NCB 南洋商業銀行

Security Information

This webpage sets out the security information of the electronic banking ("e-banking") Services offered by Nanyang Commercial Bank, Limited ("the Bank"). e-banking services refers to banking services delivered over the internet, wireless network, ATMs, telephone network or other electronic network, terminals or devices, including but not limited to the Bank's Internet Banking, Mobile Banking, Phone Banking, NCB e+ Mobile Application ("NCB e+"), Automated Banking and WeChat official account.

Latest / Important Security Information

- To safeguard your online banking security, verification code is required in Internet Banking / Mobile Banking login. During the Internet Banking / Mobile Banking services login process, customers are required to input the Internet Banking No. / User name and Internet Banking Password as well as a Verification Code.
- To safeguard your banking security, customers are required to input the NCB e+ Password as well as SMS OTP before reviewing account information or updating documents for account opening application on NCB e+.
- In order to provide better security for online investment services, Two-factor Authentication and agreement to receive specified transaction notification are required for every designated transaction conducted through Internet or Mobile Banking. For details of Designated Transactions Secured by the Two-factor Authentication on Internet and Mobile Banking, please visit the Bank's website "e-Banking Services > Two-factor Authentication".
- Customers are reminded not to log into Internet/Mobile Banking or provide any sensitive personal information through hyperlinks, QR Code or attachments embedded in any third-party websites, mobile Apps, emails, SMS or instant messages. To ensure secure transactions, customers should input directly the website address of the Bank into the browser address bar when logging into Internet Banking or mobile banking services.
- Customers should be aware of the obligations in relation to security for e-banking services including observing and following in a timely manner the "Conditions for Services" and the relevant security measures specified from time to time by the Bank for the protection of customers.
- Customers should be responsible to take reasonable steps to keep any device (for example, personal computers, security devices that generate Mobile one-time passwords and smart cards that store digital certificates) or secret code (for example, Internet Banking password, phone banking password and NCB e+ password) used for accessing e-banking services secure and secret, including but not limited to:
  - destroy the original printed copy of the secret code;
  - not to allow anyone else to use their secret code;
  - never write down the secret code on any device for accessing e-banking services or on anything usually kept with or near it;
  - not to write down or record the secret code without disguising it.
- If a customer acts fraudulently or with gross negligence such as failing to properly safeguard his device or secret code for accessing the e-banking services, he will be responsible for any direct loss suffered by him as a result of unauthorised transactions conducted through his account.
- Customers will be liable for all losses if customers have acted fraudulently. Customers may also be held liable for all losses if customers have acted with gross negligence (this may include cases where customers knowingly allow the use by others of their device or secret codes) or have failed to inform the Bank as soon as reasonably practicable after customers find or believe that their secret codes or devices for accessing the e-banking services have been compromised, lost or stolen, or that

unauthorised transactions have been conducted over their accounts. This may apply if customers fail to follow the safeguards set out of this article if such failure has caused the losses.

- Customers are reminded to stay vigilant to anything abnormal when logging into e-banking services (e.g. unusual pop-up screens, unusually slow browser response, multiple requests for password input etc).
- During the e-banking logon process, the Bank will not request customers to enter any numbers to their security device to obtain security code. In case of doubt, please do not follow the instructions of the suspicious web page or input any data. Customers are advised to terminate the operation of e-banking services immediately. Please contact the Bank in case of any enquiry.
- Customers should keep their personal information (including biometric data) secure. The Bank will not enquire customer's personal information, e.g. user name, password, one-time password or other account details by email, SMS, instant messaging or phone.
- Before inputting OTP as the transaction authorization for any transaction, you should verify the details of transaction request carefully, such as transaction type, amount and currency, etc. in order to confirm these are actually referring to the intended transaction. If you have any enquiry, please contact us immediately.
- To safeguard their payment cards, card information and authentication factors, customers should stay vigilant against card frauds and scams, particularly those involving online transactions and binding of cards to mobile payment services.
- Customers may need to bear the consequences of not properly protecting their physical cards, card information, and authentication factors. In particular, the consequences for ignoring pre-and post-card transaction related communications from the bank.

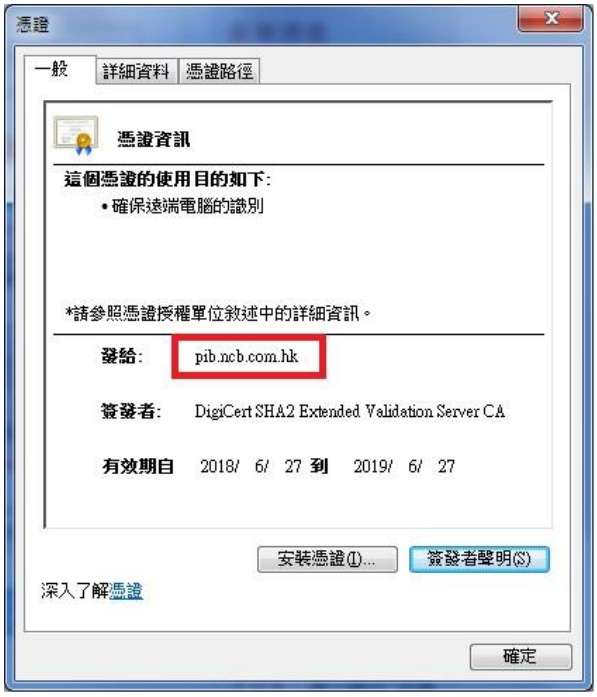
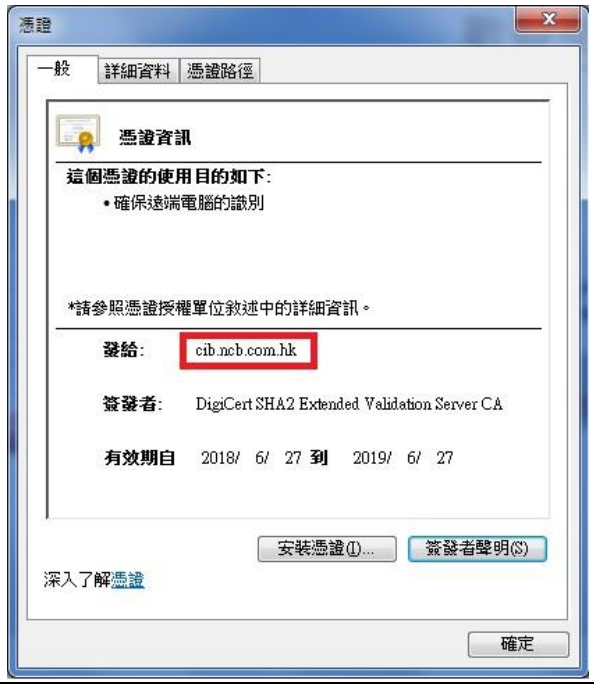
Online Security Tips and Information

