Personal Security INFO & Precautions:

IDENTITY THEFT:

Identity theft is on the rise. Unlike other types of fraud, identity theft begins whenever a criminal gains access to a person's means of identification, regardless of whether the victim is aware of that access.

Here are some ways you can protect yourself from identity theft...

- Before you reveal any personal information, find out how it will be used and if it will be shared.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time.
- Guard your mail. Deposit outgoing mail in postal boxes or at a post office. Promptly remove mail from your mailbox after delivery. Ensure mail is forwarded or re-routed if you move or change your mailing address.
- Put passwords on your credit card, bank and phone accounts. Avoid using easily available information like your birth date, the last four digits of your SIN or your phone number.
- Minimize the identification and number of cards you carry.
- Do not give out personal information on the phone, through mail or over the Internet unless you have initiated the contact or know who you're dealing with.
- Keep items with personal information in a safe place. An identity thief will pick through your garbage or recycling bins. Be sure to tear or shred receipts, copies of credit applications, insurance forms, physician statements and credit offers you get in the mail.
- Give your Social Insurance Number (SIN) only when absolutely necessary. Ask to use other types of identification when possible.
- Don't carry your SIN card; leave it in a secure place.

Source: Canadian banking association

E-MAIL SCAMS:

What is phishing?

"Phishing" or "spoofing", is a technique where e-mail is sent by dishonest individuals to try to obtain personal information about people. The Canadian Bankers Association defines "phishing" as follows:

Phishing/spoofing – Using an e-mail claiming to be a legitimate enterprise in an attempt to get consumers to divulge personal information. The email usually directs users to visit a Web site where they are asked to enter personal information such as passwords and account numbers.

How to recognize e-mail scams...

In recent months, users of online commercial sites, payment organization sites and those of certain financial institutions have been the target of this practice. The messages contained in scam e-mail look like they originate from recognized sources. Web sites that use phishing are generally very skilled at imitating legitimate sites whose logos users readily recognize. You should beware of e-mails that direct you to sites and ask you to supply your personal, banking or credit information, especially if they insist that it is urgent that you do so immediately.

To help you better identify these scams, here are a few examples of typical messages used in phishing e-mails.

...Owing to the large number of cases of identity theft, you must confirm your banking information. If you do not, access to your account will be suspended.

...We believe that someone has attempted to illegally access your bank account. Please complete this form to enhance the security of your account.

...Our technical teams are currently updating our software. Please confirm your personal data...

...If your current information is not updated, your purchasing rights will be restricted in five days.

Would you like more information on this topic? Refer to the E-mail Fraud section on the Canadian Bankers' Association website >>>
http://www.cba.ca/en/ViewDocument.asp?fl=3&sl=308&tl=312&docid=570

Have you received a scam e-mail?

If you think you've received a phishing e-mail and that the sender is claiming to be from your Bank, Credit Card Company or Credit Union … do not click on a hyperlink or copy and paste it on your browser screen and do not give the information requested.

Keep the e-mail?

Contact your Bank, Credit Card Company or Credit Union and ask them if they want the information. If not just delete it.

SPYWARE:

Definition...

Spyware is a type of software that installs itself on your computer, usually without your knowledge. It collects information on you by tracking your Internet surfing habits, identifying your preferences and, in some cases, even recording your keystrokes. This information is then sent to a third party for advertising purposes or other potentially malicious activities.

This practice is not illegal because the software manufacturers usually do not have criminal motives. Nevertheless, it is a threat to individual privacy and could compromise the confidentiality of information.

Spyware can install itself in many different ways and is difficult to detect, as it usually does not appear in the list of programs installed on your computer. You can "catch" spyware by downloading free software containing it, visiting certain websites, sharing files online (peer-to-peer) or after being infected by a virus. Simply by clicking on "I accept" or "OK," you could provide a way for spyware to sneak into your system.

Signs of Spyware Infection...

Spyware is likely present in your system if:

- Your computer is performing more slowly than usual
- You are automatically redirected to a page you did not type into your browser
- You are constantly bombarded with pop-up advertisements
- New tools or icons suddenly appear in your Internet browser or the settings for your homepage change
- Your computer crashes or freezes more frequently

Treatment

Since spyware programs are practically invisible and can attack at any time, we recommend that you install anti-spyware software on your computer and enable the automatic update and clean-up features to ensure that your workstation remains spyware-free at all times.

