The root of the problem

When it comes to banking technology, more and more banks are developing smart phone applications (apps), which allow you to perform basic banking functions. Apps are and are going to continue to be the way of the future. Customers are now able to connect with their bank on levels that they have never been possible before. Although Apps present a unique ability, they also offer a unique challenge and can even open your bank up to potential fraud in ways that they have never imagined before. To better understand the potential risks, we need to understand what an app can do.

• • •

Apps are an extremely convenient way for customers to view their accounts. Customers love the ability to go to a store and right before they purchase an item, they check their account to make sure that they have enough cash. They also can assist individuals in transferring money between their accounts or even to another account holder. So far many people would think that this is simply just a mobile website. Wrong! Apps take it one step further. They can locate your position via GPS and give you turn-by-turn directions to the bank. It is even possible to video chat with a personal banker right through their phone (4G required on both phones in the conversation).

My favorite feature is the ability to deposit your checks. Amazing! Now as soon as your customer gets paid (the payroll check), they can log into their bank app, take a picture of their check right from their phone, and deposit it into their bank. Customers love this feature, but it can pose some serious threats to your organization.

Here’s why. When you program a banking application, you are programing for a specific operating system. In most cases banks produce an app for a phone operating system like Android for non-iPhones or iOS for the Apple iPhone/iPad/iPod. You can incorporate a number of security features into the application, which would normally protect your organization’s data. This normally thwarts traditional attacks. Here is where it all can go wrong.

The security features that are being installed are trusting that their device has not been altered. What does this mean? I am sure that many of you have heard of “jail breaking” or “rooting” your device. Jail breaking is to Apple as rooting is to Android, (in simple terms.) To be honest, jail breaking and rooting have tremendous advantages. When you jail break or root your device you are now allowing it to function in ways that were not originally intended. Most cell phone users jail break/root their device to install apps that allow them to create a mobile Wi-Fi hotspot right from their phone. Doing so voids their warranty, but modifying the device is not illegal. It is what you can do with it that is illegal, such as installing applications, which you never paid for, etc.

So where am I going with all of this? When you have root access on your phone, you are not limited by the rules that Google or Apple places upon their apps. Rogue Apps could be created that are worse than any virus you could have imagined. Imagine a harmless Wi-Fi tethering application that has access to your camera. Anytime that you take a picture of a check to deposit it could not only be sent to your bank but to countless others. Imagine if your customer deposits a check through their app and a fraudster has intercepted the image and has already collected funds before

your bank has the time to process the check. It essentially can create virtual check theft or, worse, yet virtual kiting.

Smart phones can be trained to do just about anything so FIs need to do their homework with respect to security and operating systems. Customers will continue to demand mobile applications. So, extra due diligence is an important step to learning about the type of app program security and what an FI should do to protect and secure the process. It is a new world.

Smart Phones are cool and convenient, but they are not without risks. Watch for our follow up blog that digs deeper in the root of the problem and security alternatives.

—Simon M. – Son of Wombat!

Simon M. Fisher is an aspiring entrepreneur. He currently serves as Chief Marketing Officer for Myriad Devices, a technology company based in Fargo, N.D. that specializes in development of mobile applications. Simon enjoys traveling, spending time with family, and keeping up with current trends in technology.