What Have We Done to Protect You

- We have adopted the 128-bit or above Transport Layer Security ("TLS") encryption to ensure the security of your data during transmission and prevent any unauthorised access by the third party to your data.
- Our web servers are protected by firewall systems to prevent any unauthorised access to the Bank's system.
- Customers' login attempts are recorded systematically. In the event of several consecutive login attempts with incorrect password, the related Internet Service will be suspended immediately.
- The Internet Services will be automatically disconnected after remaining inactive (i.e. no operational instructions have been received) over a period of time to prevent unauthorised transaction.
- The Internet or Mobile Banking Services of the Bank provides customers with "Mobile Token" and "Security Device" as two-factor authentication tools. When designated investment transactions are conducted through Internet or Mobile Banking, the Bank would send a one-time password via text message (SMS) as part of the two-factor authentication process for online trading.
- To ensure you can receive our notification messages for the security of your online transactions, if you changed your contact information, please login to your internet banking "Setting > Change Personal Information" to change your personal information with Two Factor Authentication. Besides, you can update your E-mail address and mobile number by downloading the form from our website (www.ncb.com.hk/pform) and returning the completed form to our branches. You can also visit any of our branches for registration.
- If you have changed your contact information and the information as same as your registered Proxy ID (mobile phone number or email address), please login to your internet banking to update your Proxy ID accordingly.

Security Certificate

We use Extended Validation ("EV") SSL Certificate to allow customers to verify the authenticity of our websites by checking the address bar of your browser. The address bar is green for browsers of Microsoft Internet Explorer Version 9 or above which is one of the security features of EV SSL. For browsers of Microsoft Internet Explorer, you can also check the certification details, including the validity date of the certificate and the following information, by clicking the "security lock" icon at the login page of our internet banking service. Please note that the layouts may be different for different browser versions. For details on the EV SSL Certificate, please refer to the website of DigiCert, the issuer of the certificate.

	
Personal Internet Banking Domain name issued to: pib.ncb.com.hk Issued by: DigiCert SHA2 Extended Validation Server CA	Corporate Internet Banking Domain name issued to: cib.ncb.com.hk Issued by: Symantec DigiCert SHA2 Extended Validation Server CA

Recommended browsers for minimum security requirements

To ensure customer data security, please install any of the browser versions we recommend to log into the Internet Banking.

Personal Internet Banking	Corporate Internet Banking
● Microsoft Internet Explorer (Version 11 or above) ● Mozilla Firefox (Version 45.2 or above) ● Apple Safari (Version 8 or above) ● Google Chrome (Version 43 or above)	● Microsoft Internet Explorer (Version 11 or above) ● Mozilla Firefox (Version 45.2 or above)

NCB 南洋商業銀行

Information Security Tips

1. Beware of fraudulent website

   Customers are reminded to be vigilant of any fraudulent websites which seek to pass off as the Bank's websites. Unless you are certain that you are connected to the websites of the Bank, particulars of your Internet Services should not be provided.

2. Fraudulent emails

   Please note that viruses, Trojan software and hacker programmes can be distributed via emails. Virus like "Worms" can even reproduce and deliver infected emails to the recipients in your address book. Hence, you should not open any unknown or suspicious emails. Instead, you should delete them immediately. Please do not log into Internet Services through hyperlinks or QR Code embedded in any emails or SMS. You should also perform virus scanning before opening any attachment. In addition, you should pay extra care as fraudsters will perpetrate frauds using emails.

   Please do not rely solely on email correspondences for any remittance transaction. You should use other channels (e.g. telephone, fax, etc.) to confirm the transaction and the beneficiary details before completing the remittance.

   Example 1 of fraudulent emails: Commercial email scam
   A fraudster hacked into the email correspondences between a foreign buyer and its service provider over a few months. After getting to know the details of their transaction, the fraudster sent out fictitious emails at an email address very similar to that of the service provider, requesting the foreign buyer to make a remittance to a fraudulent account.

   Example 2 of fraudulent emails: Fraudulent claims of estate
   A fraudster claimed to be a bank staff in an email, inviting the recipient of the email to pretend to be the next-of-kin of a deceased client who has left a huge sum of unclaimed fixed deposit. Upon receiving favourable reply, the fraudster requested the recipient to pay a fee in advance for preparing the necessary documents in order to claim that estate. In the end, the email recipient was deceived.

   Example 3 of fraudulent emails: Unauthorised device binding and fund transfers.
   Customers were tricked into entering their e-banking credentials and SMS One-Time Passwords (OTPs) by phishing emails with embedded hyperlinks that appeared to be sent by the Bank. Utilizing the mobile apps of the Bank, fraudsters connected their mobile devices to the victims' bank accounts with the credentials and OTPs. Even though the device binding had a deferred execution period, customers were deceived into helping the fraudsters activate their devices after the deferred period by offering assistance (such as entering another SMS OTP). The scammers had complete access to the consumers' bank accounts and used it to transfer funds to foreign bank accounts without authorization.

3. Fraudulent Instant Messages

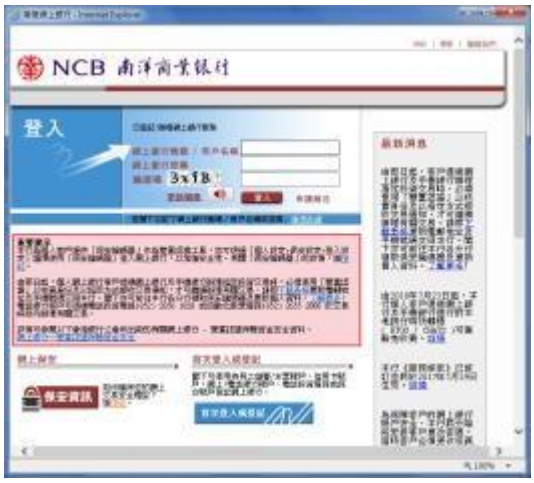
Customers are reminded to be vigilant of any fraudulent instant messages impersonating the Bank or purporting to be from a bank staff. These messages usually induce recipients to provide personal or account details for identification or investment scheme participation. Customers should not respond to these messages, click any suspicious links, download any suspicious files or provide any information.

