member

Internet
Transactions
Protection

Internet

Transactions

Are you

Secure?

We're working to keep your Internet transactions secure.

To protect your financial and personal information while online, your credit union's Internet transaction application uses a variety of security measures to maintain your privacy and security. For example, while you are performing online financial transactions, your data is encrypted to ensure that your information cannot be read or modified while it is being downloaded to your computer.

You are the key to your financial transactions security.

Even with your credit union's online security measures in place, it's important to remember that YOU need to take steps to keep your computer secure. There are ways to control access to the valuable information that you maintain on your computer or input to access a secure site.

Don’t be the weak link.

Internet fraud is on the rise. Not only your home computer but any computer can become infected with “spyware” or viruses that attempt to collect your internet transaction and login information prior to entering the secure environment that your credit union provides. And with today’s powerful online transaction systems, someone pretending to be you may be able to:

- Transfer funds to another location
- Apply for loans that you are not aware of
- Set up automatic credit card payments for cards that are not yours.

Whether you use WINDOWS, LINUX or MACINTOSH operating platforms, you need to be concerned about computer security.

Invest in peace of mind.

Reputable retailers sell a variety of software and hardware solutions to make your computer more secure. Here are a few recommendations to enhance the security of any computer that is attached to the internet:

Firewall

Considered the first line of defense for protecting private information, a firewall helps prevent unauthorized access to or from your home or office network. Although some computers come with a standard operating system firewall, it should not be considered sufficient to keep out intruders. An additional firewall, that will detect new forms of attacks or attempted intrusions, should be installed and upgraded regularly. Firewalls can be implemented in both hardware and software, or a combination of both.

Anti-Virus Program

Computer viruses are pieces of destructive computer codes that are easily spread from computer to computer without the users' knowledge. In some cases they are used to collect and transmit personal information to a third party such as passwords and online transaction location information. In others, they are intended to harm the computer they infect and make it unusable. Virus protection programs or anti-virus software is not a must for computer users, because the number and destructiveness of new computer viruses is increasing exponentially.

To ensure you are protected from new viruses, update your anti-virus software at least once a week and run it to detect if your computer has become infected with a virus. With a good quality program, updates are available online through the software provider's web site and in many cases can be automatically update as new releases become available.

Anti-Spyware Programs

Spyware will not harm your computer as a virus might. It is programming that is picked up through accessing internet sites and downloaded on to your computer without your knowledge or consent. Spyware secretly gathers information about you and relays it to advertisers or others who want to know more about you and your online habits. Criminals are now using this technology to install key loggers or screen capture programs that allow them to collect personal information and passwords to secure sites and the sites URL locations which is a breach of your personal privacy. Because spyware is becoming increasingly powerful and difficult to remove specialized anti-spyware programs should now be considered as important as anti-virus technology. To ensure that you are protected from new spyware programs update your spyware detection software at least once a week and run it

It against your computer at the end of each online session to detect new attachments. God quality products have an automatic or requested update feature where updates are available online through the software providers website. It is preferable to have more than one version of spyware detection available to run on a computer as no one version can detect all attachments.

Other Security Suggestions

Here are some additional things you can do to enhance the security of your internet financial transactions.

- Use a multi-digit password — one that is difficult to guess.
- Change your password regularly.
- Do not use software that 'memorizes' passwords unless the product keeps them in an encrypted form and displays them only in a masked form on the screen.
- Keep your passwords and Personal Identification Numbers (PIN) safe and never share them.
- Do not use the same password for different secure sites.

- Observe the look of your online transaction site. If it changes check the URL carefully to ensure that you have not been hijacked to a bogus site.
- Never leave your computer while it is logged on to a password protected site than can perform online transactions.
- Follow the instructions provided to properly exit online secure sites and then clear your cache.
- Never send confidential or personal information through an e-mail, even if you think the e-mail is going to an organization or person you trust.
- Do not conduct online financial transactions where you can be observed or at Internet café's or libraries where a previous user may have accessed a site that downloaded a key logger.
- Always confirm that you are accessing online transactions through the correct credit union web site address.
- Disable file sharing in WINDOWS products.

- Do not follow links provided in an e-mail form, that appears to be from your credit union or any other financial institution, that request you to provide personal information. If you are unsure, call your financial institution through a known number, other than one that may appear in the content of the e-mail, to verify the message was sent from them.

Talk to your Credit Union

If you have any concerns about the safety and privacy of your personal information, or if you have noticed unusual activity in your accounts, please contact your credit union as soon as possible. **They will be happy to answer your questions.**

Note: information which includes all facts, data and other information, collectively the "information" within this pamphlet is of a general nature, Is intended only for informational purposes, is subject to change without notice and is not intended to be relied on by members as advise on any particular manner.

Churchbridge Credit Union

Bringing Communities Together

www.churchbridgecu.ca

1-877-890-2797