Mobile Banking Best Practices

Protecting the security of your money and identity is our priority.
Let's work together to protect it.

Your mobile phone is much more than just a phone. It's a computer in your pocket. Because it stores your personal information, contact lists, photos, videos and more, it's crucial that you protect it. Don't leave your phone lying in public areas. Lock your phone anytime it is lying idle. Use mobile phone security software (eg. Antivirus and Malware) and patch updates to protect yourself against viruses, trojans, hackers, thieves and other. The following list includes a few items to help you better protect yourself:

Secure your passwords

Having a strong password should be a priority. *One tip for creating strong, easy to remember passwords is to use phrases or sentences that include numbers, reduced down to abbreviations. For example, monkeys are fun to see, becomes mRf2c, which looks like a random group of characters but is much easier to remember.* ***(Do NOT use this as it is only an example)***. Change your password often. When you are finished accessing your online accounts or social networks, make sure to **LOG OUT**.

Research apps before you download them

Apps are one of the main ways malware and viruses enter a mobile phone. Do your research to find out if the app comes from a reliable source. Make sure to download updates regularly. These updates usually include fixes to security flaws discovered in apps.

Be cautious on public Wi-Fi networks

Many public Wi-Fi areas are not encrypted and are prime targets for hackers to access information. If you are accessing any type of personal information, be cautious and try to avoid apps and webpages that can identify you.

Don't jailbreak your phone

When you jailbreak your mobile phone, you are making it possible for an "unapproved" app to be downloaded onto your device and you may be removing needed security features. Although not foolproof, Apple, Android and Blackberry all have inspection processes they put apps through before they are approved to be put into the marketplace or store.

Be mindful with mobile banking

Mobile Banking uses encryption technology to ensure that all the data you are using is safe but there are still ways hackers and thieves can access your information. Sending text messages with even a user name to your account can be an aid in accessing your information. If emails or text messages from the credit union come to your mobile phone, look at them and immediately delete them. If you use your smartphone for mobile banking and your phone is lost or stolen, notify your credit union immediately. The credit union can then more actively monitor your account.

Document and register your mobile phone

There are numerous ways you can locate a lost cell phone. Almost all require that you sign up for something beforehand. First, write down somewhere safe your phone's IMEI, MEID or ESN number (it's on the sticker under the battery). That is a unique identifier you can give to the police or your wireless carrier if your mobile phone gets lost.

All the carrier-based services need to be activated before you lose the phone, because you either need to reply to a text message or change some settings on your phone to accept tracking. Android phone owners can load a third-party program which offers phone-tracking, remote lock, backup and wipe services. Apple iPhone owners can subscribe to MobileMe and use its Find My iPhone feature. BlackBerry users can try the third-party Berry Locator which will send a message to your lost BlackBerry and show you where it is on a Web-based map from any PC or use third-party tracking apps.