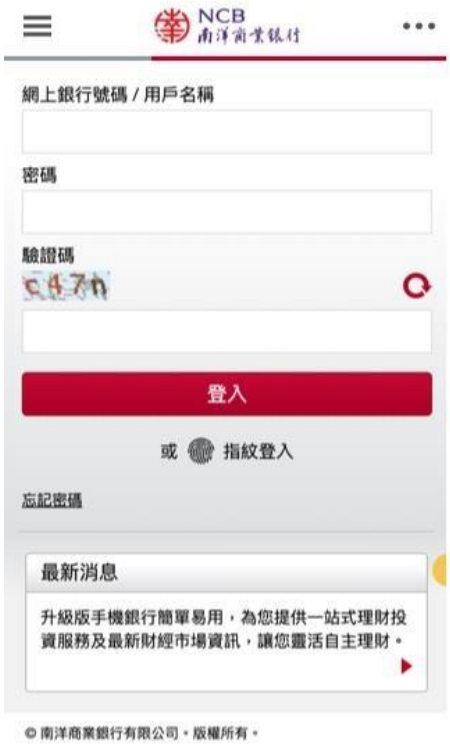
4. Man in the Browser Attack

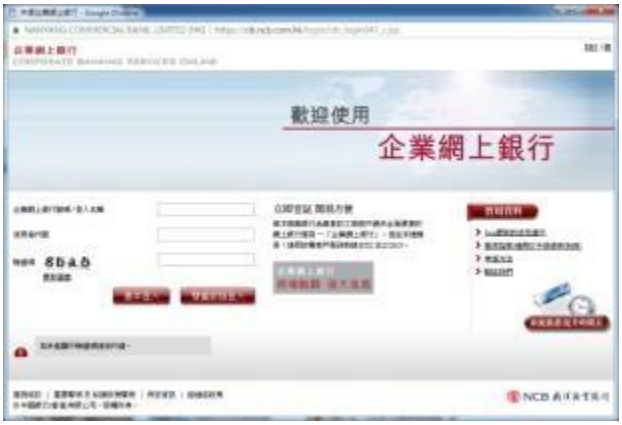
The suspected Trojan Horse cases have recently been reported by few corporate customers when they used the corporate ernet banking service. During the login process, a fake webpage was displayed requesting the customers to input their login names and passwords, as well as the one-time transaction confirmation codes generated by their "security devices".

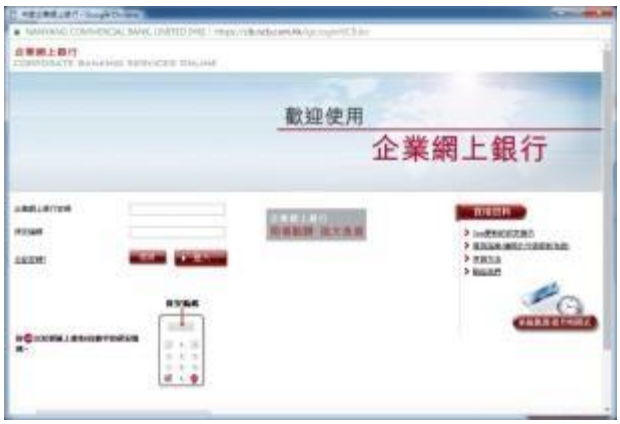
To ensure that customers are securely protected when using Internet Banking Service, the Bank would like to remind customers to stay vigilant of any unusual login webpages during their internet banking login process (such as unusual screens pop up and/or the unusually slow computer response). If customers find any webpage suspicious, they should not follow its instruction or input any information and should close the browser immediately. The one-time transaction confirmation code generated by the "security device" is only required for "designated transactions". The Bank's Internet Banking login process does not require customers to enter the one-time transaction confirmation code (Please refer to the following login page).

The Bank would like to remind customers to install firewall and anti-virus software in their personal computers and keep them up-to-date. They should also avoid visiting or downloading software from suspicious websites, and be wary of opening attachments or any hyperlinks in emails from unfamiliar sources. Please do not click the hyperlinks or open the attachments in suspicious emails purporting to be sent by banks; You can access our banking service through https://www.ncb.com.hk or our mobile banking. Please do not login the banking service through any link in suspicious email, SMS or website search from search engine. If in doubt, please contact us to verify whether an email is actually sent by the Bank.

<table>
<tr>
<td>Personal Internet Banking Login
 

Input the Internet Banking No. / User Name, password and verification code, and press “Login”</td>
<td>Mobile Banking Login
 

Input the Internet Banking No. / Username, password and verification code, and press “Login”</td>
</tr>
<tr>
<td>CBS Online "2FA Login" process* (Not applicable to e-Cert users) Please enter Corporate Internet Banking Number / Login Name and User ID, and then press "2FA Login"
 

*Customers can select "Basic Login" for account enquiry</td>
<td>In the "2FA Login" page, please enter Corporate Internet Banking Password and Security Code generated by the "security device"
 
</td>
</tr>
</table>

5. Common Signs of Phishing Emails, SMS and/or instant messages

The “Phishing” fraudsters often send out emails or SMS purportedly from our bank in order to trick you into providing account details, passwords, personal information or credit card numbers. To stay vigilant, some common signs of phishing emails, SMS and/or instant messages are listed below.

- Grammatical mistakes, typos or misspelling is found in the content.
- The name of the sender shown in emails, SMS and/or instant messages may be exactly as same as our name.
- It usually appears as an important notification from our bank or request for personal information to verify your account details, such as notification for a huge amount of fund transfer or notification for a new security function activation, that customer is required to click the hyperlink or open an attachment.
- Embedded hyperlink or attachment is normally found in email. The hyperlink looks like a genuine website address of our bank, but it refers to another website address when mouse-over it.

