Protecting Your Mobile Device

Your mobile device provides convenient access to your email, bank and social media accounts. Unfortunately, it can potentially provide the same convenient access for criminals. UNION Savings BANK recommends following these tips to keep your information – and your money – safe.

Use the passcode lock on your smartphone and other devices.
This will make it more difficult for thieves to access your information if your device is lost or stolen.

Log out completely when you finish a mobile banking session.

Protect your phone from viruses and malicious software, or malware, just like you do for your computer by installing mobile security software.

Use caution when downloading apps.
Apps can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary "permissions." For example, a Flashlight app doesn't need access to your location in order to work. Also, check the user reviews in advance of the download because it is a good resource for user feedback.

Download the updates for your phone and mobile apps.
Each time an update is made available, review the permissions and types of access the app is granted.

Avoid storing sensitive information on your phone.
Don't store passwords or a social security number on your mobile device.

Wipe your mobile device of data before you donate, sell or trade it.
Do this by using specialized software or using the manufacturer's factory reset process. Some software allows you to wipe your device remotely if it is lost or stolen.

Beware of mobile phishing.
Avoid opening links and attachments in emails and texts, especially from senders you don't know. And be wary of ads (not from your security provider) claiming that your device is infected.

Be cautious of public Wi-Fi.
Public connections aren't very secure, so don't perform banking transactions on a public network. If you need to access your account, try disabling the Wi-Fi and switching to your mobile network.

Be aware of shoulder surfers.
The most basic form of information theft is observation. Be aware of your surroundings especially when you're punching in sensitive information

Report
Report any suspected fraud to us immediately at 815-235-0800.