Tips to Secure Mobile Banking Services

Here's how you can secure your mobile banking services to keep all your financial data from harm.

Security Tips for Mobile Banking

Use Authentic Banking Software

Make sure you install authentic software on your mobile phones, and ensure it is from a trusted and approved source. Most of the banking software for mobile phones is developed by third-party firms, so before you download anything, confirm with the bank for the authenticity and the latest version.

Password Protection

Protect your mobile with a password, and set the maximum number of incorrect passwords a user tries to enter to three. After three unsuccessful attempts, the mobile should automatically wipe out all the data that is stored on it for security reasons. Choose passwords that are composed of alphanumeric and special characters, and those which others cannot guess. Do not use date of birth, SSN, or any names as passwords. Change your password often.

PIN Protection

Change the personal identification number (PIN) or access code for your phone regularly and do not reuse old pins. Use a combination of numbers that is difficult to guess for anyone, and does not include SSN or date of birth.

Manage Personal Information

Avoid storing your bank account details (account number, credit/debit card number, PIN) on your phone. Do not use the auto-fill option on the browser which stores your mobile banking user ID and password. Never share these details or any other information with others through texts and e-mails via your phone. Make it a point to go through your account statements on a regular basis if you are into mobile banking and bring any unusual activity to the notice of the bank immediately. If you receive paper statements, save them in case you need to track your transaction details; they might also be helpful to reverse a transaction you never actually carried out. If you have signed up for text alerts, you should be alerted of every activity being carried out on your account. If you give your mobile for repair, delete the browsing history, cache, and any other temporary folders that may contain sensitive data so that it does not fall into the wrong hands. Disable any mobile banking application you might have downloaded. Keep the Bluetooth feature disabled if not in use. Install an antivirus software on your mobile device which will protect the data and keep malicious viruses away. Always remember to log out from the banking application after you have completed your banking transactions. Never log in to your banking account over a non-secure Wi-Fi network, like the ones at a coffee shop or a shopping mall.

Beware of Phishing

A technique used by schemers to illegally acquire personal information from users without their knowledge. When it comes to mobile banking, phishers send fake text messages to users asking for their bank login details. In some cases, users may also receive instant

messages and e-mails which ask them to dial a phone number or directs them to an authentic-looking website which prompts them to log in and reveal all account information. Other ways of phishing prompts users to download applications on their smartphones, which install the harmful keylogging virus which can track the keys the users press, which then enables phishers to monitor the activity on their victims' devices to gain access to personal data. In many cases, users do not realize that the texts and emails sent are fake, or that they are being directed to a fake website since it looks just like the bank's login page. Be very careful if you receive any such texts or e-mails. As a rule, banks will never ask you for your PIN, credit/debit card number, SSN, or any other account information via a text message or e-mail. If you are doubtful about the source of the e-mail or text message and receive any such message, delete it! It's likely an attempt to phish for information.

Report a Lost/Stolen Mobile

In case you lose your mobile, report it immediately to the local police as well as your service provider. Then call the bank and request them to deactivate the banking applications you might have downloaded, so no one can gain access to your account information.

Mobile banking is not without its pros and cons. On one hand, you have all the information you need at your fingertips at the click of a button and the slide of a finger, and do not need to visit the bank. But at the same time, you must remain attentive at all times by keeping a tab on your account activity so your data and money remain safe and secure.