6. Your password and personal information should be well protected

- Upon receipt of your password mailer, please change the password via the Internet Services immediately and destroy the password mailer.
- Please memorise your password. Do not write or store the password on any of the devices used for the Internet Services or anything which is usually kept with these devices, or record password in any way without covering it.
- Please change your password regularly, -do not use your name, date of birth, ID/passport number, telephone or lucky number, or other easy-to-guess numbers or words as your password, and avoid selecting the same password that you have used for accessing other web services.
- Do not disclose your user name and password of your Internet Services to anyone (including bank staff and the police). You should also avoid disclosing your personal information such as ID/passport number and date of birth to anyone.
- Do not allow anyone else to use your Internet Banking Services.
- If you have lost or disclosed your password/security device(s), or suspected that your password or security device(s) has/have been used by an unauthorised party, or found any unauthorised transaction(s) associated with your account, please contact us immediately, or directly contact the Hong Kong Police Force.
- Please carefully examine the transaction details listed in the statement of account, advice and confirmation. In case of any error or suspicious transaction, please notify us immediately.
- You can conveniently access your transaction records via the Internet Banking.

7. Protect your personal computer against hackers and viruses

- Please download and install updates and patches for your operating systems and browsers regularly.
- Please install firewall systems on your personal computer.
- Please install anti-virus software on your personal computer. Update the virus definition file and perform virus scanning regularly.
- Please set a passcode for locking device that is difficult to guess and activate the auto-lock function.
- Avoid downloading or installing programmes from unreliable sources or opening suspicious files or emails. This helps protect your personal data against hackers' programmes or viruses.
  If you access our Internet Services via wireless network, please check your network security settings.

8. Take precautionary measures while you are using Internet Banking Service

- Do not access the Internet Banking Service using a shared computer in public places such as cafes or bars with internet access.
- Only pre-set and access reliable wireless networks for internet connection.

- Do not log into the Internet Services through hyperlinks or QR Code embedded in any emails, SMS or search engines.
- Close all other internet browsers before accessing Internet Banking. Do not open other internet browsers or visit any other websites while you are using the Internet Services.
- Make sure no one can see your user name and password when you log into the Internet Services.
- Please check your last login and logout records every time you use the Internet Services. Please also check your account balance and transaction records regularly. If you discover anything suspicious, please contact us immediately.
- Click the "logout" button to exit from the system after you have finished all your online transactions. Please always clear the cache and history in your browser after using our online service.
- Do not leave your computer unattended before logging out the Internet Banking Services.
- To learn more about other online security measures, please click here.

9. Dual authorisation for financial transactions (Applicable to customers of CBS Online only)

- To enhance security and ensure the accuracy of transaction details, you are advised to set up dual authorisation for financial transactions to be conducted via CBS Online.

10. Review and adjust your services' limits

- Please review your services' limits regularly and to make necessary adjustment that suits your transaction needs.

Security tips for Mobile Banking

How to download Personal Mobile Banking Apps?

- Personal Mobile Banking provides various banking and securities services. You can input " www.ncb.com.hk/app " in mobile browser to download the Apps;
- Search "NCB"(Nanyang Commercial Bank) for free download of the Apps through the online App stores (Google Play and App Store).
- If there are suspicious App for downloading, please do not login and stop proceeding the download immediately.
- To ensure the search wording is correct and prevent from downloading any counterfeit Apps which is attached with phishing program / Trojan to steal the login information.
- Do not reproduce and install any suspicious Apps on your mobile device(s).
- If there is any abnormal operation, e.g. suspicious pop up pages or a delay login, please stop the login immediately.

Is Mobile Banking secure?

- The Bank's website is protected with strong encryption (128-bit SSL). Access is protected by personalised user name and password. The system is protected from duplicate access, i.e. customers cannot log into the system at the same time using different mobile phones or computers. The session will be automatically disconnected after remaining inactive over a period of time to prevent unauthorised transaction.

How can I access and log into Mobile Banking?

- Please download “NCB” (Nanyang Commercial Bank) from official application stores, open the mobile application, click “login” and then log into the Mobile Banking using your relevant Internet Banking number/user name and password.

Have you obtained any security certification for your Mobile Banking?

- We have obtained the certificate issued by DigiCert for our Mobile Banking.

What should I be aware of when using Mobile Banking?

- Do not save or keep your password in a browser, and disable the "Auto-Complete" feature to prevent any third party from unauthorised access to your login information via the browser.
- Avoid logging into the Mobile Banking via wireless network (i.e. Wi-Fi) which is public or without password setting. We advise using encrypted and reliable mobile internet connection.
- Activate the auto-lock function of your mobile device and avoid logging into Mobile Banking in a crowded area and be careful when entering your password via specific mobile device. The format of password may be enlarged with clear display. It would indirectly disclose your login information to other people.
- Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) or Payment Apps not in use. Choose encrypted networks when using Wi-Fi and disable Wi-Fi auto-connection settings.
- Avoid using the mobile device from other to login Mobile Banking and sharing your mobile device with others.
- It is recommended to setup firewall and install anti-virus software / mobile security App in your mobile device and update regularly. You can visit HKCERT website for reference: https://www.hkcert.org/mobile-security-tools, to select the appropriate Apps.
- To protect your online transactions, we will check whether your mobile device is jailbroken or rooted and with recommended operating systems for minimum security requirements upon using of the Bank's Mobile App. Customer may not be allowed to access the Mobile Banking via such device. Please pay attention to the reminder.
- Please check your last login and logout records every time you use our Mobile Banking. You should also check your account balance and transaction records regularly. If there are suspicious transactions, please contact us immediately.
- You should ensure proper protection of your password and personal information and hold accountability of this:
  - Please memorise your password. Do not write the password on any of the devices used for Mobile Banking or anything which is usually kept with these devices, or store the password in the mobile phone or record it in any way without covering it.
  - Do not use your name, date of birth, ID/passport number, telephone or lucky number, or other easy-to-guess personal information, numbers or words as your password and avoid selecting the same password that you have used for accessing other web services.
  - Do not disclose your user name and password of Mobile Banking to anyone (including bank staff and the police). You should also avoid disclosing your personal information, such as ID/passport number and date of birth, to anyone.
  - Do not allow anyone else to use your Mobile Banking or password.
  - Please change your password regularly.
  - If you have lost or disclosed your password/lost your security device(s), or suspected that your password or security device(s) has/have been used by an unauthorised party, or found any unauthorised transaction(s) associated with your account, please contact us immediately, or directly contact the Hong Kong Police Force.
- Please download and install the latest version of the Bank's Mobile App, other Mobile Apps, operating systems and browsers regularly in the official App stores (Google Play and App Store) or our website. Do

not install Mobile Apps from mistrusted sources. If there is any suspicious App, please do not download, login and should stop operation immediately.

