iTRUST Safety instructions for customers

CTBC new corporate internet banking platform, iTrust, adheres to the latest and highest international security standards and industry technical specifications. It also complies with local regulatory authorities' standards, ensuring that you can confidently use the various services provided by our internet banking platform.

Our corporate internet banking is highly secure. Based on an analysis of current online transaction security issues, most incidents arise from human negligence. As long as you pay a little attention, you will not suffer any losses!

For this purpose, we offer the following security instructions for your reference and remind you to pay attention at all times:

1. **Confidentiality during Account Opening and Application for Internet Banking**:
    - When opening account or applying for internet banking, interact directly with our staff to avoid potential fraudsters. Change your password discreetly to prevent others from observing it and gaining unauthorized access to your account details.

2. **Safeguarding Various Passwords**:
   (For example: login password, voice password, CA device password, random dynamic password device startup password, etc.)
    - Avoid using easily guessable numbers (such as unified business number, personal ID number, birthday, phone number or repeated numbers) as passwords.
    - When you apply for relevant business, please change the password in the password letter sent to you by CTBC as soon as possible and remember it.
    - Change passwords periodically, especially if you suspect a security breach.
    - Never share your passwords with anyone.
    - Do not write down passwords where others can easily access them.
    - Be cautious when entering passwords.
    - Passwords for different transactions should be distinguished to avoid being guessed all at once.
    - When the login password you use is incorrect 5 times in a row, and the device password is incorrect 4 times in a row, our bank will suspend the functions of the corresponding internet banking, voice system, CA device, or random dynamic password device. If you want to restore the relevant functions or suspect that someone is trying to guess the password in an incorrect way, please immediately contact the customer service hotline for assistance from our bank's dedicated personnel.

3. **Verify the Legitimate iTrust Website**:
    - Before logging in, please confirm whether the website you logged in to is a legally registered website for CTBC corporate internet banking. The global website for our bank's corporate internet banking is as follows:
      Taiwan: https://itrust.ctbcbank.com

4. **Remove Your CA Device After Transactions**:
    - To prevent unauthorized use of your CA device, remove it from the computer after completing transactions/authorizations.

5. **Immediate Reporting of Lost CA Devices: (temporary loss reporting)**
    - Your CA device stores your electronic certificate. If it is lost, please immediately apply to our bank for temporary suspension of the certificate (temporary loss reporting) to avoid being stolen by others and affecting your rights. Please contact the customer service hotline for the application procedures, and a dedicated person will assist you.

6. **Immediate Reporting of Lost Random Dynamic Password Devices**:
    - In addition to the CA device, you may use our bank's random dynamic password device or mobile device to authorize transactions. Please keep this device safe. If it is lost, please immediately contact our customer service hotline to apply for reporting the loss or unbinding the mobile device to avoid being stolen by others and affecting your rights.

7. **Log Out and Close the Browser After Transactions or Temporary Absence**:
    - When you leave your seat temporarily or have completed transactions or inquiries, remember to log out and close the browser to prevent others from using the browser's related functions to obtain important information about your transactions or inquiries.

8. **Beware of Unauthorized Use of Your Identity**:
    - When you log in to internet banking, the system displays a message similar to "repeat login" and forces to log in. If the same message appears repeatedly, or if you receive a login notification but have not logged in to internet banking, it is possible that someone else is using your identity to use internet banking. Please contact our bank as soon as possible.

9. **Avoid Using Public Computers for Internet Banking**:
    - Please try not to use computers provided in public places for online transactions, in order to avoid data such as unified business number, user code, password and all transaction records temporarily stored on the computer being intercepted by malicious individuals.

10. **Regularly Update Your Antivirus Software and Scan for Viruses**:
    - At present, malicious individuals can obtain relevant data stored on your computer through viruses or similar malicious code (such as Trojan virus). Please install antivirus software on your computer, regularly update the version, and clean up the virus.

11. **The Internet is Trapped Everywhere!! Teach you how to identify fake websites and fraudulent emails:**
    - When you log in to our internet banking, CTBC will not ask you to enter the password of your security device on non-Bank websites.
    - Please install personal firewall and antivirus software on your personal computer and update the version at any time.
    - Avoid opening emails from unknown sources and downloading software from suspicious websites.
    - Please do not log in to internet banking through links in emails, internet search engines, suspicious pop-up websites, or other suspicious channels. Please enter the verified website address directly in the browser address bar or add the website to my favorites by logging in and clicking directly. If you find any suspicious websites, please contact CTBC immediately.
    - If your computer has abnormal window jumping or slow execution speed, it is recommended that you log out of internet banking and use updated antivirus software to scan.
    - Do not share any personal information to others via email or phone, including login password or OTP password.
    - Check transaction records regularly. If you find any suspicious transactions in your account, please report it to CTBC immediately.
    - Please follow the login instructions and security prompts announced by CTBC to complete transactions in internet banking.

Thank you for your further understanding of the services provided by CTBC new corporate internet banking platform. We hope this reminder can assist you in making safer use of the convenience brought by internet banking. If you have any concerns about the security of online transactions, feel free to contact our customer service hotline in various regions around the world. Our dedicated person will provide you with more detailed explanations.

Customer Service hotline
Taiwan: **0800-017-888 or (886) 2-22555-1380**