Mobile Banking Security Best Practices

Go to your app store and search: **SouthSoundBankMobile**

According to recent studies, security is the number one fear among potential mobile banking customers. The good news is that technology advancements and established risk mitigation do make mobile banking secure and safe. In addition, mobile banking is a great tool you can use to detect fraudulent activity because it provides an easy way to check your account on a regular basis for suspicious activity. The security measures and best practices include:

- **Account Data** – No confidential customer information or account data, such as account numbers, are ever stored on your mobile device, and sensitive information is not sent via text messages.
- **Activation** – The installation process that is used between the Online Banking software and your Smartphone. Activation requires customers to use their existing online banking access ID and password. Your device is authenticated using a one-time security code via SMS (text) message or answering a series of questions obtained from the Online Banking software.
- **Alerts** – You can set up alerts to notify you of account balance information or check(s) clearing. This information can be sent via text message and will contain masked account numbers. Alerts created in Online Banking will arrive to your selected device in accordance with the chosen alert. **Do not respond to these messages.**
- **Anti-Virus Software** – Install mobile anti-virus and anti-spyware software on your device and keep it updated.
- **Application Downloads** - Only download and install a bank application from reliable sources such as Apple iTunes or Google Android stores; and report any banking application that appears to be malicious to South Sound Bank.
- **Bill Pay** – You can send money to billers, however you need to log into your Online Banking via a computer to set up new billers.
    - **PopMoney –** You can send, receive, and set up PopMoney Transfers
- **Bluetooth** – Disable your Bluetooth or set the Bluetooth status as hidden until you want to share something.
- **Connection** – Only connect to the Bank via a secure connection or a non-public Wi-Fi network and remember to log out of the mobile banking app when you are finished with your session.

- **Device Fingerprinting** – Upon activation, our system creates a "fingerprint" of your device. The enhanced layer of security enrolls your phone to our system. The system collects non-personal information such as screen size, device address, and operating software version so that the system can have another form of authentication to confirm the correct user is accessing our software.
- **Device Profiling** – Mobile banking not used in the last 90 days may require stepped up authentication to enhance security, which includes answering security challenge questions.
- **Encryption** – The transport layer is secured from the mobile device to the web service using SSL (HTTPS). The link from the mobile device to the mobile app is secured using SHA256. This security ensures that the device you're using acknowledges the trust certificate assigned to South Sound Bank. The data is encrypted using AES-256.
- **Firewalls and Routers** – This software program protects against unauthorized malicious intrusion. It is best practice to check your device to ensure that you have protection in place.
- **Fraud** – Suspect fraud related activities? Call your Branch of Account immediately.
- **Identity Protection** – Never respond to a "phishing" text or email that requests your PIN, account number, or any card information. South Sound Bank will never request this information in this manner. And don't open files that are unsolicited if they are not from a known source.
- **Locked Out** - To unlock your access to Mobile Online Banking, call your branch of account to have a staff member unlock your Mobile Access.
- **Lost or Stolen Phone or Tablet** – Call your branch of account for assistance.
- **Monitor** – Monitor your accounts on a regular basis to more readily detect unauthorized activity.
- **Transfer of Money** – You can transfer money to and from your South Sound Bank accounts.
- **Unauthorized Transaction** – In the event of an unauthorized transaction, certain protections are in place for consumers as long as the error is reported to the Bank within 60 days of receiving your statement showing the unauthorized activity.
- **Username and Password** – Used to confirm your identity and ensure the confidentiality of your mobile banking session, sessions will be locked out after three incorrect login attempts. Never share your access credentials. Best practice is to never automatically allow your device to log you in or save any of your login information. In addition, have a password set to protect your device when not in use.

Mobile Capture Best Practices

The following are tips and/or requirements for using Mobile Capture with South Sound Bank. Please read through each of the below items before using this product.

- Before logging in, close all apps.
- Sign in and select deposit.
- Sign/Endorse the back of your check and label it "**For Mobile Deposit Only**".
- Enter check amount into the deposit amount box and carefully review item to confirm that the legal and written amount are the same.
- Flatten folded or crumpled checks before taking your photos.
- Keep the check within the view finder on the camera screen when capturing your photos. Try not to get too much of the areas surrounding the check.
- Take the photos of your check in a well-lit area.
- Place the check on solid dark background before taking the photo.
- Hold the camera as square to the check as possible to reduce corner to corner skew.
- Make sure that the entire check image is visible and in focus before submitting the deposit.
- Make sure no shadows across the check.
- Make sure all four corners are visible.
- Make sure the check image is not blurry.
- Make sure the MICR line (numbers on the bottom of the check) is legible.