- Do not download the QR code through any social media casually, please ensure the QR code is from a trusted source before scanning.
- Stay vigilant when you scan the QR code, ensures the QR code is from a trusted source before scanning.
- Please carefully verify the beneficiary masked name before using QR code or Proxy ID for payment.
- Please carefully verify the merchant / shop name before you scan the QR code or Proxy ID for payment.
- Please carefully examine the transaction details listed that generated by QR Code.
- Please check the transaction record issued by the Bank after the transaction.
- Do not disclose the QR code generated by our NCB mobile application to others unless you are conducting fund transfer or payment transaction.
- You should use all reasonable care to keep your mobile devices secure. If you find that your mobile devices have been lost or stolen or that any unauthorised transactions have occurred, you should contact us immediately, or directly contact the Hong Kong Police Force.

What should I be aware of when using Biometric Authentication service?

- Upon the successful registration of the “Biometric Authentication” service on your mobile devices, any fingerprint or Face ID that being stored on your mobile device can be used for the purpose of the “Biometric Authentication” service. You must ensure that only your fingerprint or Face ID is stored on your mobile devices, and ensure the security of the security codes as well as the passwords or codes that you can use to store your fingerprint or Face ID and register the “Biometric Authentication” service on your mobile devices.
- For security reasons, do not use jailbroken or rooted mobile devices.
- You can cancel the “Biometric Authentication” service by disabling the option of "Enable Biometric Authentication Login and Use Mobile Token" via "Left Menu > Setting > Mobile Token Setting" after logging in Mobile Banking or contacting our customer service hotline or accessing any of our branches to "suspend mobile token". Please note that after you cancel the “Biometric Authentication” service, your fingerprint or Face ID will be continuously stored on your designated mobile devices. You may consider cancelling the data at your own decision.
- If your fingerprint or Face ID record of your designated mobile devices has been changed or the “Biometric Authentication” service has not been used for a specified period of time (which shall be defined by the Bank from time to time), your “Biometric Authentication” service will be suspended. You are required to re-register or re-activate the “Biometric Authentication” service.
- You must not use “Biometric Authentication” if you have reasonable belief that other people may share identical or very similar biometric credentials of you. For instance, you must not use Face ID for authentication purpose if you have identical twin or triplet siblings.
- You must not use “Biometric Authentication” if the relevant biometric credentials of you are or will be undergoing rapid development or change. For instance, you must not use Face ID for authentication purpose if you are an adolescent with facial features undergoing rapid development.

What if there is an incoming call or weak signal when I am placing an instruction? How can I ensure the instruction has been submitted?

- If your instruction has been successfully submitted and executed, a transaction reference number will be displayed on the webpage of the Mobile Banking. You can also check the last ten transaction records as to whether the instruction has been successfully submitted and executed.

Do I need to close the web browser after logging out Mobile Banking?

- You are advised to close the web browser after logging out and delete the temporarily saved and past historical records on a regular basis.

Security tips for NCB e+ Mobile Application

How to download NCB e+ Mobile Application ("NCB e+")?

- Search "NCB e+" for free download of the Apps through the official online App stores (Google Play and App Store).
- If there are suspicious Apps for downloading, please do not login and stop proceeding the download immediately.
- To ensure the search wording is correct and prevent from downloading any counterfeit Apps which is attached with phishing program / Trojan to steal the login information.
- Do not reproduce and install any suspicious Apps on your mobile device(s).
- If any abnormalities are found, e.g. unusual layout or unusual slow login response, please stop the operation immediately.

Is NCB e+ secure?

- NCB e+ is protected with strong encryption (128-bit SSL). Access is protected by telephone number and SMS OTP. The session will be automatically disconnected after remaining inactive over a period of time to prevent unauthorised operation.

How can I access and log into NCB e+?

- Please download NCB e+ from official application stores, open the mobile application, log into the NCB e+ using your telephone number and SMS OTP.
- Customers are required to input the NCB e+ Password as well as SMS OTP before reviewing account information or updating documents for account opening application on NCB e+.

What should I be aware of when using NCB e+?

- Avoid logging into the NCB e+ via wireless network (i.e. Wi-Fi) which is public or without password setting. We advise using encrypted and reliable mobile internet connection.
- Activate the auto-lock function of your mobile device and avoid logging into NCB e+ in a crowded area and be careful when entering your password via specific mobile device. The format of password may be enlarged with clear display. It would indirectly disclose your login information to other people.
- Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) or Payment Apps not in use. Choose encrypted networks when using Wi-Fi and disable Wi-Fi auto-connection settings.
- Avoid using the mobile device from other to login NCB e+ and sharing your mobile device with others.
- Customers should avoid connecting the mobile device to any personal computer that is suspected to be infected by computer virus. The mobile device is also infected. At the same time, it is recommended to setup firewall and install anti-virus software / mobile security App in your mobile device and update regularly. You can visit HKCERT website for reference: https://www.hkcert.org/mobile-security-tools, to select the appropriate Apps.
- To protect your personal information, we will check whether your mobile device is jailbroken or rooted and with recommended operating systems for minimum security requirements upon using of NCB e+. Customer may not be allowed to access the NCB e+ via such device. Please pay attention to the reminder.
- Customers are advised to set the auto-lock function for mobile devices, and do not choose personal information, numbers or characters that are easy to guess as passwords, and avoid using passwords registered on other websites as login passwords. Please download and install the update programs of this mobile application and other applications, mobile operating systems and browsers regularly through the designated official software application store (please refer to the Bank's website for details) or the Bank's website.

- When customers download or use NCB e+, information about your mobile device (including IP address, device ID and operating system), login and logout time will be recorded for the purpose of operational enhancement, statistical analysis and anti-fraud. Relevant information will not be retained for longer than necessary to fulfill the purpose.
- You should ensure proper protection of your NCB e+ Password and personal information and hold accountability of this:
  - Please memorise your NCB e+ Password. Do not write the password on any of the devices used for Mobile Banking or anything which is usually kept with these devices, or store the password in the mobile phone or record it in any way without covering it.
  - Do not use your name, date of birth, ID/passport number, telephone or lucky number, or other easy-to-guess personal information, numbers or words as your NCB e+ Password and avoid selecting the same password that you have used for accessing other web services.
  - Do not disclose your NCB e+ Password to anyone (including bank staff and the police). You should also avoid disclosing your personal information, such as ID/passport number and date of birth, to anyone.
  - Do not allow anyone else to use your NCB e+ or NCB e+ Password.
  - Please change your NCB e+ Password regularly.
  - If you have lost or disclosed your NCB e+ Password/lost your security device(s), or suspected that your NCB e+ Password or security device(s) has/have been used by an unauthorised party, or found any unauthorised transaction(s) associated with your account, please contact us immediately, or directly contact the Hong Kong Police Force.
- You should use all reasonable care to keep your mobile devices secure. If you find that your mobile devices have been lost or stolen or that any unauthorised operations have occurred, you should contact us immediately, or directly contact the Hong Kong Police Force.

