Mobile Device Security Tips

Use your devices built in Lock function – One of the best ways to protect your device is by having your device automatically lock with a strong PIN/password. Locking your device will help to prevent unauthorized access to your device and deter theft.

Do not "jailbreak" your device – "Jailbreaking" is the process of removing the locked features or limitations imposed by the provider's (ie. Apple, Android, Windows) operating system. Altering the firmware on a device may open it to security vulnerabilities and may prevent the device from receiving future operating system and security updates.

User your devices security features – Enable encryption and remote wipe capabilities if they are available. Refer to your phone's user manual or contact your mobile provider for more information on these features.

Keep operating systems and apps up to date – Manufacturers, service providers and software providers regularly update their software to fix vulnerabilities. Make sure your device's operating system and apps are updated regularly and running the most recent version.

Only Install Apps From Trusted Sources – Download apps from reputable sources only. You can download the First National Bank of Spearville iPhone App from the iTunes App Store. You can download the First National Bank of Spearville Android App from Google Play.

Guard Your Personal Information – If an app is requesting more permissions than seems necessary, do not install it. If the app is already installed then uninstall it.

Don't Respond to Requests for Personal Information – Fraudulent emails, texting, calling and voicemails are on the rise. Requests for personal information or a request for immediate action are almost always a scam. First National Bank of Spearville will never make an unsolicited request for your private information.

Don't use public Wi-Fi – Smartphones and tablets are susceptible to malware and hacking when using unsecured public networks. To be safe, avoid logging into accounts, especially financial accounts, when using public wireless networks or free Wi-Fi hotspots.

Disable unwanted services/calling – Capabilities, such as Bluetooth, provide an easy way for a nearby, unauthorized user to gain access to you data. Turn these features off when they are not required.

Use a mobile security software solution – Install anti-virus software, if available.

Block web adds or don't click them – Malware can find its way on to your mobile device through a variety of methods, including advertisements. The malicious ads are especially dangerous because they are often delivered through legitimate ad networks. Messages may not appear to be outright spam, but can lead to malicious websites when clicked on.

Don't click suspicious links and attachments – It may be difficult to spot some phishing attempts, so it's important to be cautious about all communications you receive, even if it is from a familiar sender. Be careful when clicking on links or attachments contained within messages.