Online Security Tips and Information

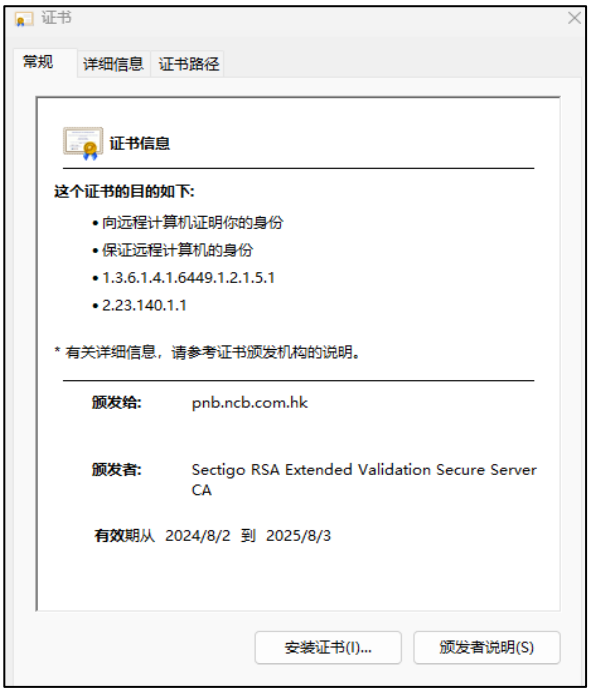
What Have We Done to Protect You

- We have adopted the 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 Internet Banking and Mobile Banking service are protected by multiple cybersecurity protection schemes 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 e-Banking Service will be suspended immediately.
- The Bank provides customers with the log enquiry function over the Internet Banking (Personal and Corporate); for example, customers can check the recent login records after logging in Internet Banking which covers the login date and time, the geographical location and the browser information, and that shall facilitate early detection of unauthorised e-banking activities.
- The e-Banking 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 Banking Services will be automatically disconnected when customers try to login to one's Mobile Banking after he/she has already logged to the Internet Banking.
- The e-Banking Services of the Bank provides customers with "Mobile Token" and "Security Device" as two-factor authentication tools. For details, please refer to Two-factor Authentication Tools.
- To ensure you can receive our notification messages for the security of your e-banking transactions, if you changed your contact information (such as email address or personal address), please login to your Internet Banking "Setting >

Update Customer Information", to change your personal information with Two Factor Authentication. If you need to update your contact information such as mobile phone number, please visit any of our branches for registration.

Security Certificate

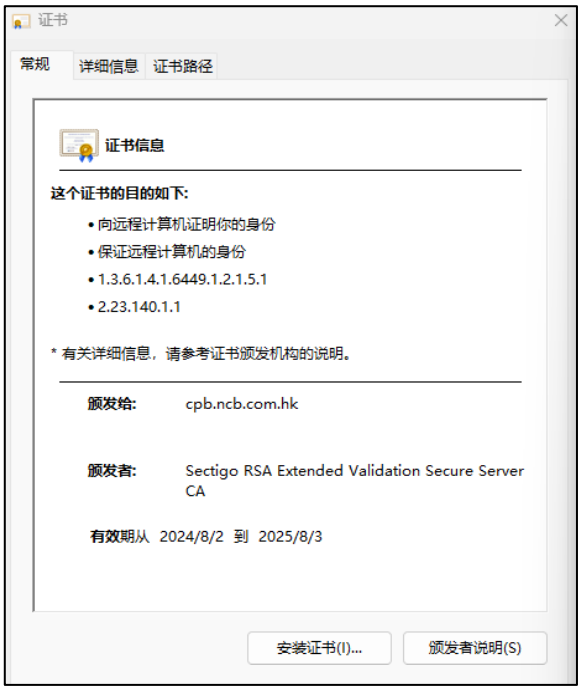
- We use Extended Validation ("EV") SSL Certificate to allow customers to verify the authenticity of our websites by checking the address bar of your browser. The address bar is green for browsers of Microsoft Internet Explorer Version 9 or above which is one of the security features of EV SSL. For browsers 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 Sectigo, the issuer of the certificate.



Personal Internet Banking

Domain name issued to: pnb.ncb.com.hk

Issued by: Sectigo RSA Extended Validation Server CA



Corporate Internet Banking

Domain name issued to: cpb.ncb.com.hk

Issued by: Sectigo RSA 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**
  - Google Chrome (Version80 or above)
  - Mozilla Firefox (Version 72 or above)
  - Microsoft Edge (Version 14 or above)
  - Apple Safari (Version 10 or above)
- **Corporate Internet Banking**
  - Google Chrome (Version 80 or above)
  - Mozilla Firefox (Version 72 or above)
  - Microsoft Edge (Version 14 or above)
  - Apple Safari (Version 10 or above)

Information Security Tips

Beware of fraudulent website

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

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 e-Banking 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 reliable channels (e.g. official telephone or fax number, 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.

