Smartphone banking opens door to ill-doers

November 8 2013, by Richard Burnett

Matt Certo jumped at the chance to use his smartphone for banking as soon as his bank offered the service a few years back.

The Orlando, Fla., high-tech entrepreneur understood the technology and knew the benefits. But he also was aware of the risks.

"If I'm traveling in places where there are Wi-Fi networks I don't know, I certainly think twice about using mobile banking," said Certo, 37, chief executive of WebSolvers Inc., a digital-marketing company. "I'll use it at home to check my account, even in church to give a tithe. But not on an open Wi-Fi network just anywhere."

Many consumers find themselves facing similar security concerns as smartphone banking becomes even more popular.

Despite its seeming simplicity, however, there is far more than meets the eye to practicing safe smartphone banking, industry experts say.

"If you don't take precautions - like using only Wi-Fi networks you know are secure and making sure nobody is looking over your shoulder to see your password - then you're just increasing the odds of something going wrong," said Greg McBride, senior financial analyst for Bankrate.com, a consumer-finance company.

So far, however, nothing on a large scale appears to have gone awry in the brief history of mobile banking, experts say. There have been no massive security breaches or cyberheists of data, they say, such as those

that have occasionally hit the conventional computers of some retailers and financial institutions.

Driven by the convenience, the popularity of smartphone banking has grown dramatically in recent years. According to a recent Federal Reserve survey, 87 percent of smartphone owners now use their devices for at least some banking transactions.

Still, there are signs hackers have already begun to target smartphone users, experts say. Smartphone attacks - known as "smishing" - are on the rise. Bogus text messages purport to be from a bank, luring the user to click on a link to a fake mobile website where malicious software could invade their phone and steal their personal data.

Once malware is on your phone, all bets are off when it comes to the security of your data, said Kevin Wright, senior vice president of information technology for CFE Federal Credit Union, based in Lake Mary, Fla.

To avoid being a victim, people must know how to verify that a text message is really from their bank and what clues would signal a fake mobile website, he said. Such details should be provided by the bank when a customer signs up for mobile banking.

Customers should also avoid using a mobile Web browser for smartphone banking on a Wi-Fi network because such browsers are more susceptible to being hacked, Wright said. It is safer to use your wireless-service network and your financial institution's mobile-banking application, which should be equipped with the latest data-encryption technology, he said.

Though large banks were generally the first to the mobile market, smaller financial institutions are quickly catching up, said Suzanne W.

Dusch, vice president of marketing for the CFE Federal Credit Union.

"We entered the mobile market early several years ago, and we're on the second generation of it now," she said, adding that about a third of CFE's nearly 130,000 members now regularly use mobile banking.

Lucy Boudet, an executive at Valencia College, said she uses mobile banking to deposit money in her forgetful father's bank account when his bills are due. After scanning the check and clicking the deposit, she waits until she gets a confirmation from the bank, then shreds the check.

"I'm not typically an early adopter," she said. "But this is so neat, and it makes the whole thing so convenient, you can't help but like it."

PRACTICING SAFE MOBILE BANKING:

-Use your bank's app to connect, not a mobile Web browser.

-When possible, use your wireless network, not Wi-Fi hot spots. Beware of logging in over an unfamiliar public Wi-Fi network. If you really must use Wi-Fi, first make sure it is secure. Ask questions.

-Log out when finished.

-Beware of bogus text messages claiming to be from your bank.

-Periodically check your phone for unfamiliar apps that could be malware.