What if I quit the online submission process on NCB e+ halfway?

- Customer cannot resume the application process if they quit the online submission process halfway.

The NCB e+ or WeChat official account's web page for account opening application do not retain filled in information or uploaded documents during the application process if the application is not submitted.

How can I reset NCB e+ Password if I forget answer to security question and NCB e+ Password?

- If customer has not submitted bank account opening application, customer can reset NCB e+ Password and security question by verifying his/her identity through SMS OTP.
- If customer has submitted application and the bank account is not opened yet, customer can only reset NCB e+ Password and security question by cancelling the account opening application after verifying his/her identity through SMS OTP.
- If customer has submitted application and the bank account is already opened, customer is not allowed to reset NCB e+ Password and can only view bank account information by contacting customer service in the online chatroom or by visiting the branch.

Security tips for WeChat official account

In order to ensure the services and information are provided by the Bank, please refer to the Bank's registered WeChat ID "NCB_HK" when searching for the WeChat official account. Please do not disclose your personal and account information to any unauthorised WeChat account(s). Should you have any queries, please contact the Bank's staff immediately.

Points to note when using WeChat official account

- When performing account binding, user is required to set up an 8-digit “WeChat password” of which three or more consecutive numbers and “12345678” are not accepted. User should take necessary prudential measures to safeguard your password, please do not disclose your password to anyone (including the Bank’s staff).
- Please do not access WeChat official account via hyperlinks or QR Code embedded in any emails or SMS.
- Please do not input personal sensitive information into WeChat dialogue box. The Bank will not ask user to provide account number, password and personal information via WeChat dialogue box.
- For more details of account binding, please input "Account Binding Service Directory" into WeChat dialogue box for enquiry.
- For enquiry, security issues report and unbinding account request, please call：+852 2622 2633
- To ensure customer data security, the recommended operating systems and browsers are as follows:
  - iOS 8.2 or above (Default browser), WeChat 6.3.18 or above
  - Android 5.0 or above (Default browser), WeChat 6.3.18 or above
- Please download and install updates and patches for your Apps, operating systems and browsers regularly.

Security tips for ATM and ATM Card

Protecting your ATM Card and PIN

- Please keep your ATM Card in a safe place, destroy the original printed copy of the PIN and memorise your PIN and change it regularly.
- Do not write down or record the PIN without disguising it. Please avoid writing down the PIN on the ATM Card or on anything usually kept with or near it under any circumstances.
- For security reasons, you are advised not to use your identity card number, date of birth, telephone number, commonly used combinations of numbers (e.g. 123456) or other easy-to-guess numbers as your PIN. You are also advised not to use the same PIN to access other services, including internet banking or other websites.
- Please do not allow anyone else to use your ATM Card or PIN.
- Please note that the police and bank staff will never ask you for the PIN. Do not disclose your PIN to anyone under any circumstances.
- Before using an ATM, please check if the keypad cover is abnormal (has been removed or installed with imaging facility), also if there are any suspicious devices near the card slot and keypad. If you notice anything suspicious, please notify the related bank immediately.
- Please cover the keypad with your hand when entering your PIN at ATM or Point-of-Sale devices and make sure no one is looking over your shoulder or standing next to you.
- The Bank will send you security messages by either text messaging or other form of alert under certain circumstances. Please check once received.
- You should promptly report any notice or suspicion loss, theft, disclosure or unauthorised use of your ATM Card and/or PIN by calling our 24-hour ATM Card Service Hotline at (852) 2616 6266
  .

Exercise Care at ATM Withdrawals

- Please avoid being distracted when withdrawing cash so as not to leave banknotes and your ATM Card at an ATM unattended or uncollected. Print a receipt for record and count the banknotes immediately after each cash withdrawal.

- Do not remove from an ATM dispenser any uncollected banknotes and ATM Card at the card insertion slot left behind by a previous user. The banknotes and ATM Card will be automatically retrieved by the machine after a designated period of time.

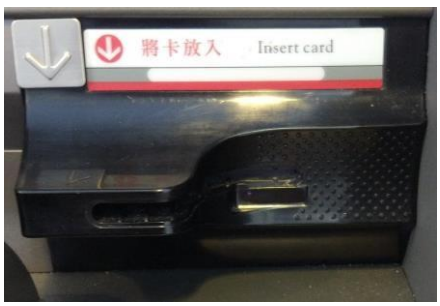
Beware of ATM Card Fraud

ATM Card fraud begins with the theft of either an ATM Card or its data: name, card number, expiration date, and verification/CVV code. Fraudsters commonly acquire card details online via malware, phishing emails, phishing website, or sometimes from ATM Card-related letters thrown in the bin. Please shred ATM Card-related letters before disposing of them. If you find that your ATM Card(s) have been stolen or that any unauthorised operations have occurred, you should contact us immediately, or directly contact the Hong Kong Police Force.

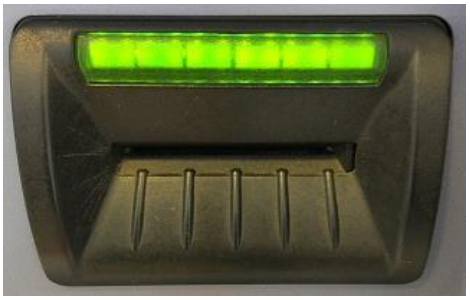
Safe Use of Overseas ATMs

- To use your ATM Card to withdraw cash from an overseas ATM on the "UnionPay" network will incur a handling fee of HKD / RMB 50 for each such cash withdrawal. Please visit "UnionPay" website www.unionpayintl.com/hk/ to find out more about overseas ATM locations and if ATM network(s) in your intended overseas destination can provide the cash withdrawal service you require.
- The overseas ATM daily withdrawal limit of each ATM Card is preset at 'zero' HKD to improve its security. You must therefore activate the ATM cash withdrawal function in advance and before you leave Hong Kong by setting the daily withdrawal limit and the validity period through the relevant designated channels to enable you to enjoy cash withdrawal service outside Hong Kong. Designated channels are: Internet Banking / Mobile Banking / Bank ATMs / 24-hour ATM Card Service Hotline (852) 2616 6266
- Please visit Notice of Enhanced Security Measures for Automatic Teller Machine ("ATM") Services outside Hong Kong (www.ncb.com.hk/nanyang_bank/popup1/ncb_esm_eng.html) for details.

