MOBILE SECURITY TIPS

More people than ever before use mobile devices[1] and tablets to stay connected and to conduct business online. This is a great convenience, but if your device isn't secure, then the data on your device could be used by cyber criminals to access your accounts and steal your money or your identity. Follow these steps to help secure your device:

ALWAYS LOCK YOUR PHONE/ TABLET WHEN NOT IN USE. Set your device to lock automatically after a few minutes of it not being in use. One of the easiest ways to secure a device is to set up a security passcode or lock pattern; set a passcode that only you know. When available, set up Touch ID or facial recognition on your device, and back that up with a unique PIN or lock pattern.

DOWNLOAD APPLICATIONS (APPS) ONLY FROM OFFICIAL APP STORES, such as Google Play,[2] Apple[3] App Store, Windows Store and Amazon. Some apps can house malware capable of stealing your data, without your knowledge, as you use your phone or debit money from an app-linked account. Although very uncommon, it is possible for a malicious app to make its way into a legitimate store. Be cautious about what permissions you grant the apps that you download. Before downloading, read the documentation provided by the app developers, understand the level of access to your phone the app requires, and check the number of downloads and reviews.

USE CAUTION WITH PUBLIC WI-FI NETWORKS. It's convenient and tempting to use public Wi-Fi hotspots, but they do not require a password and may not be secure. When your device is connected to public Wi-Fi, avoid visiting websites that contain sensitive or financial information, like your bank or credit card website. Do not share sensitive data (credit card numbers, Social Security numbers, etc.) or conduct online banking from a public hotspot.

BE ALERT TO SPAM TEXT MESSAGES. Smartphones are just as susceptible to phishing attacks as computers. These work the same as fraudulent email, directing you to a malicious link to infect your phone or to capture your personal information. Never provide personal information via a text message or a phone call.

BACK UP YOUR DATA TO THE CLOUD. Keep an ongoing backup of your phone. That way, if it's ever lost or stolen, you still have all the apps, data and accounts up to date in your backup.

AVOID PUBLIC CHARGING STATIONS UNLESS THERE IS AN EMERGENCY. Hackers have been known to set up fake charging stations in scams known as "juice jacking." After you plug in, the hackers can access your phone's data or install malware on the device.

TURN ON REMOTE TRACKING IN YOUR MOBILE DEVICE SETTINGS. Apple users have Find My iPhone, and Android users can enable Find My Device to see the last known location of the device. Both features allow you to remotely wipe your smartphone's data if it's stolen or can't be retrieved.

ALWAYS UPDATE YOUR PHONE'S OPERATING SYSTEM (OS) WHEN PROMPTED. These updates are meant to protect your device and data with the most current protection from viruses, malware and other online threats.

IF YOUR DEVICE IS LOST...

- **Remotely lock your device.**
- **Change critical passwords, including the phone and any accounts enabled on the device, especially financial accounts.**

IF YOU BELIEVE THE PHONE WAS STOLEN OR COMPROMISED...

- **Remotely wipe your device.**
- **Notify your service provider immediately to suspend service.**
- **File a police report.**

This article is for general information purposes only and is not intended to provide legal, tax, accounting or financial advice. PNC urges its customers to do independent research and to consult with financial and legal professionals before making any financial decisions.

1 A supported mobile device is needed to use Mobile Banking. Standard message and data rates may apply.

2 Google Play and the Google Play logo are trademarks of Google LLC.

3 Apple, iPod, and iPad are trademarks of Apple Inc., registered in the U.S. and other countries. iPhone is a trademark of Apple Inc.

PNC BANK

CON PDF 0220-0153