ANTI-SPYWARE PROGRAMS:

We strongly recommend* that you install a recognized anti-spyware program on your computer. It is also very important that you enable the automatic update feature so the program is automatically updated through the manufacturer's website. An outdated version will not be able to recognize recent spyware.

Visit the following sites for more information about anti-spyware programs :

Ad-Aware & Spybot Search & Destroy

http://www.docsdownloads.com or http://www.1securepc.com
http://www.1securepc.com/

Online Personal Banking Security:

1 - Security

1.1 Does your Bank follow a specific code of procedure for the protection of personal information?

In cooperation with other financial institutions and the Canadian Bankers Association, all Banks have established a code of procedure for the protection of personal information on individual users. This code of procedure, which all Banking employees undertake to follow, ensures that the information about you in your personal file is used only to:

- Properly manage your products and services
- Inform you about other products and services that may be of interest to you
- Meet your expectations more effectively
- Only employees who need to access your personal file in the course of their work are allowed to consult it.

1.2 Is there a special department at each Bank that looks after online security?

Yes, all Banks have an Information Security Group that focuses on matters related to security and confidentiality. Its mission is to:

Identify and manage information security risks, while taking into account their impact on Bank business

Establish information security policies, strategies and standards

Assist and advise owners of information in evaluating risks and required levels of protection, and in choosing appropriate security measures

Make all Bank employees aware of the importance of information security and of their involvement.

1.3 When I do my banking via Internet Banking Solutions, how do you ensure the confidentiality of my transactions?

A number of precautions have usually been taken to maintain the confidentiality of the information you transmit when you perform your transactions via Internet Banking Solutions. In fact, with the measures already implemented by the Bank and the preventive measures we recommend to you, your banking transactions are as secure when you do them online as they would be at the counter in your branch.

1.4 What measures have been taken to ensure maximum security and confidentiality?

To ensure maximum security, a number of measures must be taken by both the client and the Bank.

For the client:

- You must choose a password known only to you
- Regularly change your password. We strongly recommend that you change it at least once a month
- If possible, use a personal firewall
- End the session as soon as you are finished

For the Banks/Credit Unions:

Banks apply the most rigorous security standards as evidenced by our use of 128-bit encryption (currently the highest level of security commercially available in North America) to protect the confidentiality of your transactions.

They also ensure your protection by automatically cutting off your session whenever it is inactive for an extended period (6 minutes).

1.5 What is a Banking “Peace of Mind Guarantee”?

The “Peace of Mind Guarantee” is offered to users of Internet Banking Solutions at most Banks. This guarantee ensures that you are reimbursed for any losses caused by fraud while banking on the website, even though you took appropriate measures to protect your access number and password. In this case, you must advise you Bank immediately by calling their anti-fraud hotline and cooperate fully with any investigation concerning the fraud.

1.6 What is encryption and how does it work?

Encryption is a data encoding process that ensures the security of the transmitted data. To be able to read an encrypted file, the client must have access to a secret key protected by a password to decode the information. In other words, regular text is converted into scrambled code (illegible text) during transmission, and is decoded into legible text at the reception point. The two most widely used encryption levels are 40-bit and 128-bit. Given the importance of your financial information, we have opted for 128-bit encryption, one of the most secure systems currently available on the North American market.

1.7 What is the difference between 128-bit and 40-bit encryption?

128-bit encryption provides significantly more cryptographic protection than 40-bit encryption. It has become increasingly necessary to use longer keys to counter the growing potential for computer-related criminal activity, as demonstrated by a recent study by several leading cryptographers.

“128-“ and “40-“ bit encryption refer to the size (length) of the key used to encrypt the message. Roughly speaking, 128-bit encryption is 309,485,009,821,345,068,724,781,056 times stronger than 40-bit encryption. Even taking into account Moore’s Law, which states that computing power doubles about every 18 months, 128-bit encryption represents a very strong method of encryption for the foreseeable future.

