

Mobile Banking Security Tips for Consumers

Many of us can't imagine life without our mobile phones. Not only do they store all your contacts, making it unnecessary to remember a phone number ever again, but depending on the type of phone they also allow you to send text messages, check and send e-mail, browse the web and check your account balances on the go.

While Text and Mobile Banking is certainly convenient, they can pose a security risk if users aren't careful. Here are several ways you can protect your phone or tablet from cyber threats.

1. **Password-protect your mobile device and lock your device when it's not in use. Keep your mobile device in a safe location.**
2. **Don't use the auto-login feature on your phone**
3. **Avoid storing confidential information like passwords and social security numbers on your mobile device.**
4. **Save mobile links as bookmarks to avoid mistyping the URL.**
5. **Add Wauchula State Bank's SMS short code to your device's contact list with a distinctive name. This will allow you to recognize that incoming messages are from Wauchula State Bank and not spoofed.**
6. **Be aware of your surroundings. Do not type or display any confidential information if others around you can see.**
7. **Log out completely when you complete a mobile banking session.**
8. **Frequently delete text messages from us on your mobile device, especially if they contain sensitive information.**
9. **Never disclose personal information about your accounts via a text message, i.e. account numbers, passwords, or any combination of information that can be used to steal your identity.**
10. **Protect your data in case of theft.** Because they're so portable, the biggest threat to a mobile device is loss or theft. Several mobile products offer features to locate and recover a lost or stolen phone. Typically they also include the ability to lock the phone and wipe out all private data if it can't be recovered. There are licensed security programs available for mobile devices that allow you to remotely lock and wipe the phone by text message.
11. **If you change your mobile number or lose your mobile phone, immediately disable your device within your Online Banking User Services – Mobile Enrollment page or contact customer service during regular business hours to change the details of your mobile banking profile.**
12. **Protect your phone from viruses and malware** just like you do for your computer by installing mobile security software. Apps are available that let you scan your phone for malware and back up and restore your data online. These apps scan other apps, settings, media and phone contents in search of suspicious files.
13. **Be aware that malware exists and fraudulent applications will continue to pop up.** Don't download applications onto your phone without checking them out first. If in doubt, verify the legitimacy of Wauchula State Bank's Mobile Banking application with us before downloading it to your Smartphone - verify that the app publisher is Wauchula State Bank, or if possible, go through our Home Page to download the application.



Wauchula State Bank

14. **Download the updates** for your phone and mobile apps
15. **Report any suspicious banking application that shows Wauchula State Bank's name and/or logo** and appears to be malicious to us at your earliest convenience.
16. **Monitor your accounts regularly** and consider having electronic alerts on account activity sent to your email or mobile device. Please report any suspicious activity to us immediately.
17. **Encrypt data.** Install an encryption solution if confidential data must be accessed or stored using a mobile device, but you should avoid using or storing confidential data whenever possible.
18. **Connect to secure Wi-Fi networks and disable Wi-Fi when not in use.** When you're not using them, it's best to disable features like Bluetooth, infrared or Wi-Fi. Avoid joining unknown Wi-Fi networks when you need to connect.
19. **Use caution when downloading apps.** Check consumer reviews before you download an app. When you search for an app in the store, many of the descriptions will include recent reviews from other people who downloaded the app. Read the app's privacy policy, which contains disclosures about what information the app collects and how it uses that information.
20. **Review and set privacy settings.** Many apps have privacy settings within the app itself, typically in the "settings" or "privacy" tab. The settings can manage activities like whether the app can access your local information. Check the privacy default settings to make sure you agree with them. You can also review the privacy settings for your device's operating system. For example, you can turn off the phone's ability to geolocate you or create a password to protect the phone.
21. **Never unlock or "jailbreak" the default security settings.** While some sites may promote the use of unauthorized applications, games, etc., the end result is the same – you've left your device open for criminals to abuse with targeted mobile malware. You should never override the security settings in your tablet or phone, especially if you plan to access personal or business email, mobile banking or other sensitive information on the Internet.
22. **Replace your phone properly.** Many wireless providers offer programs that encourage you to upgrade your phone every few years. If you decide to get the latest model, be sure to delete all information stored in your device before discarding, exchanging or donating it.
23. Research shows a steady, significant growth in mobile malware. Numerous security experts have issued warnings recently about cybercriminals' increasing interest in mobile platforms. Following the steps outlined above will go a long way toward thwarting some of these threats.



Wauchula State Bank