Let's Talk Finances

Tips for Mobile Banking

By Charles Schmalz
President of
East Wisconsin Savings Bank

Many consumers use mobile devices to access their online accounts, track spending, and manage money. However, since your mobile device could be easily lost or stolen, you should be sure to follow good security practices. With that in mind, we offer some tips that will help you use your financial apps safely and securely.

Set account alerts. Most mobile banking systems allow you to sign up for text or email alerts or push notifications on your mobile device to notify you if your account balance drops below a set dollar amount, thereby helping you avoid overdrawing from your account. You may also be able to receive alerts if your bank detects unusual activity or potentially fraudulent transactions involving your account. Some systems even let you set spending limit alerts to help keep track of your spending.

Research apps before downloading. Just because the name of an app resembles the name of your bank or another familiar company, that doesn't mean it is their official app. Fraudulent apps are created all the time, so take care to verify that you have the correct one before adding any personal information to your new app.

Be on guard against unsolicited email or text messages appearing to link to a financial institution's website. Those could be "phishing" messages, which often contain an urgent request (such as a warning that you need to verify bank account or other personal information) designed to lure you to a fake website where fraudsters hope to steal your information and ultimately your funds.

Be proactive in securing your mobile device. Never leave your mobile device unattended, and make sure you enable the auto-lock feature to secure your mobile device when it is left untouched for a period of time. Be sure to create a strong password or PIN on your mobile device and don't make it obvious (like your birthday or social security number). You should periodically change your pin or password, which also helps keep it secure. Most importantly, don't give that password or PIN to anyone, or write it down where others can find it. You may also want to consider using a mobile device with a biometric authentication method, which verifies your identity by scanning your physical characteristics, such as your fingerprint or face.

Be careful where and how you conduct transactions. Don't use unsecured Wi-Fi networks to conduct your private business. Fraud artists might be able to access the information you are

transmitting or viewing. Also, don't send account numbers or other sensitive information through regular email or text messages, because they are also vulnerable to hackers.

Take additional precautions if your device is lost or stolen. Check with your wireless provider in advance to find out about features that enable you to remotely erase content or turn off access to your device or account. Contact your financial services providers to let them know about the loss or theft of your device. Notifying your bank quickly will help prevent or resolve problems should any unauthorized transactions occur as a result.