Electronic Banking Safety Tips

**ATM Card Safety**

**Treat your card like cash. Always store your card in a safe place.**

**Keep your PIN a secret.** ATM transactions and PIN debit purchases require the use of a secret code known as a personal identification number or PIN. Memorize your PIN, and never write it on your card or store it with your card. Never let someone else enter your PIN for you.

**Do not disclose information about your card over the telephone.** No company or individual needs to know your PIN…not even your financial institution. If you perform transactions over the telephone using your ATM or debit card, never disclose your PIN.

**Never disclose information about your card in response to an unsolicited e-mail or request.** E-mail is a common channel for fraud perpetration. Never provide your debit or credit card number, PIN or any other non-public personal information to any entity in response to an unsolicited e-mail or request. Your financial institution will never ask you for your PIN.

**Make certain your Internet shopping sites are secure.** Look for secure transaction symbols when shopping online to ensure your account information is protected. Always log off from any site after you make a purchase. If you can’t log off, shut down your browser to prevent unauthorized access to your account information.

**Protect your card’s magnetic stripe.** Do not expose your card’s magnetic stripe to magnetic objects. Magnetic objects can damage your card.

**Report a lost or stolen card at once.** Immediately call your financial institution if your card is lost or stolen to reduce the chance that it will be used improperly. Immediate notice of lost or stolen cards will also limit your potential liability for unauthorized transactions.

**Review your account statements for unauthorized transactions.** Review all account statements from your financial institution promptly, and report any errors (including transactions you believe may be unauthorized) as soon as possible. Prompt notification will limit your potential liability for unauthorized transactions.

**ATM Safety**

**Always observe the ATM surroundings before conducting a transaction.** If anyone or anything appears to be suspicious, leave the area at once. If you drive to an ATM, park as close as possible to the terminal. Observe the entire area form the safety of your car before getting out.

**If an ATM is obstructed from your view or poorly lit, go to another ATM.**If possible, report the problem to the ATM operator or your own financial institution.

**It is a good idea to take another person with you when using an ATM, especially at night.**

**Minimize the time spent at the ATM when conducting a transaction.** Have your card out and ready to use. Do not allow a stranger to assist you in making a transaction, even if you have trouble or your card gets stuck. When your transaction is complete, put your card, money and receipt away and immediately leave the area. Never count your money while at the ATM.

**Block the view of others when using the ATM.** Stand between the ATM and anyone waiting to use the terminal. Shield the keypad as necessary when entering your PIN and transaction amount.

**If you see anyone or anything suspicious, cancel your transaction and leave the area at once.** If anyone follows you, go immediately to a crowded, well-lit area and call the police.

**Look for possible fraudulent devices attached to the ATM.** If the ATM appears to have any attachments or alterations to the card slot or keypad, do not use the ATM. If possible, report the problem to the ATM operator or your own financial institution.

**PIN Safety**

* Never allow the cashier, sales clerk or any other person to enter your PIN for you, even if they are assisting you with the transaction. Always keep your PIN a secret.
* Block the view of others when using a PIN debit terminal.
* Be certain the transaction is complete and review your receipt before leaving.
* Change your password regularly and use a different password than you use for other websites. Make it difficult for others to guess your password by using a combination of letters and numbers in your password. If you think someone knows your password, change it right away.

**Internet Banking Safety**

* **Secure Online Banking and Investing.** We offer you secure access to your banking and investment accounts
* **Session timeout.** To protect you further, your online session will end after a period of inactivity. If you wish to continue accessing your online banking or investment accounts, you will have to sign on again. You should always sign off when you are done and, if using a computer that isn't your own, you should clear your browser's cache and close the browser window.
* **Clear Your Browser's Cache.** If you use a public or shared computer to access CIBC Online Banking, it is vital that you sign off when you are finished. Once you have signed off, you should enhance your security by clearing the browser's cache. The cache maintains a copy of web pages that have been viewed recently.
* **General security** over your personal computer such as virus protection and physical access controls should be used and updated regularly. Contact your hardware and software suppliers, or Internet service provider, to ensure you have the latest in security updates.

**Password Safety**

The prime objective of Authentication mechanism is to provide access to information to only legitimate and authorised users and deny access to unauthorised persons. This can be ensured in many ways. But the most common way of ensuring accessibility to the authorised users is through password mechanism. Password is the front line protection for user accounts. It is based on possessing a secret word by the legitimate user which is known to the computer as well. Access to the sensitive information is possible only to the user who knows the password.

• Although the password is the most inexpensive way of ensuring protection to sensitive information, it has many drawbacks. A poorly chosen password may result in compromise of the confidential information or even the Bank's entire network. The confidential information is safe and secure only on the strength of the password. Therefore, it is our responsibility to keep a strong password to protect our Bank's sensitive and confidential information from falling in to unauthorised hands. Following are some of the important tips for selecting and securing your password.

• Keep the minimum length of the password as 8 characters as far as possible. It may take some time to remember and even type. But it is worth the trouble because it will be very difficult to guess or break.

• Do not use birthdays, names of the family members, pet names etc.

• Do not use the word "password" for password and or any other dictionary word.

• Use a mixture of numbers, special characters and symbols and different cases (combination of capital and small letters)

• Keep changing your password at periodic intervals.

• Never share your password with any one - not even with your superiors, friends etc. In the extreme circumstances, if it has to be shared, then change it immediately.

• Never write your password anywhere on your desk/ board

• Never use the same password for all your accounts.

• Here is a tip to select a complex password, but easy to remember.

• Select any pharse which you know or means something to you., It may be from a song or a nursery rhyme eg. "This may be one way to remember", the password can be "TMb1w2r!" or some other variation of this.

• Only you can protect your bank's information and prevent any security incident from happening. Therefore, each one of you should do your part to keep our Bank's data secure and safe. Take precautions to protect your password and the Bank's sensitive information and responsibility for the usage of your password.