

5 Easy Rules for Safe Mobile Banking



Not sure if a check cleared? Check your account balance. Running low on funds? Transfer money between accounts. Need to pay a bill? Use online bill pay, all while renewing your drivers' license.

Mobile phones make life's necessities fast and convenient, but the steady increase in cyber attacks over the last few years has people asking, is mobile banking safe? According to stories reported by MSNBC, the Vancouver Sun, and guidelines on the Symantec website, it can be. As long as you follow these five simple rules:

1. Use different passwords for each of your accounts, including social media. According to the latest threat report from Symantec, cyber criminals are mining social networks, tracking internet searches and employing phishing schemes in attempts to gather personal information commonly used in passwords. Most people use the same password for all of their accounts, so attackers know if they crack one, they'll have access to all. Protect yourself with complex passwords (capital and lower case letters, numbers and symbols) and set a recurring reminder to change them frequently. Running out of ideas? Try using lyrics from a song or a line from your favorite book or magazine article.
2. Do not access your accounts outside your bank's official mobile banking application. Two popular schemes used by hackers involve selling legitimate applications tainted with malicious logic, and sending users to a website that looks like their bank's but is really a digital façade. In both cases, people unwittingly open the door to their personal information. Your bank's official mobile banking application will take you directly to their secured site, allowing you to manage your money while lowering your risk of attack.
3. Download anti-virus software. For most of us, the installation of security software on personal and work computers is a given, but when it comes to our smartphones we see it

as excessive. This is a mistake. Security experts agree that smartphones are like small computers with as much or more access to personal information as our laptops, and we should protect them in the same way.

4. Do not respond to or click through emails that appear to come from your bank and/or ask for personal or account information. This common phishing scheme gives cyber thieves complete access to your finances and before you know it, you're cleaned out. Your bank, credit card company and investment firm will never ask you for this information and it is always safer to access accounts via your bank's approved application or by typing the url into your browser than by clicking on a link. This is true, even if the link was sent through legitimate communication.
5. Set up automatic bill pay on your bank's website in lieu of having companies electronically pull money from your account. This keeps you in greater control of your money and minimizes the number of people and entities who have access to your account. It is also makes it easier to see suspicious transactions.