IOWA STATE BANK

Mobile Banking Security Tips

Mobile devices (smart phones and tablets) are computers with software that have led to many conveniences, such as mobile banking, accessing email, and web browsing from the devices. Unfortunately, cyber threats have also continued to increase. The following tips can help protect you and your mobile device.

Lock your Device. Use the keypad lock or phone lock function on your mobile device so that when it is not in use, no one else can use it or view your information. Be sure to keep you device in a secure location when you are not using it to protect it from being stolen or used by an unauthorized party.

Use your mobile phone's security features. Enable encryption and remote wipe capabilities if available. Consider using additional security software and antivirus solutions that may be available for your type of mobile phone. Refer to your phone's user manual or contact your mobile provider for more information on these features.

Do NOT follow links sent in suspicious email or text messages. Do not follow these links as it may lead you to websites that cause malicious code to be downloaded to you device. Never reveal account information or passwords in an email or test message claiming to be from the bank. We will never ask you for this information via test or email.

Do NOT store sensitive or personal information on your mobile device. If an unauthorized party accesses your mobile device, you will be more vulnerable if you store personal information such as passwords and account numbers on the device. It is a good idea to delete browser history, test messages and files from your device regularly.

Be careful when downloading apps. Download apps only from reputable sources such as your provider's app store to avoid downloading apps with malware or malicious code.

Disable Bluetooth, infrared, or Wi-Fi when not in use. Attackers have been known to exploit weaknesses in software that uses these interfaces.

Set Bluetooth-enabled devices to non-discoverable. When in discoverable mode, your Bluetooth-enabled devices are visible to other nearby deices which may include a cyber-attacker's device.

Avoid joining unknown Wi-Fi networks or public Wi-Fi hotspots. Attackers can create fictitious Wi-Fi hotspots designed to attach mobile phones and may monitor public Wi-Fi networks for unsecured devices.

Protect yours money. When banking and shopping, check to be sure the site is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information.

Notify the Bank if your Mobile Phone is Lost or Stolen. If your mobile phone is lost or stolen, contact the bank to have your mobile app deactivated on the lost device. If necessary, wipe the phone. Some mobile service providers offer remote wiping, which allows you or the provider to remotely delete all data on the phone.

Delete all information stored in a device prior to discarding it. Check the website of the devices' manufacturer or as your service provider for information about securely deleting data. Your service provider may also have useful information on securely wiping your device.