1.8 Why is it important to erase my browser’s cache memory?

To protect the confidentiality of your financial information and improve the performance of your Web browser, we recommend that you erase your cache memory after each Internet Banking Solutions session. This is particularly important if the computer you use for your banking transactions is shared with other users.

Follow these instructions to clear your browser’s cache:

NETSCAPE 4.x & Firefox:

From the “Edit” menu, select “Preferences”.
Select the “Advanced” option.
Select the “Cache” option.

To remove all the files currently in your memory cache, click on “Clear Memory Cache”.
Click on “OK”.
To remove all the files currently in your disk cache, click on “Clear Disk Cache”.
Click on “OK”.
To exit, click on “OK”.

MICROSOFT INTERNET EXLORER 5.x:

From the “Tools” menu, select “Internet Options”.
Click on the “General” tab.
Click on the “Delete Files” button in the “Temporary Internet Files” box.
Click on “OK”.
Click on the “Clear History” button in the “History” box.
Click on “OK”.
To exit, click on “OK”.

1.9 What can I do to secure my transactions?

Simply take the following precautions:

Never reveal your password, not even to a family member or anyone claiming to be a Bank employee.

- Never leave personal information in plain view.
- Never leave your computer when carrying out a transaction via Internet Banking.
- Always sign out from your session by clicking on “Quit” before leaving your computer.
- Always erase your browser’s cache memory.
- Never send confidential information by e-mail, unless it is encrypted.
- Avoid using a password that is easy to guess.
- Change your password on a regular basis and do not use the same password more than twice during a year.
- Never use the same password for several software applications.
- Never use a password that contains part of your banking access codes (i.e. Client Card, credit card, PIN).
- Consider installing anti-virus software and a personal firewall on your computer.
- When your Client card is lost or stolen, please immediately reach your Bank’s call center.
- Go through your banking statement thoroughly and acknowledge us of any irregularity.
- Avoid using any software that save your password on the login page of the Internet banking Solutions.

Note: Remember that your Bank will never need to obtain your password or Personal Identification Number to provide you with support.

1.10 When I carry out a transaction using Internet Banking, how can I be sure that my session is secure?

If you use Netscape Navigator or Microsoft Internet Explorer :

A small closed lock will appear in the bottom right corner of your screen, indicating that the session is encrypted.

1.11 What is the difference between http and https?

Https guarantees that the information transmitted is secure (encrypted). Note that the encryption may be 40-bit or 128-bit.The Bank only uses 128-bit encryption in order to maximize security.

1.12 Is the transmission of information by e-mail secure?

In general, information contained in e-mail is not protected. However, e-mail attachments can be protected if they are encrypted before transmission. An “ordinary” e-mail should never contain any confidential information unless it is provided on the secure form accessible via our website.

1.13 Are the on-line forms accessible via the internet?

Yes. Most Banking forms, including the one for sending e-mails, use 128-bit encryption. The small closed lock located at the bottom of your screen confirms that the form is encrypted.

1.14 What is a cookie?

A cookie is a feature that enables a browser to store information provided by user and save it in a small text file on the hard disk. For more information, visit our Support section.

INTERNET SOFTWARE:

MICROSOFT INTERNET EXPLORER

By following the instructions below, you will be able to download a freeware version of Microsoft Internet Explorer ® with 128-bit encryption. We recommend that you print this page and keep it with you while downloading the Microsoft browser.

For users of Windows 98/XP/ME/2000/NT 4.0

To download the English version of Microsoft Internet Explorer 6.0, go here >>> http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/download.asp.

Once at the site, follow these easy steps to download the browser.

Under “Download”, click on “Go” next to “Select language”.
Under “Download”, click on “Internet Explorer 6.0 Service Pack 1”.
Choose to save the program on your disk.
In the window “Save As”, select the file “Desktop” and click on “Save”.

After the download, click twice on the new icon “ie6setup.exe” on your desktop.
Follow the steps in order to install your browser.
Note: If you have Windows 2000 as your operating system, you have to download Windows 2000 High Encryption Pack to be able to download Internet Explorer 6.0 Service Pack 1. Get it here >>>
http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp.

