Online Banking Security

The security mechanism of CTBC Bank Corporate Online Banking (eTrust) fully complies with the latest and highest security standards of global standards and industry technical specifications, and also meets the standards of local authorities, so you can use the Online banking services provided by the bank with confidence.

CTBC Bank Corporate Online Banking (eTrust) is quite safe. According to analysis, most of the security problems in online transactions today are due to human negligence, so as long as you pay attention, you won't suffer any loss.

In this regard, we would like to provide you with the following safety tips and remind you to review them from time to time.

- **Confidentiality when opening an account and applying for Internet banking**
  In view of the fact that unscrupulous persons may use various ways to obtain your transaction password, it is recommended that you handle the process of opening an account only with the banker, and do not allow other people to snoop when you change your password, so as to avoid the possibility of someone obtaining the account opening information and transaction password, which may affect your rights and interests.

- **Please keep your passwords in a safe place.**
  (e.g., Log-in password, iKey password, and Token Password)
  We suggest following the guidelines below.
  1. *Online access to your account is only possible once you have authenticated yourself by using the correct user ID and log-in password.*
  2. *Do not use a log-in password that is easy to remember or guess, e.g. Customer ID, Personal ID number, birthday, phone number, or repeated numbers.*
  3. *Change your passwords immediately once you received your password letter.*
  4. *Change passwords periodically and use strong password rules recommended by online banking so as to protect your online security.*
  5. *Pleases remember and do not share your passwords with anyone.*
  6. *Safeguard your passwords. Do not disclose passwords to others nor record them anywhere visible to avoid theft.*
  7. *The passwords for different purposes should be differentiated so that no one can guess them all at once.*
  8. *To protect your accounts, your access will be locked after 5 unsuccessful log-in attempts and 4 unsuccessful devices log-in attempts. If you want to reactivate functionality or suspect that someone is trying to guess your password incorrectly, please contact our customer service for further assistance.*

■ **Please make sure that the web address you logged in is a legally registered CTBC Online Banking web address.**

Before logging in, please confirm that the website you are logging in to is a legally registered CTBC Corporate Online Banking website. The Bank's Corporate Online Banking websites worldwide are listed below:

Taiwan：https://corporate.ctbcbank.com/tw/
Hong Kong：https://corporate. ctbcbank.com/hk/
New York：https://corporate. ctbcbank.com/ny/
Vietnam：https://corporate. ctbcbank.com/vn/
Singapore：https://corporate.ctbcbank.com/sg/
India : https://corporate.ctbcbank.com/in/
Japan：https://corporate.ctbcbank.com/jp/
China：https://corporate.ctbcbank.com.cn/

■ **128-bit Secure Sockets Layer (SSL) Technology**

Secure Sockets Layer (SSL) technology is used within your Internet banking session to encrypt your personal information so that no one else can read it. We use 128-bit SSL encryption, which is accepted as the industry standard.

■ **Additional Security Mechanism for Transactions**

To add an extra level of security, a digital signature (through an I-Key containing digital certificate) and one-time password (OTP) generated by Token if checker is requested are used when performing online transactions. Please plug-in I-Key every time while making a transaction. Your transaction will be initialed successfully only after inputting correct I-Key password. The checker(s) subsequently need to approve the transaction by inputting the correct OTP generated by Token. Please follow the *"Online User ID and Password"* guidelines for I-Key password and Token password. Please pull out I-Key from your computer and keep it in the secure place after the online transaction is done. Safeguard your I-Key and Token. If I-Key or Token is lost ,damaged , or stolen, please promptly contact our Customer Service.

****Please remember your I-Key password and Token Password and if you input wrong I-Key password or Token Password for 4 consecutive times, your I-Key or Token will be locked and you need to contact our Customer Service for further help.***

■ **Timeouts**

Internet banking online session will automatically log you off or timeout if your computer remains inactive for a period of time. You need to login again to resume your session. Please remember to log out every time and close your browser when you

finished using online banking.

■ **Please be alert to any unusual activities and contact the Bank if you have any abnormalities**

When you log in to Online Banking, the system displays a message similar to "Duplicate Login". If the same message appears repeatedly, it is possible that someone else is using Internet Banking under your identity, so please contact us as soon as possible.

■ **Please avoid using computers and WIFI networks provided in public to access Internet banking, conduct Internet transactions, and use financial services**

In order to prevent the interception of information such as Customer ID, User ID and Password, as well as all transaction records temporarily stored in the computer by any person who has the intent to do so, please do not use computers and WIFI networks provided in public to log on to Online Banking, carry out online transactions and financial services.

■ **The Online Security Tips**

We understand your concerns about online security. Enjoy the benefits of Internet banking service by following the guidelines below:

1. *During the Internet banking logon process, the bank's will **NOT** ask customers to enter any numbers displayed on the web to the security device to obtain security code.*
2. *Customers should continue to take precautionary measures to keep their computer safe to guard against Trojan Horse attack, including: Install personal firewall and anti-virus software in their personal computers and keep them up-to-date.*
3. *Be very cautious about opening attachments in e-mails from unfamiliar sources, and avoid visiting or downloading software from suspicious websites.*
4. *Never access the Internet banking accounts through hyperlinks embedded in emails, Internet search engines, suspicious pop-up windows or any other doubtful channels. Customers should connect to a bank website through typing the authentic website address in the address bar of the browser or by bookmarking the genuine website and using that for subsequent access. If customers find the website of the bank suspicious, they should not enter any information (including user ID, password and OTP) to the website and should report to the bank immediately.*
5. *If any unusual screens pop up and/or the computer responds unusually slow, customers are advised to log out from the Internet banking and scan the computer with the most updated version of virus protection software.*
6. *Don't disclose any personal information including logon password or OTP to any person through any means such as e-mail, over the phone or in person.*
7. *Review the transaction records regularly and report to the bank immediately if identify any suspicious transactions in the bank accounts.*
8. *Follow the Internet banking logon instructions and security tips published by the banks when conducting Internet banking transactions.*

Thank you for your continued understanding of the services provided by CTBC Corporate Online Banking. We hope this reminder will help you enjoy the convenience of Online banking in a safer way, and if you have any concerns about the security of Internet transactions, please feel free to contact our customer service lines in any region of the world, and we will have specialists to provide you with more detailed explanations.

☎Customer Service

Taiwan: 0800-017-888 / **Hong Kong:** (852)2916-1816 / **China:** (86) 21-2080-5888
New York: (212) 457-8903 / **Vietnam:** (84) 28-3910-1888 ext.6301~6304
New Delhi: (91) 11-43688888 / **Japan:**(81) 3-3288-9888 / **Singapore:**(65) 6351-4888