CBI Federal Credit Union

Safeguarding Your Information

In today's high-tech world, we are able to do things more quickly and conveniently electronically whether it is to send a letter via email, pay bills or even go shopping online. With this increase in speed and convenience comes an increase in risk. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public**. At CBI Federal Credit Union**, the security of member 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 and 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 lower-case 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 send your personal information such as account numbers, social security numbers, passwords etc. via email or texting.

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. Log off from sites when you are done. When you are ready to leave a site, you have logged in to, 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 put into place increased security controls where weaknesses are found, particularly for members with business accounts. Some items 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?

What to Expect from CBI Federal Credit Union

- CBI FCU will **NEVER** call, email or otherwise contact you and ask for your user name, password or other online banking credentials.
- CBI FCU will **NEVER** contact you and ask for your credit or debit card number, PIN or 3-digit security code.
- CBI FCU will put information on our website to share with you regarding current fraudulent situations that we are aware of.

Credit Cards and Debit Cards

Our credit card provider and debit card provider may identify themselves as Card Member Services. They may contact you to identify suspicious activity that they have detected on your card. They do utilize automated calls to verify the activity. Depending on the responses given by you, they may transfer the automated call to a LIVE OPERATOR. **They will never ask for your card expiration date or CVC (security) code on the back of the card.**

They will:

- Verify your street address or phone number
- Verify the last four digits of your Social Security Number

They may:

- Ask for your full name
- Ask for birth date
- Ask to verify the amount of your last transaction, the merchant name, or payment amount.

If you are uncomfortable with the call, please hang up and call the credit union at (800) 699-5417. Then for specific types of fraud after hours please use the following:

Credit Card: Call (800) 325-3678

Debit Card: Call (973) 682-2652 for outside the United States (800) 472-3272.

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 CBI FCU. Ultimately, if you notice suspicious account activity or experience security-related events, including comprise of your PIN, or a debit to your account that you don't recognize, please contact the credit union immediately at 1-800-699-5417. In order to protect you, we may change your account number and block your account and reissue a new PIN: