SAFEGUARDING YOUR SMARTPHONE

FIRST TENNESSEE

With the increasing popularity of smartphones, more and more people are using apps to conduct personal business online – business that often requires the use of sensitive information such as bank account numbers, credit card data, or passwords.

While your smartphone can make life simpler, you should also be aware of potential threats to the security of your smartphone and the precautions you can take to keep it secure.

There are three areas where smartphone users can potentially fall victim to fraudulent activity. Keep these in mind as you use your smartphone as well as the related tips for preventing fraud.

LOST PHONES

If you've owned a smartphone for any length of time, chances are you've probably misplaced it, at least temporarily. The danger here is that, if you've made purchases on your phone or, perhaps, conducted banking activities with it, someone who finds or steals your phone may be able to extract sensitive personal information from it.

- **Tip #1** – Set PINs and passwords on your phone's homescreen to prevent unauthorized access to your phone. Configure it to automatically lock after 5 minutes or less of being idle.
- **Tip #2** – Wherever possible, use different passwords for each of your important log-ins.
- **Tip #3** – Don't modify your smartphone's security settings, as it can undermine valuable built-in security features.
- **Tip #4** – Keep your smartphone's operating software up-to-date by enabling automatic updates from your service provider. You may also want to install security apps that allow you to remotely locate and erase all of the data stored on your phone.
- **Tip #5** – Always report a stolen phone. Wireless providers in conjunction with the FCC have established a stolen phone database that will help your provider prevent your phone from being activated without your permission.

APP DOWNLOADS

Hackers often use apps to entice smartphone users into downloading malware that can steal information or cause damage to your phone.

- **Tip #1** – Only install apps from trusted sources. If you have doubts, you can check user reviews, confirm the legitimacy of the app store, and compare it to the app sponsor's official website.
- **Tip #2** – Understand app permissions before you select to download. Check the privacy settings for any app you want to install and use caution when granting permissions for an app to have access to your personal information
- **Tip #3** – You may also want to install security apps that allow you to remotely locate and erase all of the data stored on your phone.

SURFING ON OPEN WI-FI NETWORKS

Cybercriminals often use unprotected Wi-Fi hotspots to target people online.

- **Tip #1** – Avoid public hotspots and instead use protected Wi-Fi from sources you trust or your own mobile wireless connection.
- **Tip #2** – Ignore pop-ups or prompts to download software. They are usually a hacker's attempt to infect your phone with malware or spyware.
- **Tip #3** – If you don't get automatic updates, manually update your smartphone's security software before you travel. Wi-Fi in airports and hotels can be potentially troublesome if your smartphone is not fully protected with the latest security updates.

©2013 First Tennessee Bank National Association. Member FDIC. www.firsttennessee.com