Mobile Device Security

CUMIS Risk Solutions Group

CUMIS

Introduction

Mobile technology is an essential part of credit union business, with more and more members accessing credit union services primarily on smartphones and tablets. These devices are now as powerful as traditional computers and need even more protection than 'desktop' equipment because of their mobility.

Credit unions should be continuously educating their members on how to keep their mobile devices secure. The purpose of this resource is to provide information to credit union staff, so they can educate members on how to protect their mobile devices.

According to Stat Counter, Android and iOS have about 99% of the market share in Canada, so this resource will focus on those operating systems as opposed to other operating systems currently available.

Best Practices

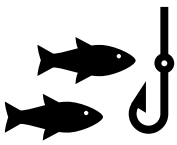
Enable password protection

A suitably complex password (six-digits) will protect your phone from the average criminal if lost/stolen. For convenience, most devices now also offer biometric security (i.e. fingerprint or face ID) for a combination of security and convenience. Arrange settings so your phone is automatically locked after an inactive period.

Do not connect to public Wi-Fi hotspots

It is difficult to verify who controls a public Wi-Fi network or prove that it belongs to who you think it does. Someone else could access your private login details while you are connected. Never login to online/mobile banking while connected to public Wi-Fi. Instead, use your mobile data network, which has built in security.

SMS Phishing (or SMShing)

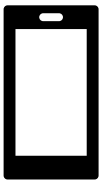


Phishing attacks account for more than 80% of reported security incidents. Never download attachments or click on text-message links that come from unrecognizable people or phone numbers. Never disclose any personal information (account numbers, passwords, social insurance number or birth date) via any form of electronic messaging.

Best Practices

Ensure your device can be remotely accessed

Most smartphones allow users to remotely track the location of a device, lock the device, erase the data and retrieve a back up if it is lost or stolen. If you lose your device or change your number, remove the old number from your mobile banking profile and contact your credit union ASAP.

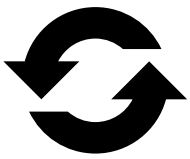


Use discretion when downloading apps

Only download apps from the App store or Google Play. Even the most innocent-looking app can contain software designed to steal personal data, make fraudulent charges or even hijack your phone. Be sure to manage the apps your children can download on your device.

Keep your device up to date

Software updates include security patches to keep devices protected. Devices should be set to automatically update. Strongly consider replacing devices when they reach the end of their software supported life.



CUMIS

Best Practices

Keep your apps up to date

Just like the operating system on your device, all the applications that you have installed should also be updated regularly. These app updates will patch any security holes that have been discovered.

Turn off Bluetooth

Do not turn on Bluetooth in public/crowded spaces and do not connect to unknown sources or accept files from these devices. Mobile viruses can be spread through Bluetooth connectivity.

Online Shopping

Avoid making purchases and banking transactions— or any communication that conveys a password, account number or credit card number— unless you are certain that you are on a secure site/connection (i.e. https://)