For Macintosh users

Microsoft ended support for Internet Explorer for Mac on December 31st, 2005, and is not providing any further security or performance updates. For more details, please visit Microsoft website.

NETSCAPE NAVIGATOR

By following the instructions below, you will be able to download a freeware version of Netscape with 128-bit encryption . We suggest that you print this page and keep it with you while navigating through the Netscape download site.

Users of Windows 98/XP/ME/2000/NT 4.0

To download Netscape Communicator 7.1, click here >>>
http://browser.netscape.com/ns8/download/archive71x.jsp.

Once at the site, follow these easy steps to download the browser:

Click on “Free Download”.
Then click on “Download Now”.
Choose to save the program on your disk.
In the window “Save As”, select the file “Desktop” and click on “Save”.
After the download, click twice on the new icon “NSSetup” on your desktop.
Follow the steps in order to install your browser.

For Macintosh users

To download Netscape Communicator 7.0, click here >>>
http://browser.netscape.com/ns8/download/archive70x.jsp.

Once at the site, follow these easy steps to download the browser:

On the webpage “Archived Products”, click on “Version 7.0”.
Choose to save the program on your disk.
In the window “Save As”, select the file “Desktop” and click on “Save”.
After the download, click twice on the new icon on your desktop.
Follow the steps in order to install your browser.
After the download is complete (Macintosh):

Use your decompression program to decompress and decode the .bin or .hqx file on your desktop. If you have installed Stuffit Expander (you can obtain a copy by visiting http://www.aladdinsys.com/), simply drag the file onto the Expander icon, and the file

will unstuff to reveal a file with the extension .smi. Double-click on this new file and follow the installation instructions.

ADOBE ACROBAT READER

Click here on Adobe Acrobat Reader >>>
http://www.adobe.com/products/acrobat/readstep.html;

Choose your language in the dialog box along with the platform used (Windows 98, 2000, Mac OS X, etc.) in the second box;

Click on Download;
Choose Save program to disk;
In the Save as window, select the Office directory and click on Save;
After downloading, double click on the new icon that appears in the office;
Follow the steps to install the software.

GLOSSARY:

Here are some definitions of Internet-related terms...

Antivirus software

Software that protects your computer against viruses. For more information about antivirus software, see the Antivirus software section.

Authentication

Process that verifies the identity of a person or any other entity, or that guarantees the source and integrity of messages that pass through a computer network such as the Internet.

Browser

Program installed on your computer that you use to surf the Web. The two main browsers on the market are Internet Explorer (Microsoft) and Netscape Navigator (Netscape), called Netscape Communicator when part of the software package in Version 4. These programs let users search for and access information online.

Cache memory

This memory is mainly characterized by very high access speed. It can be built into a hard disk or be separate, and its size is limited by its high cost. For more information on cache memory see the Cache memory section.

Cookie

A code that a server stores, often temporarily, on your hard disk to identify you on its service (commercial reuse). Both Netscape and Internet Explorer let you refuse this type of exchange.

Digital signature

Electronic seal generally produced by an algorithm associated with a public key, which guarantees both the source and integrity of the message transmitted. The signature makes it impossible for the sender to repudiate the message after it has been sent, and for the recipient or a third party to commit forgery during reception or transmission.

Encryption

Encryption is a data encoding process that ensures the security of transmitted data. To be able to read an encrypted file, the recipient must be able to access a secret key or a password to decode the information. In other words, regular text is converted into scrambled code during transmission and is decoded into regular text at the point of reception. The two most widely levels of encryption are 40-bit and 128-bit encryption. Because your financial information is important to us, we have opted for 128-bit encryption, one of the most secure systems currently available on the North American market.

Firewall

A server designed to prevent hackers from penetrating a network connected to the Internet. This server ensures the security of internal information on a local network by filtering input data and controlling output data according to a specified security criteria. For more information see the Firewall section.

Spyware

Spyware is a type of software that installs itself on your computer, usually without your knowledge. It collects information on you by tracking your Internet surfing habits, identifying your preferences and, in some cases, even recording your keystrokes. This information is then sent to a third party for advertising purposes or other potentially malicious activities.

