Safeguarding Your Information

In today's high tech world, we are able to do more things electronically, whether it is to send a letter via email, pay bills or shop online. With this increase in speed and convenience also comes increased risk. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. At La Capitol Federal Credit Union, the security of our member's information is a priority. We are strongly committed to the safety and confidentiality of your records. One of the best ways to avoid fraud is to become an educated consumer; we would like to help you in this endeavor. Please take a moment to read this important information on how to keep yourself safe when conducting business online.

How to Keep Yourself Safe in Cyberspace

An important part of online safety is knowledge. The more you know, the safer you'll be. Here are some great tips on how to stay safe in cyberspace:

1. Set good passwords. A good password is a combination of upper and lowercase letters and numbers, and one that is not easily guessed. Change your password frequently. Don't write it down or share it with others.

2. Don't reveal personal information via email. Emails and text messages can be masked to look like they are coming from a trusted sender when they are actually from someone else. Play it safe. Do not email or text your personal information such as account numbers, social security numbers, passwords, etc.

3. Don't download that file! Opening files attached to emails can be dangerous, especially when they are from someone you don't know as they can allow harmful malware or viruses to be downloaded onto your computer. Make sure you have a good antivirus program on your computer that is up to date.

4. Links aren't always what they seem. Never log in from a link that is embedded in an email message. Criminals can use fake email addresses and make fake web pages that mimic the page you would expect. To avoid falling into their trap, type in the URL address directly and then log in.

5. Websites aren't always what they seem. Be aware that if you navigate to a Website from a link you don't type, you may end up at a site that looks like the correct one when in fact it's not. Take time to verify that the web page you're visiting matches exactly with the URL that you'd expect.

6. Logoff from sites when you are done. When you are ready to leave a site you have logged into, logoff rather than just closing the page.

7. Monitor account activity. Monitor your account activity regularly — either online or by reviewing your monthly statements, and report any unauthorized transactions right away.

8. Assess your risk. We recommend periodically assessing your online banking risk and putting into place increased security controls where weaknesses are found — particularly for members with business accounts. Some things to consider when assessing your online banking risk are:

- Who has access to your online business accounts?
- How and where are user names and passwords stored?
- How strong are your passwords, and how often are they changed? Are they changed before or immediately after terminating an employee who had access to them?
- Do you have dual controls or other checks and balances with respect to access to online banking transactions?

9. Don't download that app! Downloading applications of unknown or suspect origin could compromise your mobile device login credentials. Make sure your download our mobile app from the Apple Store or Google Play.

10. Don't use a jailbroken phone! This means you trust a stranger with your device!

Safeguarding Your Information

- With jailbreaking your phone, it disables the "sandboxing" feature of iOS, a key part of the operating system's security architecture.
- Sandboxing makes sure third-party apps access only certain pieces of user data and certain parts of the iPhone's operating system. On a non-jailbroken iPhone, there's little chance malicious code can damage your system. No app can flip through an address book, photos or location data without telling the user about it. Disabling sandboxing, however, lets apps access all user data without having to ask for it!
- If you can't validate the app, or don't trust who wrote it, don't download it! Malicious apps are often designed to look exactly like popular, harmless ones. Don't trust free versions of games that normally cost a few dollars.
- There's also the possibility that a badly written app or firmware update, let alone a malicious one, could lock-up the phone. Unlike a desktop computer, there's really no way to factory restore the device when that happens.

What to Expect From La Capitol Federal Credit Union

- La Capitol Federal Credit Union will NEVER call, email, or otherwise contact you and ask for your username, password, or other online banking credentials.
- La Capitol Federal Credit Union will NEVER contact you and ask for your credit or debit card number, PIN, or 3-digit security code. Please see below for more information about how our card provider, PSCU, approaches customer service calls.

Credit Cards & Debit Cards

Our card provider, PSCU, may identify themself as Card Member Services. They will never ask for your card number, expiration date or CVC (security) code.

They will:

- Verify your street address.
- Verify the last four digits of your Social Security Number.
- Verify your date of birth.

They may:

- Ask for the last four digits of your card number.
- Ask you to verify the amount of your last transaction or payment.
- If you are uncomfortable with the call, please hang up and call them back on the number located on the back of your card.

Rights and Responsibilities

With respect to online banking and electronic fund transfers, the Federal government has put in place rights and responsibilities for both you and the credit union. These rights and responsibilities are described in the Account Information Disclosures you received when you opened your account with La Capitol Federal Credit Union. It is your responsibility for maintaining appropriate security for computers and mobile devices accessing internet banking including, but not limited to, virus and spyware protection, operating system and application updates, and firewalled internet connections. If you notice suspicious account activity or experience security-related events, please contact the credit union immediately at 1-800-522-2748.