ICBC E-Banking Risk Reminder

The Applicant should take note of the following warnings when using the ICBC E-Banking

1. Login to the correct website

- The Applicant who uses ICBC E-Banking through personal computer should log on directly to the Bank's website www.icbcthai.com. It is suggested to add this website's address to the favorite browser and not visit the Bank's website via indirect links.
- The Applicant who uses ICBC E-Banking through mobile phone should install the Bank's application ICBC Mobile Banking from "App Store" for iOS or "Play Store" for Android system.
- The applicant shall verify the developer of the bank's application before downloading the application to ensure the downloaded application came from the trusted developer, not the fake application.
- The applicant shall update the bank's application to be a current version on his mobile devices regularly.

2. Keep the account number, User Name and Password confidential

- For the security of the Applicant's information and funds, the Applicant should read the contents of this Risk Reminder thoroughly before setting the Password. When setting the Password, any personal-related information such as name, birthday, or telephone number should not be used as the Password.
- The Applicant shall keep confidential the User Name and Password as well as other passwords and information related to the use of ICBC E-Banking and shall not disclose such information to other persons.
- The Applicant shall change the Password regularly at least every 3 months.
- The Password for the ICBC E-Banking shall not be the same as those set for the bank card or other user password on other websites.
- The Password shall not be saved or stored on the computer, any electronic file or written down on paper that is not kept in a safe place.
- Every time the Applicant logs on to the ICBC E-Banking, the "last log-on time" should be checked against the actual log-on time.

3. Set your ICBC E-Banking's profile for your own secure

- The Applicant shall set the log-on notification via E-Mail at the setting menu. The Applicant shall change password immediately and contact the Bank's Call Center if getting notified but have not done the log-on transaction by yourself.
- The Applicant shall set the "Reserved Information" at the setting menu and verify "Reserved Information" on the welcome page to detect any unusual situation.

4. Use the authentication tool correctly

- USB-Shield and E-Password Token are an important tool for the security of the ICBC E-Banking. USB-Shield or E-Password Token (as the case may be) can be obtained from any branch of the Bank.
- The Applicant should keep the obtained USB-Shield or E-Password Token (as the case may be) and the Certification Password properly.

5. Keep Code Card properly

- The Code Card should be kept in a safe place to prevent it from being used by unauthorized persons and from loss and theft.
- The cover film on the Code Card, over time, can be scratched, when scratched the characters of the stored Transaction Password can easily be retrieved by others. Thus, the Applicant should take necessary measures to protect the scratched Transaction Password. It is, therefore, suggested that when over half of the cover film on the Code Card is scratched, further security protection methods should be taken by the Applicant. Consequently, a new Code Card should be issued when all the cover film on the Card is scratched.

6. Protect the Applicant's mobile phone

- The Applicant should not modify or alternate the Applicant's mobile phone system, used to log on ICBC E-Banking such as Jailbreak or Root.
- The Applicant who receives the Bank's SMS on the Applicant's mobile phone should take caution in using the mobile phone, keeping it safe from phone virus and unauthorized users.

7. Ensure the safety of the Applicant's computer

- Download, install or update Applicant's computer, widget, operating system and browser determined or provided by the Bank for the security.
- Install and promptly update anti-virus software.
- Install firewall program.
- Never open emails from unknown sources.

8. Other necessary protective measures

- Never allow any unauthorized person to use the Applicant's computer.
- Never use the ICBC E-Banking from publicly used computers such as Internet bars, public library, etc.
- Set a password on the computer or the mobile device to prevent others accessing confidential information.
- Never leave the computer or the mobile device idle while using ICBC E-Banking.
- Never run the Remote Assistance programs of the operation system while using ICBC E-Banking.
- Check that the payment amount and the billing amount are correct before confirming any transaction conducting via the ICBC E-Banking.
- Click "Logout" on the right top corner of the webpage to exit the ICBC E-Banking after each use.