Carolina ALLIANCE BANK™

here for you. *every day.*

12 Ways to Protect Your Mobile Device from Hackers

As more and more consumers rely on their mobile devices to bank, browse and shop on the internet, it is extremely important that they exercise certain measures to protect their devices from online threats. The American Bankers Association is recommending 12 tips to help consumers safeguard their data and protect their mobile devices from fraudsters.

"Mobile usage has grown tremendously in recent years and consumers are using their phones to access and transmit very sensitive information," said Doug Johnson, ABA's senior vice president of payments and cybersecurity policy. "It's extremely important that consumers avoid doing their banking and shopping on unsecure networks to limit their exposure to online threats."

ABA recommends that consumers take extra precaution to protect the data on their mobile device by doing the following:

- 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.
- Download the updates for your phone and mobile apps.

Carolina ALLIANCE BANK™

here for you. *every day.*

- Use caution when downloading apps. Apps can contain malicious software, worms and viruses. Beware of apps that ask for unnecessary “permissions.”

- Avoid storing sensitive information like passwords or a social security number on your mobile device.

- Tell your financial institution immediately if you change your phone number or lose your mobile device.

- 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.

- Wipe your mobile device before you donate, sell or trade it using specialized software or using the manufacturer’s recommended technique. 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.

- Watch out for 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.

- Report any suspected fraud to your bank immediately.