You're the *One*™

MOBILE BANKING SECURITY

MidWest*One* Mobile Banking provides you with a convenient way to check your account activity on the go, transfer money, pay bills, pay other people and even deposit checks. Similar to other electronic banking services, the proper security controls should be in place to ensure your information remains safe. When it comes to security, it is best to treat your mobile device the same way you should treat a laptop or desktop computer. Here are our top mobile banking security tips:

Your First Line of Defense: Protect Your Phone

Mobile devices tend to get misplaced, which is why it is important to password protect your phone or tablet. Convenience is nice; but the more complex your password, PIN, swipe pattern or other form of authentication can be the better. This includes biometric authentication, such as fingerprint verification. When using fingerprint verification much as Touch ID® for iPhones, remember that anyone with a fingerprint registered in your device will be able to access the apps enrolled in Touch ID®.

Safeguards at Your Finger Tips: Utilize Security Features

Just as you protect your home computer with an anti-virus program, you should do that same for your mobile devices. Some devices come with an anti-virus preinstalled; but there are also plenty or free and paid services available. Many home computer anti-virus programs include protections for one or more of your mobile devices. It is also extremely import to ensure your device remains up-to-date with the latest software. Set you device and apps to update automatically. This will ensure you are protected from the latest vulnerabilities as soon as possible.

Proceed with Caution: Stick to Authorized Apps from the App Store

Only download apps from the authorized app store or via links directly from your financial institution's website. Fraudsters often create fake apps designed to trick users into entering their login information for secure sites. For the most part, app stores to a good job ensuring the authenticity of apps.

Don't be Fooled: Avoid Mobile Fraud Scams

You're probably familiar with the various types of scams carried out by telephone or e-mail; but fraudsters have also been known to use text messaging. Texting is not a secure form of communication; a trustworthy financial institution would never request personal information from you this way. Fraudsters also often put links to malicious websites in these texts or urge you to call a telephone number. If something doesn't seem right, contact your financial institution using the phone number on their website – not the number in the suspicious message.

Convenience vs. Security: Take Reasonable Precautions to Avoid Fraud

Other mobile banking security best practices include:

- **Don't access your financial information while connected to unsecured, public wireless internet**
- Delete old account alert text messages or e-mails
- **Review your account regularly for unauthorized activity**
- Familiarize yourself with the auto-lock and remote wipe features on your device
- Do not jailbreak or root your device

Message and Data Rates May Apply.

MidWest*One* Bank®

MidWest*One*.bank
800.247.4418

Member FDIC

EQUAL HOUSING LENDER

Updated 11/07/2016