

Simple Steps for Secure Mobile Banking



“Banks invest millions to secure their banking channels, including mobile banking, but it takes consumers making good decisions to avoid carefully crafted scams and schemes, as well.” – Independent Community Bankers of America (March 10, 2010)

Mobile Banking and Associated Risks

Southwest Missouri Bank offers mobile banking by text messaging (SMS or short messaging service) or through mobile Web.

SMS communications involve text message exchanges between customers and banks. Customers with registered phones can request text alerts, balance inquiries, and transaction inquiries. Because the Bank will only accept instructions from the registered phone, lost or stolen phones are at risk.

Mobile Web, like online banking, uses an Internet browser to give customer access to the Bank’s Web site. As such, mobile browsers are susceptible to the same kind of security risks (viruses, malware, phishing scams, and spoofed Web sites) as their home or office computer counterparts.

Seven Steps to Safer Mobile Banking:

1. Never provide personal identification or banking information over your mobile device unless you initiate the contact and you know that you’re dealing directly with the Bank.
2. Assume any unsolicited text request for personal or banking information is fraudulent. Giving this information places your finances and privacy at risk.
3. Avoid sharing sensitive information such as your password, account number, or answers to secret questions. Don’t save this information anywhere on your mobile device or phone.
4. Don’t set the Web or client-text service to automatically log you in to your bank account. If your phone is lost or stolen, someone will have free access to your money.
5. Set the phone to require a password to power on the handset or awake it from sleep mode.
6. Notify the Bank immediately if you feel your personal banking information has been compromised.
7. Contact the Bank and your mobile service provider if your phone is lost or stolen.