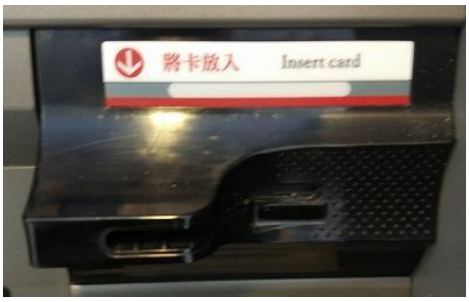
The normal card slot of ATM



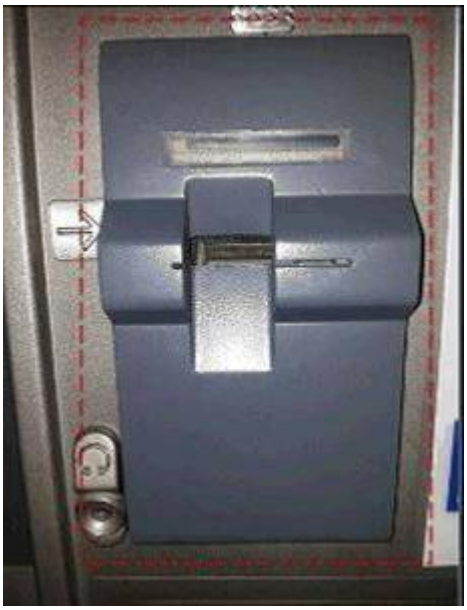
The normal card slot of Cheque Deposit Machine



The normal card slot of Cash Deposit Machine



An unusual card reader installed at the card slot



Two Factor Authentication

Two-factor Authentication Tools

To enhance online security, the Internet Banking and Mobile Banking Services of the Bank provides customers with a "Security Device" and "Mobile Token" as the two-factor authentication tools. "Security Device" with audio capability is also provided for the convenience of the visually impaired using Internet/Mobile Banking. Customers are required to use the "Security Device" or "Mobile Token" and agreement to receive specified transaction notification to conduct online Designated Transactions. For details of Designated Transactions Secured by the Two-factor Authentication on Internet and Mobile Banking, please visit the Bank's website "e-Banking Services > Two-factor Authentication".

In addition, corporate customers can apply the "Security Device" through Internet Banking or at any of our branches.

Mobile Token

"Mobile Token" is a built-in function of NCB Mobile App. Once the "Mobile Token" is activated, you will be spared the hassle of carrying a separate physical "Security Device" to truly enjoy convenient and secure banking.

Upon activating the "Mobile Token" on compatible mobile device, you can confirm designated Mobile Banking transactions or designated investment transactions via the preset passcode or using "Biometric Authentication". In addition, you can also confirm designated Internet Banking transactions by generating a one-time "Security Code"/"Transaction Confirmation Code" via the "Mobile Token".
Points to Note for “Mobile Token”:

- For security reasons, customer can only activate “Mobile Token” on one mobile device and please do not login Mobile Banking and activate "Mobile Token" on others’ mobile phone.
- For personal customers, upon successfully activation of “Mobile Token”, the “Security Device” (if any) will be suspended. For reactivation of “Security Device”, customers are required to suspend the “Mobile Token” on your mobile device.
- “Mobile Token” is not applicable for Corporate customers.
- Please keep your mobile device that has activated “Mobile Token” function in a safe and secure place. In case of loss or damage, please suspend the “Mobile Token” and contact us immediately or deactivate the “Mobile Token” through another device “Login to Mobile Banking > Menu on the left> Setting > Mobile Token Setting > Suspend Mobile Token”
- When you activate or suspend Mobile Token, your login setting of Personal Internet Banking with two-factor authentication will be deactivated immediately. You will need to reactivate by selecting "Setting > Security Setting > Login Setting" from the menu via Personal Internet Banking.

Biometric Authentication

You can register "Biometric Authentication" (e.g. Fingerprint, Face ID) on your mobile device for the following services when you activate the "Mobile Token":

- Log in Mobile Banking
- Enable the "Mobile Token" to confirm designated Mobile Banking transaction
- Enable the "Mobile Token" to generate a one-time "Security Code"/"Transaction Confirmation Code" to confirm designated Internet Banking transactions.

To learn how to activate the "Mobile Security Code", operating system requirements and compatible mobile devices, please visit: www.ncb.com.hk/1/etoken

Please ensure proper protection of your biometric authentication information, including but limited to fingerprint(s), facial feature(s) or any other biometrics as recognised by the Bank from time to time, and ensure the confidentiality of the security codes as well as the password that you use to store your biometric credential(s) and register the biometric authentication on your designated mobile device. If you have found or suspected your biometric credential(s) has/have been compromised, please contact us immediately, or directly contact the Hong Kong Police Force.

Security Device

Application for the "Security Device" can be made through our Internet Banking, at any of our branches or via Customer hotline. Upon receipt of customers' application, we will send the "Security Device" to customers' registered correspondence address.

Please be reminded of the following when you use the "Security Device":

- You are required to register your mobile number and activate the two-factor authentication function before applying for a "Security Device". Please visit any of our branches to complete the procedures.
- Upon receipt of the "Security Device", please log into the Internet Banking immediately and follow our online instructions to activate the "Security Device".
- No extra software / driver or authorisation code generated by a third party is required.
- Customers can choose to log into the Internet Banking by entering a one-time Security Code generated by the "Security Device" to enjoy extra protection for banking online.
- Customers are required to enter specific transaction information (e.g. registered account number) into the "Security Device" to generate a one-time Transaction Confirmation Code for Designated Transactions.
- Please keep your "Security Device" in a safe and secure place. You should not allow anyone to use your "Security Device" or leave it unattended. In case of loss or damage, please contact our staff immediately.

