First County Bank™
It's where you belong.

CustomerFirst
CONTACT CENTER
Weekdays 203.462.4400
Touch Tone 203.462.4300

MOBILE BANKING: PERSONAL INFORMATION SECURITY TIPS

Mobile Banking is an increasingly popular way to monitor and manage your money. A Federal Reserve study published in March 2014 found that 51% of smartphone owners had used mobile banking in the previous 12 months, up from 48% last year. Among consumers who don't use mobile financial services, 69% cited security concerns as a reason they hadn't.[1]

Here are some tips that can help you to keep your personal information out of the hands of cybercriminals while using your mobile device.

- **Passcode protect your mobile device.** Passcode-protect your mobile device and enable the screen lock feature after a few minutes of inactivity. This will make it more difficult for thieves to access your information if your device is lost or stolen.

- **Know the features of your device.** When purchasing a smartphone, know its features and default settings so that you can reduce the attack surface by turning off features that you don't use.

- **Log out completely.** When you finish a mobile banking session "log out".

- **Obtain malware protection for your mobile device.** Protect your phone from malicious software viruses by installing antivirus apps.

- **Use caution when downloading Apps.** Beware of apps that ask for unnecessary "permissions" that are not key to their functioning. Look at app user ratings, reviews, and the number of downloads, and steer clear of any that are badly rated or seem unpopular. Use only official bank apps.

- **Download the updates.** Updates don't just add new features; they remove bugs, plug security holes and protect your operating system from emerging cyber threats.

[1] The Board of Governors of the Federal Reserve, March 2014, "Consumers and Mobile Financial Services, 2014", http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf

- **Be cautious when connecting to unknown wireless networks.** These networks could be rogue access points that capture information passed between your device and a legitimate server.

- **Avoid storing sensitive information.** Passwords or a social security number should not be stored on your mobile device.

- **Be aware of shoulder surfers.** Be aware of your surroundings as most basic information theft is accomplished by observation.

- **Wipe your mobile device before you donate, sell or trade it.** Specialized software or manufacturer recommended techniques can be used to wipe your device clean of data.

- **Report any suspected fraud to your bank immediately.** Tell your bank immediately if you change your phone number or lose your mobile device.

If you have any questions, please feel free to call the CustomerFirst Contact Center at (203) 462-4400.