Annual Privacy Notice

Privacy Notice– *Federal law requires us to tell you how we collect, share, and protect your personal information. Our privacy policy has not changed and you may review our policy and practices with respect to your personal information at www.evergreendirect.org or we will mail you a free copy upon request if you call us toll-free at 1-800-327-4286.*

evergreenDIRECT Credit Union Member Education
Internet Security
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 also comes increased risk. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. At evergreenDIRECT Credit Union, the security of customer 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 strong passwords. A strong 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. Web sites aren't always what they seem. Be aware that if you navigate to a Web site 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 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. Use secured computers. When performing financial transactions, using secured computers whenever possible, such as your home or work computer will be safer than using publicly available computers.

9. 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 evergreenDIRECT

evergreenDIRECT will NEVER call, email or otherwise contact you and ask for your user name, password or other online banking credentials.

evergreenDIRECT 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 providers approach customer service calls.

Debit and Credit Cards

Our card providers will identify themselves 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.

They may:

- Ask for the last four digits of your card number.
- Ask to verify the amount of your last transaction or payment.

At any time if you are uncomfortable with the call, please hang up and call the credit union.

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 evergreenDIRECT. You can also find them online under the disclosures link at www.evergreenDIRECT.org. Ultimately, if you notice suspicious account activity or experience security-related events, please contact the credit union immediately at 1-800-327-4286.

evergreenDIRECT Credit Union
P.O. Box 408 Olympia, WA 98507-0408
360-943-7676/800-327-4286
www.evergreenDIRECT.org