Privacy and Security: Staying Safe on the Internet

Internet Security

The Internet has changed the way financial institutions do business. Internet banking provides convenient access to information and the ability to perform transactions from home, work or other locations. It is important to be aware that when you communicate via the Internet, other people and software can also communicate with your computer. An inadequately protected computer can be accessed by an unknown party or a virus in a very short period of time.

What we are doing to protect your security

We take many precautions to protect the online banking portion of our environment and ensure your information is safe. Our online banking services offer you the best security currently available in a commercial environment so that your personal and financial information is protected while in transit between your computer and our server. This is done through the use of industry standard security techniques such as encryption. Encryption ensures that information cannot be read in transit or changed by scrambling the data using a complex mathematical formula. Some browsers can create a more secure channel than others, owing to the 'strength' of their encryption.

We use only the strongest channel currently available - referred to as 128-bit SSL (Secure Socket Layer). If you have a browser that only supports 'weaker' encryption such as 40-bit or 56-bit SSL, you will need to upgrade your browser before using our Internet banking site. The longer and more complex the 'key' is, the stronger the encryption. The 40 and 128 refer to the length of the key. Since 128 is longer than 40, it is more secure. According to Netscape, 128-bit encryption is trillions of times stronger than 40-bit encryption.

We also ensure that only individuals who provide an authentic Personal Access Code can access your account information. To help you protect your information, your online banking session will end automatically if there has been no activity for 15 minutes. Access to our databases is strictly managed and systems are in place to help ensure security is not breached, including the physical security of our computer hardware and communications.

For more information on the specific policies and practices that we use to safeguard your personal and financial information, Please see our Privacy Policy.

What you need to do to protect your computer and PAC

Protecting your Personal Access Code (PAC)

Just as you play a vital role in ensuring the security of your home and your possessions, you too share in the responsibility for ensuring that your personal information is adequately protected. While we take strong measures to protect the security and privacy of your information, there are important steps that you should take to help protect your information when using the internet.

In order for us to ensure that only you are accessing your accounts, we need a unique way of knowing that it's you. Just as the key to your home protects unwanted entry, the online banking 'key' - your Personal Access Code (PAC) - ensures that only you can access your accounts.

It is your responsibility to ensure that your 'key' to our Internet banking site is protected. Please observe the following security practices:

- Select a PAC that is easy for you to remember but difficult for others to guess.
- Do not select a part of your PIN or other password as your PAC.
- Keep your PAC confidential and do not share it with anyone.
- Do not write down your PAC or store it in a file in your computer.
- Never disclose your PAC in a voice mail or e-mail, or over the phone.
- Ensure that no one observes you typing your PAC.
- Change your PAC frequently (every 90-120 days).

Protecting your computer

We have provided a secure channel for our members to communicate with us. Once the information has reached your computer, however, it's up to you to protect it. To protect your information, you should:

- **Never leave your computer unattended** while using our online banking services.
- **Always exit our Internet banking site using the "logout" button** and close your browser if you step away from your computer. Your browser may retain information you entered in the login screen and elsewhere until you exit the browser.
- **Prevent the browser from caching** (storing) the pages that you view by taking advantage of the Enhanced Security feature. In order to take advantage of this feature, you must use the logout button when you exit our Internet banking site. Please note that the Enhanced Security Feature does not prevent the caching of .pdf files. Therefore, it is strongly recommended that you manually delete cached files (as further described below) from your computer after each use of our Internet banking site.
- **Secure or erase files** stored on your computer by your browser so others cannot read them. Most browsers store information in non-protected (unencrypted) files in the browser's cache to improve performance. These files remain there until erased. They can be erased using standard computer utilities or by using your browser feature to "empty" the cache.
- **Disable automatic password-save features** in the browser and software you use to access the Internet.
- **Do not use Memorize Account feature** on publicly available computers. Our Internet banking site provides you the option of having your log-in ID automatically filled in. You should not select this option on publicly available computers.
- **Install and use an anti-virus program.** Ensure your anti-virus software is enabled and configured to run daily updates and regular virus scans.
- **Install and use a personal firewall** on your computer to ensure others cannot access your computer through the Internet.

- **Install new security patches** as soon as your operating system and Internet browser manufacturers make them available.
- **Install an anti-spyware program**. Ensure your anti-spyware is enabled and configured to run daily updates and regular spam scans.

Protecting your information when using a public computer

The practice of accessing your account information through publicly accessible computers and public wireless networks is strongly discouraged. The use of computers at locations such as Internet cafes, public libraries, hotel lobbies and public wireless networks such as "hotspots" to name a few examples, greatly increases the risk of possible unauthorized access to your accounts. Use of these access points are to be avoided and if it is determined to be the compromise point, this would have a negative impact on your ability to be compensated for your losses.

You should be extra vigilant when using publicly available computers. Even if you adopt the tips above to protect your information, you need to bear in mind that even benign programs, like popular desktop search programs, can pose a security risk. Certain programs, such as Google Desktop, cache items that you have viewed so you - or potentially, an unwelcome third party - can easily search and find those pages again later.

If you come across a program like this when you are using a public computer, the Enhanced Security feature will not stop these types of programs from caching the pages you view. You can adjust the search program preferences so it does not store secure pages you wish to view. If you forgot to adjust the preferences before banking online, you can remove the stored items via the Google Desktop results page by clicking on the Remove items link.

To learn more about browser security, please visit the Netscape and Microsoft web sites (as applicable). To ensure a safe and secure Internet session, only visit reputable sites. If you visit any questionable web site before accessing our Internet banking site, we recommend you close your browser and restart it before proceeding to our Internet banking site.

Fraud: Recognize it. Report it. Stop it.

Electronic identity theft can occur when you respond to a fraudulent email that asks for your personal banking information. Armed with this information, a person may be able to access your accounts or establish credit, pay for items or borrow money using your name. You can help protect yourself from electronic identity theft by following some simple precautions.

Safety precautions for online banking

- The easiest way to tell if an email is fraudulent is to bear in mind that we will **never** ask you for your personal passwords, personal information numbers or login information in an email.
- When banking online, check the address of any pages that ask you to enter personal account information. In the toolbar at the top of the page, any legitimate Internet banking web site will begin with 'https' to indicate that the page is secure.

- Look to the padlock on your screen. If the page is legitimate, by clicking on the padlock, you can view the security certificate details for the site. A fraudulent site will not have these details.
- Type in our web address yourself to ensure you are transacting with our server.
- Check your account and credit card statements regularly and carefully to ensure that all transactions are legitimate.

Notify Kerrobert Credit Union Limited immediately upon discovering or suspecting that unauthorized activity has occurred or that your PAC or PIN may have been compromised.