How does the "Security Device" work?

- Each "Security Device" contains a unique serial number, internal information and a clock. Once the "Security Device" is activated, the internal clock will synchronise with our system. When you press the button on the "Security Device", a one-time Security Code will be generated according to the information and clock inside the Device. The Code, for verifying the identity of customers, is valid within a short time interval. If the time permitted for the entry of the Security Code expires, you have to press the button again to generate another Security Code.

How do I use the "Security Device"?

- Different Security Codes will be generated by the "Security Device" depending on the nature of transactions. Customers should follow online instructions to complete authentication procedures.
  - When logging into the Internet Banking or performing general transactions, you should press the button at the bottom right hand side of the "Security Device". A 6-digit Security Code will be displayed on the LCD screen of the "Security Device". The Security Code, valid within a short time interval, is for one-time use only.
  - When performing "Designed Transactions", you should press the button at the bottom left hand side of the "Security Device" and enter the digits highlighted in RED online into the number keys of the Device. After you have input the required information, please press the left button at the bottom again. A 6-digit Transaction Confirmation Code will be displayed on the LCD screen of the "Security Device". The Transaction Confirmation Code, valid within a short time interval, is for onetime use only.

I have entered the "Security Code" or "Transaction Confirmation Code" into Internet Banking, but my transaction instruction cannot be verified. Why?

- Your transaction instruction may not be verified by Internet Banking due to the following reasons:
  - Entry of incorrect code
  - The time permitted for entry of the code has expired
  - The "Security Device" has been hit or exposed to heat, cold or wet conditions or magnetic fields

- Please follow our online instruction and enter a valid "Security Code" or "Transaction Confirmation Code". If your transaction instruction still cannot be verified, please contact our staff to reset the status of your "Security Device".
- In case the verification process is still not successful after resetting of the device's status, Customers can apply to replace a "Security Device" and it will be free of charge.

What if the message "BATT" is displayed on the LCD screen?

- "BATT" means that the "Security Device" will soon run out of battery. The battery normally lasts for 3 to 5 years, depending on the frequency of your usage. Personal customers must visit any of our branches to apply for replacement. Application can be made online by corporate customers. Please note that the battery of the "Security Device" cannot be replaced. Any attempt to remove the components of the "Security Device" may cause malfunction of the Device.

OTP for activation of "Security Device" and "Notification of Execution of Designated Transactions"

- The Bank's SMSs (if any) in respect of "OTP" and "Notification of Execution of Designated Transactions" will be sent only to your mobile phone number registered with the Bank. Such SMSs will not be forwarded to any other mobile phone number even if you have enabled the "SMS Forwarding Service" provided by any the following local mobile phone service providers in Hong Kong:
  - SmarTone Mobile Communications Holdings Limited
  - CSL Limited
  - Hutchison Telephone Company Limited
  - China Mobile Hong Kong Company Limited
- You are advised to check carefully the transaction details sent by the Bank through an SMS and an email against the transaction conducted by you via the Internet Banking/Mobile Banking. Please contact us immediately if you have any enquiry.

FAQ

What is 128-bit SSL encryption?

- Our Internet Services have adopted 128-bit SSL encryption, one of the online security standards for commercial application. All data transmitted via the Internet Services are protected by this technology to ensure data security.

What precautions should I take when I set up my password?

- Do not use your date of birth, ID / passport number, telephone number or any combinations of your English name as your password.
- Do not use 3 or more consecutive identical alphabets or digits, e.g. "333", "bbb" etc.
- Do not use sequential alphabets or digits, e.g. "123", "abc, etc.
- Do not use your user name / login ID as your password.

How often should I change my password?

- You are advised to change your password regularly. If you have not changed your password over certain period of time, our system will remind you automatically.

How can I protect my personal information?

- You may be asked to provide personal information (such as your ID / passport number and date of birth) as additional identity verification when you use the internet banking service. Be vigilant and do not casually disclose your personal information to anyone. You should also keep documents (such as letters and bank statements) which carry your personal information in a proper and secured manner.

Why should I update my operating systems and browsers regularly?

- It helps to fix security problems of the operating systems or web browsers if you update and download "patches" provided by software vendors regularly. This helps to prevent your computer from virus attacks or unauthorised access from hackers.

How can I set up the security settings of Wireless LAN?

- Do not place the Access Point ("AP") too close to doors and windows to avoid data captured and decrypted by any third party.
- Take appropriate security measures to protect the Wireless LAN. Do not disclose the security setting of your wireless network to any third party.

Precautionary measures for using internet?

- Encrypt your data if you have to keep your personal information in an electronic storage medium to prevent unauthorised access or use by third parties.
- Do not save or keep your password in your browser and disable the "Auto-Complete" setting to prevent third parties from accessing your information via the browser.
- Disable the "File and Printer Sharing" function of the Windows system and set up proper access permissions of your computer to prevent unauthorised access to your data by third parties via the network.
- Do not download or install illegal or unknown softwares to prevent infection from computer virus or Trojan programmes. Remember to scan for virus before opening any files from external sources.

Where can I obtain more information on precautionary measures for Internet Banking and ATM Services? ★

Hong Kong Monetary Authority – SMART TIPS ON USING INTERNET BANKING SERVICES
https://www.hkma.gov.hk/eng/smart-consumers/internet-banking/#using-internet-banking-services

- Hong Kong Monetary Authority – SMART TIPS ON USING AUTOMATED TELLER MACHINES
  https://www.hkma.gov.hk/eng/smart-consumers/atms/
- The Hong Kong Association of Banks "Internet Banking"
  https://www.hkab.org.hk/DisplayArticleAction.do?ss=17&lang=en&sid=5
- Hong Kong Police Introduction to Cyber Security and Technology Crime
  https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/
- Office of the Government Chief Information officer – "The InfoSec Web Site"
  https://www.infosec.gov.hk/en/

Hotline and websites

-	Customer Services Hotline	(852) 2622 2633
-	24-Hour ATM Services Hotline	(852) 2616 6266
-	24-Hour Security Incidents Hotline	(852) 2850 1100 (Electronic Banking)
-	Website	www.ncb.com.hk
-	Personal Internet Banking	pib.ncb.com.hk/login/nanyang/ibs_lgn_index_e.jsp
-	Corporate Internet Banking	cib.ncb.com.hk/login/cib_login043_e.jsp