Navigant CREDIT UNION®

Mobile Banking Best Practices

Mobile devices are becoming more and more of a standard tool for businesses, and banking is just one of the functions many business members use regularly on their portable devices.

With this trend, comes a need to ensure business members are employing mobile security best practices to safeguard their information. Below are the top 10 actions users can take to secure their devices.

1. **Lock your device with a personal identification number (PIN), password or biometric options such as Fingerprint or Face ID.** It may seem basic, but locking your device is the first step to stopping unauthorized use. It's not hard to do, and it's very important! Make it a strong password that is difficult to crack. Configure your device to lock automatically after a certain amount of time.
2. **Keep your phone operating system updated**. Download the latest release updates when you are notified of them to ensure any security patches included are installed and active.
3. **Install apps ONLY from trusted sources and stores**. Do your homework before you download an app for your smart device. Read reviews and application permission requests before agreeing and downloading the app.
4. **Consider adding a reputable mobile security app to your phone for additional protection**.
5. **Back up your data**. Most smart devices will allow you to back your data up to a cloud solution or hard drive so if the device is lost or damaged, you will still be able to retrieve your data.
6. **Log out of banking and shopping sites**. This makes it harder for unauthorized users to make fraudulent transactions.
7. **Avoid clicking/opening emails, links or attachments that you don't recognize or look suspicious.** These are often associated with Phishing attacks that enable others to break into your system.
8. **Don't 'jail break' your own device.** The Operating Systems on Mobile devices are carefully designed to maximize productivity and security. Jailbreaking the device may weaken security controls and introduce stability issues.
9. **Consider disabling Wi-Fi, Bluetooth, and Location Services when not using them**. Leaving them on all the time makes it easier for unauthorized individuals to access your information and attempt fraudulent transactions. Never log into your business banking application when on an unsecure Wi-Fi connection. Notify the credit union if you will be traveling for business or pleasure and plan to access your banking account from another state or country.

10. **Be mindful when using Mobile Banking applications.** Look for common features such as strong authentication using SMS codes or tokens. Look for dual approval functionality and alerting capabilities. Avoid using transactional applications that do not offer robust security features and functionality.