Online Banking Security

Online Banking is a secure, Internet-based service that gives you convenient, 24-hour account access. Key takes information security very seriously and is committed to protecting your personal information with us. Learn what Key is doing to enforce information security.

User Identification (User ID) and Passwords

Upon enrollment to Online Banking, we require you to create a unique user ID, rather than use your Social Security number.

You must also create a password that you can change at any time. Passwords are a unique combination of characters that help you gain access to Online Banking. To change your password, select "Self Service," "Security Center," and then "Change Password."

- The safest passwords are those that combine numbers, letters and special characters
- We strongly urge that you not use obvious passwords, such as your birth date or name
- Never share your password with anyone
- Change your password frequently

Alerts

Alerts allow you to monitor specific activity on your accounts. There are two types of alerts: bank-initiated and optional. Bank-initiated alerts provide added security by advising you of any changes within your accounts that could be related to your online security. Optional alerts are set up by you to monitor specific activity, such as balance alerts, transaction alerts or specific alerts, such as your CD reaching maturity. All alerts are sent via email and can also be accessed within Online Banking

Tips on safe computing practices when conducting your online banking at home or at a public computer:

* Never leave your computer unattended once you have signed in to online banking

* After completing your transactions, ensure that you sign out of online banking, clear your cache, and close your browser

* Keep your password and card number safe

* Never share, disclose, or provide your bank card number or password to another party or website other than your bank, Most banks will never send you an email requesting this information.

* Never save your bank card number or password on a publicly accessed computer.

* If using a public access computer such as an Internet cafÃ or public library, change your password after completing your session by calling your bank's telephone banking number.

* When selecting a password, choose a series of characters that cannot be easily guessed by anyone else. CIBC recommends an alpha-numeric combination that's more than four characters long and a combination of capital and lower case letters. Don't use: a password you use for any other service; your name or a close relative's name; your birth date, telephone number or address, or those of a close relative; your bank account number or bank card number.

* Do not share your personal verification question answers with anyone, and do not disclose them in any emails. Giving your password answers to another person or company places your finances and privacy at risk.

More tips for secure Internet Banking

Password and PIN security:

You should always be wary if you receive unsolicited emails or calls asking you to disclose any personal details or card numbers. This information should be kept secret at all times. Be cautious about disclosing personal information to individuals you do not know. Please remember that Standard Chartered Bank would never contact you directly to ask you to disclose your PIN or all your password information.

If it sounds too good to be true - it probably is:

Don't be conned by convincing emails offering you the chance to make some easy money. As with most things if it looks too good to be true, it probably is! Be cautious of unsolicited emails from overseas - it is much harder to prove legitimacy of the organisations behind the emails.

PC security:

It is important to use up-to-date Anti-virus software and a personal firewall. If your computer uses Microsoft Windows operating system, it is important to keep it updated via the Windows Update feature, equally if you use another PC operating system or have an Apple Mac you should check regularly for updates. You should be vigilant if you use Internet cafes or a computer that is not your own and over which you have no control.

Keep your identity private offline:

Your identity can be as easily stolen offline as it can online. It is important that you comply with instructions about destroying new PIN numbers and expired bank cards. You should also consider using a crosscut shredder to destroy unneeded bank and other statements that may contain sensitive personal information. It is advisable to store retained documents in a suitable locked and fireproof container.

Check your statements:

It is important to check your statements regularly; a quick check will help identify any erroneous or criminal transactions that might have been performed on your account without your knowledge.

Check your banking session is secure:

When undertaking any banking on the Internet, check that the session is secure. There are two simple indicators that will tell you if your session is secure. The first is the use of https:// in the URL. Some browsers such as Mozilla Firefox change the colour of the url window when you are in a secure session. The other indicator is the presence of a digital certificate represented by a padlock or key in the bottom right hand corner. If you double click on this icon it should provide you with information about the organisation with which you have entered in to a secure session .

Check for Spyware:

In addition to being protected by using up-to-date antivirus software you should also regularly use software to remove Spyware from you computer, as these programs record information about your Internet use and transmit it without your permission. In some circumstances this can compromise your PC security.

Always completely log off from your Internet banking session:

It is important to completely log off from your Internet banking session; simply closing the window you performed the transaction in may not close the banking session. If your computer is infected with a Trojan, you session may become hijacked by a criminal and financial transactions performed without your knowledge. It is also advisable to disconnect from the Internet if you are not planning to use it.

What Standard Chartered Bank does to make your online banking secure:

Standard Chartered Bank used a combination of Secure Socket Layer (SSL) protocol and passwords to protect your information. In addition, stronger authentication is used as appropriate to particular markets.