Online Security

We use industry standard security technology and practices to ensure your account and online transaction are safe and secure.

We do this in the following ways:

Online User ID, Log-in Password and Token Password

Online access to your account is only possible once you have authenticated yourself using the correct user ID, log-in password and one-time password (OTP) generated by Token.. Pleases remember and do not share them with anyone. We suggest following the guidelines below.

1. Change your log-in password immediately once you received your password letter.

2. Do not use a log-in password that is easy to remember or guess, e.g. birthday or phone number.

3. Change your log-in password periodically so as to protect your online security.

4. Safeguard your user ID, log-in password and Token password which is used for generating OTP on Token. Do not disclose User ID, log-in password and Token password to others nor record them anywhere visible to avoid theft.

5. To protect your accounts, your access will be locked after 4 unsuccessful attempts. You may have it unlocked by contacting Customer Service.

6. Safeguard your Token. If Token is lost or stolen, please promptly contact Customer Service.

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/or 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. If checker is needed, checker needs to approve the transaction inputting the correct OTP generated by Token. Please follow the"

Online User ID, Log-in Password and Token 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 is lost or stolen, please promptly contact 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 Customer Service.

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 have finished your online banking.

The other online security tips

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

1. Make sure you have the latest security updates and patches.

2. Install anti-virus software and the software should be updated on a regular basis with the latest virus definition files.

3. Never access Internet Banking from a public computer (e.g. cybercafe, library, etc.). Prevent others from spying on you at all times.

4. Watch out for phishing sites. Confirm if the URL is correct before accessing Internet banking service. Never use links in unknown e-mails or spoof web pages appearing to be an official website to log on to Internet Banking. Bookmark the genuine Internet banking website: https://corporate.chinatrust.com/sg/

5. Always log out after you have done in Internet banking service.

6. Pay attention to transaction notices. Check the notice promptly for accuracy. Contact Customer Service if you discover or have doubt over unauthorized use of your Internet banking account or password.

Be aware of these tips and enjoy the convenience of this service.