



Safe Computing Practices

We have taken strong measures to ensure the security of your financial transactions and the confidentiality of your information. It is also important that you take precautions as well to help keep your information safe and secured.

Use Anti-Virus Software

Computer viruses and worms like "Melissa" and "Code Red" receive a lot of media attention because they can spread quickly and wreck havoc on personal computers and corporate networks. You should always use up-to-date anti-virus software that is capable of scanning files and email messages for viruses. This can prevent your files from being corrupted or lost, as well as save you hours of frustration as you try to restore an infected computer system.

Anti-virus software will also protect you from Trojan horses. Trojan horses are typically sent to computer systems through email. They are particularly dangerous because they have the potential to allow others to gain control of your computer system remotely, without your knowledge or consent. These programs can capture and send sensitive information stored on your hard drive to any other person who has gained remote access to your computer.

A variety of anti-virus software packages are available on the market today. Many of these products install anti-virus updates to your computer automatically, as long as you have the update feature enabled.

Use Personal Firewalls

Any computer or device connected to the Internet that is not properly protected is vulnerable to a variety of malicious Internet intrusions and attacks. This applies to all cable modem, digital subscribe line (DSL) and dial-up users. However, cable modem and DSL users are particularly vulnerable because both connection methods provide "always-on" connection capability. The likelihood of a malicious individual entering your computer increases significantly the longer your computer is on and connected to the Internet.

A personal firewall will help protect you from intrusion. Firewalls create a barrier between your computer and the rest of the Internet. A firewall can be a hardware device, a software application or a combination of the two. Firewalls can prevent malicious attacks and block certain types of data from entering your computer or private network. They can also be set up to alert you if anyone tries to access your system.

Use Strong Encryption

The stronger the encryption your Web browser uses, the more difficult it is for unauthorized individuals to intercept your online activities. To enhance your protection when accessing secure Web sites, use a Web browser that supports at least 128-bit encryption.

If your browser is currently supporting 40-bit encryption instead of 128-bit, it is recommended that you download a more recent versions of your browser from the vendor's Web site.



Use Unique Passwords

Passwords are used by computer systems and Web sites to verify who you are. When you login to a secure Web site using a password, you are granted appropriate access to available services and resources. If someone else knows or guesses your password, they can access the same resources. In other words, whatever you can do when you are logged into a site, they can do too!

Always choose unique passwords that include letters and numbers. Longer passwords that have eight or more characters and mix letters, numbers and special characters are much more difficult to figure out than shorter, more straightforward passwords. You should also avoid choosing passwords that are obvious, such as family names, birthdays and telephone numbers that might be easy for others to figure out.

Tips for Creating Unique Passwords

- ✓ Never share your passwords with others, including family members.
- ✓ Always use passwords that are difficult for others to guess. Choose unique passwords that include a mix of letters, numbers and special characters.
- ✓ Don't use passwords that are obvious, like your name, names of family members, your address, or any other information that a thief might find in your purse or wallet.
- ✓ Try to avoid passwords that are real words.
- ✓ Avoid using the same password for multiple applications or Internet services. You should use a unique password for each Web site and purpose.
- ✓ If your login IDs or passwords automatically appear in the sign-in page of a secure Web site, you should disable the auto complete function to increase the security of your information.
- ✓ Change your passwords frequently.
- ✓ Choose a rock-solid password. Choosing a rock-solid password is as easy as singing your favourite song. To create an easy-to-remember password, think of a favourite song, and take the first letter in each word. For instance, The Beatles' "I Want to Hold Your Hand," could be translated into a password - iwthyh, or iw2hyh, if you substitute "to" with the number 2.

Keep Your Software Up-to-Date

The software you use and the Internet itself can impact the security of your online activities. Therefore, you should watch for security bulletins that warn you about various security "holes" or "bugs" that may impact the software and Web browser you are using. It is very important to check the Web sites of your operating system and Web browser vendors for software "patches" and "updates". It is also a good practice to regularly check our Security Bulletins section for news on applicable software "patches" and "updates". Some operating systems and software can be configured to automatically check for new updates.

Remember to Log-Off

When you are finished conducting online transactions or visiting secure Web sites, remember to properly log-off and close your browser. This will ensure that any information that is cached or stored on your computer or in your browser is erased. This will prevent others from being able to view this information later.