ANB Mobile Banking

Five Mobile Banking Security Tips

1: Beware of Phishing

Phishing refers to the practice of tricking someone into revealing private information. Fishing and phishing are similar concepts -- there's bait involved with both. With a phishing scheme, that bait might be as simple as a text message or e-mail. It may be as complex as a fake Web site designed to mimic your bank's official site, which is called spoofing.

Never follow a banking link sent to you in a text message or e-mail. These links could potentially lead you to a spoofed Web site. If you enter your information into such a site, you've just handed that data over to thieves. Always navigate to a Web site directly. Enter your bank's Web address into your phone and bookmark it. This will help you avoid bogus Web sites.

On a related note, never send your account information or password via text message or e-mail. It's a common phishing scheme to send out bogus requests for such information. Don't fall for it!

2: Avoid Banking While on Public Networks

Many mobile devices allow you to connect to different types of networks, including Wi-Fi networks. You might be tempted to check your balance or make some transfers while at your local coffee shop. But before you log into your account, make sure you're not connected to the public network.

Public connections aren't very secure -- most places that offer a public Wi-Fi hotspot warn users not to share sensitive information over the network. If you need to access your account information, you may want to switch to another network. If you're using a smartphone or other cellular device, disabling Wi-Fi and switching to a cellular network is a good solution. You never know who might be listening in over the public network.

3: Use Official Bank Apps When Possible

American National Bank offers applications for iPhone® and Android™ smartphones. These apps are more secure than sending information by SMS (text) message or e-mail. Download and install the American National Bank apps directly from the Apple App Store and Android Market by following the links below:

Click here for the Apple App Store

Click here for the Android Market

4: Be Careful What You Download

While malware is not as prevalent in the mobile device market as it is with traditional PCs, the fact remains that mobile devices are just specialized computers. That means it's possible for someone to design an app that could try to access your information. One way this could happen is if the app hides a keylogger.

A **keylogger** is a program that records, or logs, keystrokes. Every letter or number you enter into your phone could be recorded. If a hacker pairs a keylogger with code that sends off an e-mail or text message at certain times of the day, you might be sending all your keystrokes to someone anywhere on the globe.

For the moment, mobile devices are less prone to malware attacks than computers. But you should still be careful when downloading apps -- not just your banking app, but all apps. Do a little research before you download that next widget or game to make sure the app developer has a good reputation. And if you've jailbroken an iPhone or you've loaded unapproved apps, be aware that your data could be vulnerable.

5: Keep Track of Your Mobile Device

The biggest risk is also the reason why mobile banking is so popular, mobile devices are easy to carry around everywhere we go. They contain everything from passwords to contact lists to our calendar appointments. This information can be dangerous if your mobile device falls into the wrong hands.

There are a few things you can do to minimize your risk. If your device has a digital locking mechanism, use it. Some devices require you to trace a pattern or insert a PIN. While it might slow you down to have to enter a PIN each time you want to use your phone, that layer of security might be enough to keep a thief from accessing your bank account before you can report your phone as missing.

Don't be scared off from using your mobile device to access your bank accounts. Just be sure to practice good, safe behaviors and keep track of your gadgets. With a little common sense and attention, mobile banking can be both convenient and secure.