KANE RUSSELL COLEMAN LOGAN

One Mission. Your Mission.

Banking On Your Smartphone: How Secure Is It?

Banking Law / July 6, 2015

More than half of all banking customers conduct their banking on their smartphone because it is quick, easy and convenient. And it's no wonder why this number is so great: smartphones are increasingly being integrated into the lives of many Americans. And as mobile e-commerce and contactless mobile payment methods, such as Apple Pay, continue to grow in popularity, there is no doubt that banking over mobile phones will continue to increase as well.

What's The Risk?

Opinion is divided as to whether banking on mobile devices is safer than banking on a personal computer, or vice versa. On one hand, personal computers are more likely to be victimized by malicious software and viruses that could accidentally be downloaded by a user, making online banking unsafe. Users can inadvertently download Trojan viruses that lie in wait until users access their online bank accounts. The viruses log the user's login credentials, and then hackers use the stolen information to steal money from the victim's bank accounts.

On the other hand, many believe that mobile devices aren't particularly safe because when it comes to who has access to the information contained on the mobile device, numerous apps on smartphones are collecting data, which is later used or sold. Many apps use geolocation, and keep a record of where the user has been; some access information that is stored on the smartphone. What if an app were to collect your banking data? Furthermore, what do apps do when they are left open on a smartphone? Smartphone applications have a reputation for accessing the user's information and collecting that data.

Additionally, some mobile platforms are more safe than others. For instance, the Android platform is the target of malware, commonly referred to as Zeus-in-the-Mobile, or ZitMo, that is specifically designed to target a user's banking information on mobile devices using Android operating systems. To date, antivirus software has not performed well on mobile platforms. The potential threat posed by smartphone malware has prompted app providers, such as Google and Apple, to run new apps through a rigorous screening process for suspicious activity before the app can be made available for the public to purchase and use.

Apps on smartphones that have access to the internet are the least safe, since they have permission to access the internet at any time. Hackers can take advantage of this feature, especially if the smartphone user is using a public wifi connection or has bluetooth enabled. Cybercriminals can intercept bluetooth transmissions or easily hack a smartphone connected to the internet via public wifi access.

Tips for Safer Smartphone Use

The following is a short list of general ideas to consider to ensure same smartphone use:

- Smartphones can be password protected. Users should take advantage of password protection.
- When upgrading to a newer smartphone, take steps to protect the information that could be stored on your old smartphone model.

- Users should close apps on their smartphone when they are not using the application. Leaving apps running in the background leaves users vulnerable.
- Using public wifi is not in and of itself unsafe. However, using public wifi for transmitting sensitive information, such as Social Security numbers, credit card numbers, or banking information, may not be safe. Encrypted wifi or a cellular data network connection is a better, safer option.