.
- Be cautious of who you let use or "borrow" your device – they could quickly download fraudulent apps.
- Keep your device up-to-date with software releases and update and protect it with antivirus software (AVS).
- When you text someone, the message is stored on your cell phone, at least one server somewhere, and the receiver's cell phone. It will be around forever.
- Text messages, emails, alerts from Commercial Bank & Trust of PA never contain any personally sensitive information (account numbers, username, passwords). Commercial Bank & Trust of PA will never ask for this information to be submitted through any channel. Never send this secure information to anyone.
- You should review your account information via multiple channels on a regular basis to ensure consistency.

## Lost or Stolen Device

In order to safeguard yourself, there are several best practices you can follow BEFORE losing a device:

- Most smartphones offer a feature allowing you to select a PIN or pattern recognition password in order to unlock the device for use. This feature should be turned on not only when you power-on your device but anytime you turn your screen on.
- Create "strong" passwords (of unusual combinations of upper-and lower case letters, numbers, and symbols) or PIN (random numbers instead of, say, 1234 or the last four digits of your Social Security number) and periodically change them.
- Do not store your username or password in your device's notebook, contacts, or any other apps for easy retrieval.
- Check with your mobile carrier about remote wiping. Often times you can wipe the data from your phone either online or through the help of your carrier. This prevents the information from being accessed from anyone who may find or steal your device.

## What else should I be aware of?

### Social engineering

There are serious social engineering threats that users need to be aware of when engaging in mobile banking practices:

**Malware:** The intent of malware is to covertly compromise the confidentiality, integrity, or availability of the victim's data, application, or operating system. The highest risk in a mobile banking setting is from downloading rogue apps or clicking on links contained within certain websites and/or text messages. Just because the picture of an application appears to be backed by a legitimate financial institution doesn't mean it is secure.

**SMiShing** : The act of retrieving information via text message. Attackers pose as a financial institution and use SMS (texting) to ask for sensitive information. Your response and information is routed to an unauthorized individual.

**Phishing** : This has been around since the birth of Internet banking and is still applicable to mobile banking. Phishing is an attack used by tricking the victim into downloading malware or disclosing personal information.

**Vishing** : Using SMiShing and Phishing to evoke a victim into disclosing information by responding to a bogus phone number and talking to an attacker.

**Man-in-the-middle attack** : A form of active eavesdropping when the attacker makes independent connections with the victims and relays messages between them, making them believe they are talking directly to each other over a private connection, when actually the entire conversation is controlled by the attacker.

**Cloning** : The transfer of identity between one mobile telephone and another.

**Hijacking:** The attacker takes control of a phone conversation and masquerades as one of them. This could give the hacker access to the victim's financial accounts.

## NEVER "Jailbreak" your Device

Smartphones and tablets can be "jailbroken" by installing modified software that unlocks the restrictions of the device's core operating system. "Jailbreaking" or otherwise altering your device could void your warranties, violate your provider's terms of service, or even damage your device. Since jailbreaking methods are unsanctioned by manufacturers and forgo most security protocols, they can make your device unstable, susceptible to viruses, and vulnerable to exploits that feed hackers your personal information.

## Fraudulent Applications

Research any application ("app") before downloading it. Just because the name of an app resembles the name of your bank – or of another company you're familiar with – don't assume that it is the official one of that bank or company.

Take the time to read the "small print" when installing an app on any smartphone. Evaluate the information the app requires access to and consider if this information is necessary for it to run successfully. If you cannot see a reason for the app to have access to the information, you should reconsider installing it.

The iPhone app store is the only marketplace that controls "application distribution" meaning they review and restrict applications prior to allowing them to enter the app store.

Even with the strict app design controls, fraudsters may attempt to mimic the Commercial Bank & Trust of PA's Mobile Banking Application in order to create a "spoof" app. When an unsuspecting person downloads the fraudulent app and enters their log-in credentials, it is immediately sent to the fraudsters. They could then use your username and password to log-in to your account.