Central Bank

www.centralbankfl.com

Mobile Banking Security Tips

Member FDIC

Secure access to your accounts

When using our Mobile Banking application you're protected by these security features:

* Advanced encryption technology to help prevent unauthorized access
* Privacy protection of our financial information as detailed in our Privacy Notice located on our website.

Text Banking
By using our text banking, you can get quick access to balance and transaction information without exchanging personal information such as your full account number, PIN or email address

Secure technology
Our fraud prevention and security systems help protect you with the latest encryption technology and secure email communications.

Update your mobile devices
Mobile devices are essentially small computers with software that needs to be kept up to date just like on a PC or laptop. Make sure all the mobile devices in your house have the latest security protection. This may require updating your devices with a computer. Check the website of your devices manufacturer or mobile carrier for the latest software updates.

Guard your personal information
Protect your phone or tablet device just as you would your computer. Secure your mobile device by using a strong passcode and be cautious about the sites you visit and the information you release.

Think before you app
Before you download an application (app) on your device, review the privacy policy and understand what specific data the app can access. Only download apps from reputable sources.

Protect your money
When banking and shopping on your mobile device, check to be sure the sites are secure. Look for web addresses with https: in the address. This means the site takes extra measures to help secure your information. Many sites now feature a color-coded browser. If you see a green highlighted browser, this is a safe site. However, yellow and red sites should be avoided.

When in doubt, don't respond
Fraudulent texting, calling and voicemails are on the rise. Just like in fraudulent email, requests for personal information or a call for immediate action are almost always a scam.

Stay informed
Follow mobile security issues in the news and explore online resources which are listed on our website under the Cyber Security and Financial Education tab.

Fake Mobile Banking apps

Criminals may develop and publish fake mobile banking applications that look like official Central Bank but are in truth designed to steal your Online Banking credentials. Here are tips for recognizing an unofficial Central Bank app:

- The developer or author of the application is not Central Bank.
- The app is being promoted on a third-party site, somewhere other than the official app store for your mobile device.
- There is a charge for downloading the app—Central Bank does not currently charge for mobile app downloads.
- To help protect your accounts and information, never download or install a Central Bank Mobile Banking app if you spot any of these warning signs.

SMShing

SMShing and smishing are like phishing (which typically happens via email), but take place via SMS text message. A criminal sends you a text message that tries to trick you into replying with financial or personal information or clicking on links that will sneak viruses onto your mobile device. Don't respond to a text message that requests personal or financial information. Central Bank will never ask you to provide your information in this way.

Lost and stolen devices

Mobile phones and tablet devices offer convenience, but they're also easy to lose or steal, which can put your information at risk. Here are some ways you can protect yourself now in the event your device is lost or stolen later:

- Password-protect your device so it can't be accessed unless the password is entered.
- Enable an automatic screen-locking mechanism to lock the device when it's not actively being used.
- Consider using a remote wipe program that gives you the ability to send a command to your device that will delete any data.
- Keep a record of the device's make, model and serial number in case it's stolen.

Traditional online threats

Viruses, malware and other programs intended to steal your personal information or financial details are able to infect some mobile devices. If your tablet supports a traditional anti-virus product, consider installing that software. Backup the device's data and keep the copy in a safe and secure location. This will allow you to restore your data in the event you need to wipe the device clean in order to remove a harmful software threat.

Central Bank Mobile App can be downloaded from:

Available on the App Store

GET IT ON Google play

Our application name: CentralBankFL Mobile GoDough: