TIPS FOR SAFE MOBILE BANKING

Today almost everyone has a smart phone and access to the internet right in the palm of their hand. Bank OZK' mobile banking app allows members to access their account while on the go! It is quick and easy to use with countless benefits, including: checking balances, transferring funds, paying bills and mobile deposit. You no longer have to come in to a branch to do your banking. While we are working to keep your account protected, here are 5 easy steps to help you protect yourself:

1. Don't follow links. Phishing refers to the practice of tricking someone into revealing private information via a text message, an email or even a fake Web site designed to mimic your financial institution's official site, which is called spoofing. Never follow a link sent to you in an unsolicited or unfamiliar text message or email. Bank OZK will never ask for your account information or password via text message or e-mail.

2. Avoid banking while on public networks. Many mobile devices allow you to connect to different types of networks, including public Wi-Fi networks. Never log in to your online banking account while connected a public Wi-Fi network. If you need to access your account information, switch to a secure network. If you are using a smartphone or other cellular device, disable the Wi-Fi and switch to the cellular network.

3. Use the OFFICIAL app. Many institutions, like Bank OZK, offer official applications in smartphone and tablet app stores. These apps tend to be more secure than SMS message or email.

4. Be careful what you download. 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 some code that either sends off an email or text message at certain times of the day, you might be sending all your keystrokes to someone anywhere on the globe. You should still be careful when downloading any apps.

5. Keep track of your device. Mobile devices contain everything from passwords to contact lists to our calendar appointments. Information like that can be dangerous if your mobile device falls into the wrong hands. If your device has a digital locking mechanism, you should use it. Some devices require you to trace a pattern or insert a passcode. While it might slow you down to have to enter this 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.

6. Do not use a "jailbroken" or "rooted" device to access your account. Such devices are more vulnerable to malware attacks.

7. Check with your wireless provider in advance to learn about features that will enable you to remotely erase content on the device or turn off access to the device.

8. If your device is lost or stolen, let us know. We may be able to prevent or resolve any unauthorized transactions.