URL (Uniform Resource Locator)

Internet address used by browsers. The URL is the standard addressing system of all documents on all computers, both locally and on the Internet.

Virus

A hostile program designed to infect your files (mainly executable files (with the extension .exe) by inserting a copy of itself in the files. Viruses can cause various types of malfunctions such as erasing the hard disk. It is important to protect your computer from viruses by installing an antivirus program and avoiding opening files attached to e-mails of unknown origin.

Wap

Protocol designed to allow limited access to the Internet from a mobile telephone or any other small portable wireless terminal.

World Wide Web

The service behind the development of the Internet for the general public. This service provides access to network resources from hypertext links, on which you click to easily connect to other servers or access specific information.

CACHE MEMORY:

To protect the confidentiality of your financial information and improve the performance of your Web browser it is important to erase the cache memory of your browser. We recommend that you erase your cache memory each time you log off the Personal Internet Banking Solutions site. This is particularly important if the computer you use for your banking transactions is shared with other users in public places such as Internet cafes or public libraries.

How to find out the version of your browser...

For PCs

Internet Explorer 5.x

Clear cache

1) Click on Tools.
2) Select Internet Options.
3) Select the General Tab.
4) Click on Delete Files.
5) Click on Clear history.
6) Click on OK.

Activate cookies

1) Click on Tools.
2) Select Internet Options.
3) Drag the cursor to Medium.
4) Click on Personnalize the level.
5) Under the section Cookies, click on the option Activate under:
   - Authorize the cookies per session.
   - Authorize the cookies stocked on your computer.
6) Click on OK to close the window.
7) Click on Apply and then OK.

Erase cookies

1) Click on Tools.
2) Select the General tab.
3) Click on Parameters.
4) Click on Visualize files.
5) Select the cookies one by one in a block and press on Del on the keyboard.

Internet Explorer 6.x

Clear cache

1) Click on Tools.
2) Select Internet Options.
3) Click on Delete Files.
4) Click on Clear history.
5) Click on Delete cookies.

Activate cookies

1) Click on Tools.
2) Select Internet Options.
3) Select the Privacy tab.
4) Use the cursor to move the slide down to the bottom until “Accept All Cookies”.
5) Click on Apply.

Erase cookies

1) Click on Tools.
2) Select Internet Options.
3) Click on Delete cookies.
4) Click on OK.

Netscape 7.X

Clear cache

1) Click on Edit.
2) Select Preferences.
3) Double-click on Advanced.
4) Click on Cache.
5) Click on Clear cache.
6) Click on OK.

Activate cookies

1) Click on Edit.
2) Select Preferences.
3) Double-click on Privacy and security.
4) Click on Cookies.
5) Tick Allow all cookies.
6) Click on OK.

Erase cookies

1) Click on Edit.
2) Select Preferences.
3) Double-click on Privacy and security.
4) Click on Cookies.

5) Click on Cookie Manager.
6) Click on Remove all cookies.
7) Click on Close, then on OK.

Netscape 6.2

Activate cookies

1) Click on Edit, then on Preferences. The window of Preferences appears.
2) Click on Cookies.
3) Click on Enable all cookies.
4) Click on OK.

Clear cache and disk cache

1) Click on Edit.
2) Select Preferences.
3) Click on Cache.
4) Click on Clear Memory Cache.
5) Click on Clear Disk Cache.
6) Click on OK.

ADDITIONAL TIPS

Here are some additional precautions you can take to maximize the security of your Internet transactions.

- Do not remain connected to the Internet unnecessarily.
- Never leave information displayed on your screen if you leave your workstation. Always block access to the data on your computer.
- Don’t download or install freeware, shareware or demo software from an unknown source or a questionable site.
- Be careful what you throw in the recycling bin. Burn or shred all documents that contain your financial information, such as statements, credit card offers, receipts and insurance forms to prevent identity theft.
- Never open an executable file received by e-mail unless it is from a known and trusted source.
- Make sure the hard disk of your workstation and the printer are not in shared mode.
- Regularly make backups of your important files.
- If you use Microsoft Word and Excel 2000 (or a more recent version), set the security level to average or higher. You will be then notified by a dialog box of any unsigned macros and will be able to disable them.

