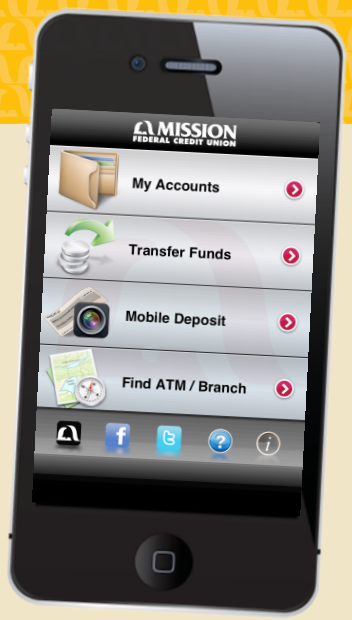
Mission Fed FAQs



Safe Mobile Banking Practices

Do you use mobile banking? If so, you are part of the growing number of consumers who do. According to a March 2013 report from the Federal Reserve, 87% of the U.S. adult population has a mobile phone and 52% of those are smartphones. Of those consumers with smartphones, 48% had used mobile banking in the previous 12 months, which was up from 42% from the December 2011 survey.

Many consumers use mobile devices to check balances and recent transactions, transfer money, make payments and deposit checks. If you already use mobile banking or are planning to use it, here are some tips to help you use it safely and securely.

Make Sure Your Mobile Device is Secure

Protecting your mobile device provides security not only for your financial transactions, but for all of your information stored on the device.

Use a strong password

To it make it more difficult for someone to access your device, you should secure it with a strong password. Don't use a password that you've already used for any of your accounts or sites. A strong password consists of combinations of lower and upper-case letters, numbers and symbols, and uses the maximum number of characters allowed.

Use security software

Mobile devices are powerful computers and need to be protected just like laptop and desktop computers. Security software can provide protection against viruses, malware and other threats to your personal information. Some security packages also provide features that can help you locate your phone if it is lost or stolen, remotely lock it and remotely wipe the data. Many devices come with security features installed, though you may need to activate them.

Secure your device when it's not in use

Always lock your device when you aren't using it, even if it is nearby.

Don't allow downloads from unknown sources

If you have an Android phone, make sure that the "install from unknown sources" feature is disabled. (It may not be available unless you have an optional memory card installed.)

Don't jailbreak, root or otherwise modify your phone

Overriding or defeating security or other limitations placed on a device is called jailbreaking or rooting. Doing so can disable security features making it vulnerable to malware, viruses, Trojans, and other malicious software.

Keep Bluetooth turned off and use it only when necessary

Make sure it is off when conducting any mobile banking activity. An active Bluetooth connection can allow nearby Bluetooth-enabled devices to connect to your phone and collect data without your knowledge.

If your device is lost or stolen, notify your carrier, your credit union and other financial institutions immediately

Your carrier can then deactivate your device. Your credit union and other financial institutions can take steps to protect your account.

Mission Fed FAQs

Use Your Mobile Device Securely

Because your mobile device is a computer, just like your laptop and desktop, you should use the same security precautions with your mobile device.

Only download apps that are signed and are from a trusted source

Before downloading an app, research it and make sure that you know what it does, what information it accesses (such as your contacts) and what permissions it wants. After installing it, monitor what the app does on the phone.

Don't store username and passwords on the device

If you must, encrypt them.

Don't allow any app to automatically login to your accounts

That helps prevent unauthorized access of your accounts.

Always log out

Even though financial institutions typically will automatically log you out after a period of inactivity, you should log out when you are finished.

Encrypt your sensitive information

Many devices have a setting that will encrypt the contents of the device and require a password to un-encrypt it.

Delete text messages received from your financial institution

If your financial institution offers messaging via texts, delete these texts frequently, as that can help prevent fraudulent access of your accounts.

Don't respond to text messages or emails asking for personal information, Social Security numbers, ATM/credit card/debit card numbers, or account numbers

Never provide personal information in a text message or an email. Your credit union will never ask for personal information or account numbers in a text or email.

Don't click on links in texts or emails from unfamiliar sources

Don't open unexpected attachments

Attachments can contain malware. Even if you know the sender, verify that they sent it before you open it.

Make Transactions Securely

Only use your credit union's app or mobile banking site to make your transaction

Use a secure network

Use your cellular network or a known secure Wi-Fi network to make your transaction. Your account and personal information could be intercepted with an unsecured Wi-Fi network.

Review your accounts frequently

You should always review your accounts frequently, whether or not you use mobile banking, and report any fraudulent transactions or other issues with your account to your credit union or other financial institution.

Mission Fed FAQs

For More Information

- **Mission Fed Mobile Banking**
  https://www.MissionFed.com/Mobile-Banking
- **Safe Mobile Banking: Our Latest Tips for Protecting Yourself**
  http://www.fdic.gov/consumers/consumer/news/cnwin1213/mobilebanking.html
- **Five Tips for Safe Mobile Banking**
  http://www.saveandinvest.org/ProtectYourMoney/P197400
- **Privacy in the Age of the Smartphone**
  https://www.privacyrights.org/fs/fs2b-cellprivacy.htm
- **Keep your phone safe**
  http://www.consumerreports.org/cro/magazine/2013/06/keep-your-phone-safe/index.htm
- **10 Rules for Creating a Hacker-Resistant Password**
  https://www.privacyrights.org/ar/alertstrongpasswords.htm

Rev. 11/13