The Do's and Don'ts of Mobile Banking

These days, your bank may be as close as your phone. But the increasing reliance on smartphones for financial transactions means that the bad guys are targeting these devices.

It's critical to exercise caution when you bank by phone, says Kevin Travis of Novantas, a consulting company for the financial services industry. "You've got to think about your smartphone as if it is a home computer," Travis says. "A lot of people still think of it as just a phone."

How thieves target your phone

You might be familiar with phishing, where criminals attempt to obtain your personal information by posing as a legitimate entity. Thieves are using text messaging, as well as email and instant messaging, to continue phishing via mobile devices. Keylogging viruses and Trojans that can track your user name, password and other information are a growing threat to smartphones, cautions Vishal Jain, a mobile services analyst with The 451 Group research company. Google pulled 50 apps from the Android mobile app store last December, following reports that they might be an attempt to phish for financial information.

Protect your financial information

Follow these do's and don'ts to safely bank by phone:

- **Do password protect your phone.** It might sound basic, but too often many people find it inconvenient to type in a password to access information on their smartphones. Take the time, advises Jain. "Since the phone is always with you, the biggest risk is losing it," he says.
- **Don't choose automatic login options.** You may pay for convenience if you rely on automatic logins, notes Jain. Don't store any login information on your mobile device either. "Never use the notepad on your phone to keep track of your banking password or other passwords," Travis says.
- **Do install mobile security software.** Protect your sensitive data with strong security software designed for a mobile device. It will help block viruses that can attempt to track every key you push.
- **Do choose your bank carefully.** Right now, according to Travis, larger financial institutions have invested in building mobile banking applications. Smaller, community-based banks may not yet have put as much resources into developing mobile banking options. "The number one way to avoid fraud is to do business with a bank that has invested significantly in security and technology designed specifically for mobile phones," Travis says.
- **Don't install third-party apps.** Only download apps from trusted sources, such as links sent by your bank or directly from your bank's website, advises Jain. Large banks may let you download the app by communicating with the bank's website, notes Aaron Maxwell of Mobile Web Up, a company that helps businesses develop a mobile presence. For instance, you can click an online banking option on the Bank of America site, select your state, indicate which smartphone you own and type in your cell phone number. Bank of America texts you with an official link to the app store. "There's no chance of accidentally picking up a phishy app instead," says Maxwell.
- **Do use your bank's mobile website.** Make sure you're actually on your bank's website by typing the name into your browser. "Remember, too, that on most smartphones, you can save a website with an icon on your mobile desktop screen, just like with an app from an app store," notes Maxwell.
- **Do communicate carefully with your bank.** Understand that your bank won't send emails or texts asking for personal information. Don't save messages from your bank containing passwords.

"As we move to this virtual type of technology, it creates more opportunities for fraud," says Travis. "The biggest risk for mobile banking is the onslaught of phishing attacks, because this is a really cheap and low-cost way of stealing your identity."