To set the security level:

Open Microsoft Word or Excel 2000;
Click on Tools in the menu bar;
Select Macro;
In the Security tab, click on the radio button to set the security level to average or high;
Click on Ok.

FIREWALLS

It is highly recommended* that you install personal firewall software on your computer. This type of software gives you additional protection to prevent unauthorized individuals from taking remote control of your station or from accessing your confidential data without your knowledge. Several sites offer information about firewalls:

http://www.firewallguide.com
http://www.pcastuces.com (French only)
http://csrc.nist.gov/publications/
http://www.docsdownloads.com (free firewall downloads)
http://www.1securepc.com (free & shareware firewall downloads)

UPDATING YOUR COMPUTER

Updates from software manufacturers should be applied regularly, especially when a vulnerability is publicized in the media. We strongly recommend* that you install the security patches for Windows, Internet Explorer and Microsoft Office. For information, go to:

http://www.microsoft.com/downloads

CHOOSE YOUR PASSWORD CAREFULLY AND MANAGE IT WISELY

Password format...

Choose a password with 8 alphanumeric characters (must be a combination of numbers and letters). For an even more secure password, combine upper case and lower case letters.

Choice of password...

Try to choose a password that you'll remember easily, but that will be hard for someone else to guess. For example, you can:

Take the first letters of each word in a sentence about you and add numbers ("I'm going on vacation on April 27" becomes "Igovo427");

Join a few words that make up a common phrase (e.g. milk1cow);

Change the spelling of words (e.g. 120burds);

Use the first letters or part of each word in an expression, song title or proverb ("Early to bed, early to rise" becomes "E2bede2r").

IMPORTANT: Do not use any of the above examples as your actual password.

Avoid choosing a password based on personal information: first name, surname, names of your spouse or children, date of birth, social insurance number, telephone number, license plate, name of a sports team, etc. Although easier to memorize, these passwords are more likely to be discovered by hackers.

PASSWORD SECURITY

Here are a few more pointers to ensure that your password remains confidential.

Never tell anyone your password, not even a family member or a person who claims to be a Bank, Credit Card Company or Credit Union employee.

Change your password regularly (at least once a month) so that it more difficult to discover. If you suspect that your password has been discovered, select a new one immediately.

Use a different password for each of your applications. Don't use the same password as the one you use to access your computer at work.

Don't use a password that contains a portion of your bank access codes (Client Card, credit card, PIN).

If possible, do not write your password down. If you absolutely have to, write it in such a way that only you will be able to recognize it, and keep it in a safe place.

Don't save your password on your computer or on a stick-it posted anywhere close to it.

Do not program any function keys to initialize a computer session.

Remember, your password is like the key to your house: you must take all the necessary precautions to prevent it from falling into someone else's hands.

CHANGING YOUR PASSWORD

To change your password, simply go to the "Profile" section of your Internet Banking, Credit Card Company or Credit Union while you are logged on.

When you change your password, please keep the following tips in mind:

Try to choose one you haven't used yet and don't use the same password more than twice in the same year;

Don't just choose two passwords and alternate between them;

Choose a secure password at least 8 characters in length. Use both alpha and numeric characters to make it that much safer.

FORGET YOUR PASSWORD?

If you really can't remember your password and could not correctly answer the secret questions, call a Customer Service representative at you Bank, Credit Card Company or Credit Union. The representative will assign you a temporary password so that you can access Personal Internet Banking. You must then choose a new secure password immediately in order to be able to continue.

SECRET QUESTIONS

By answering the secret questions when you create your password (when you access the "Profile" section of your Bank, Credit Card Company or Credit Union), you can still access your account even if you forget your password. If you have forgotten your password, simply click "I forgot my password" on the access page of your Bank, Credit Card Company or Credit Union Internet Banking and answer the questions. If you correctly answer the questions, the system will allow you to choose a new password so you can access the site. Otherwise, you can contact a your Bank, Credit Card Company or Credit Union for instructions.

You may also change your secret questions or the answers whenever you wish by accessing the Profile section of Personal Internet Banking Solutions.