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.

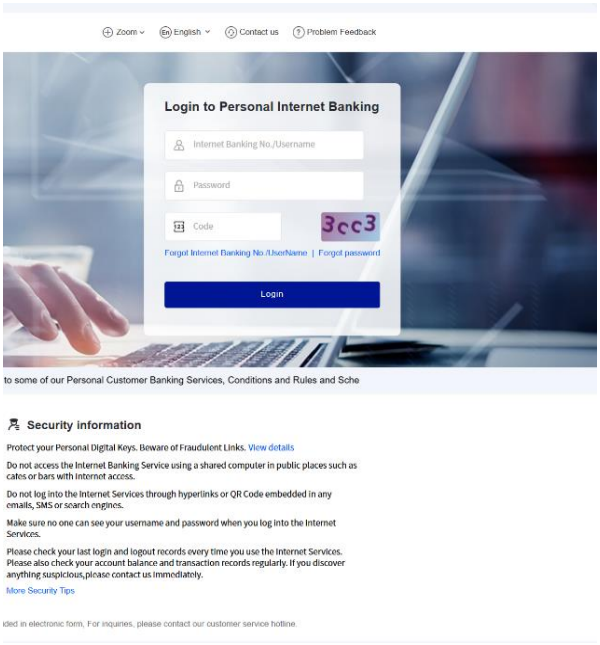
Man in the Browser Attack

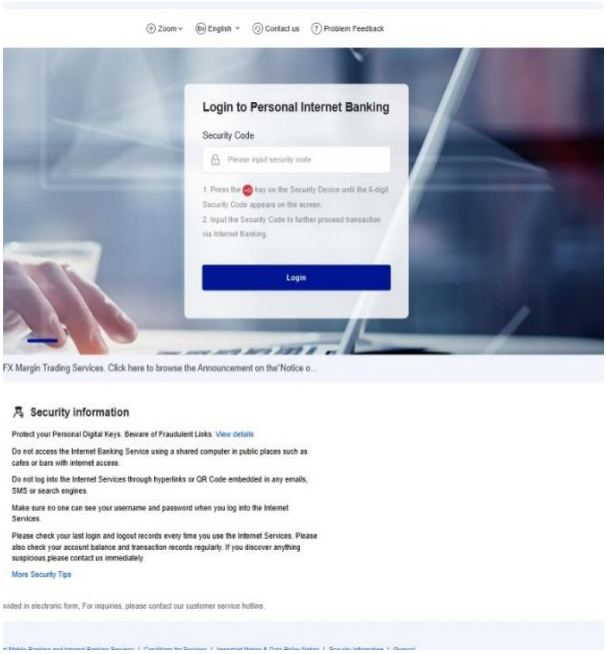
- The suspected Trojan Horse cases have been reported by few corporate customers when they used the corporate internet banking service. During the login process, a fake webpage was displayed requesting the customers to input their login names and passwords, as well as the one-time transaction confirmation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

Please refer to the following login pages of Internet Banking and Mobile Banking service

- **Personal Internet Banking Login**

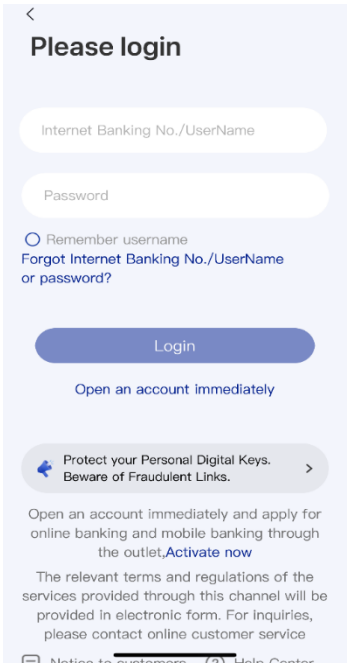
Customer with Security Device or Mobile Token must log in to Internet Banking with two-factor authentication. Input the Internet Banking No. / User Name, password and verification code, and press "Login". Then enter one time "security code" generated from "Security Device" or "Mobile Token.



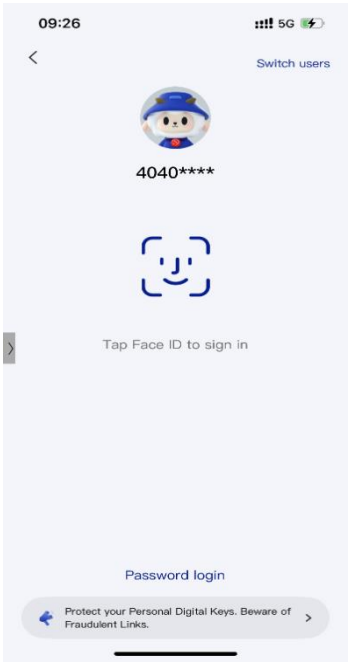


- **Personal Mobile Banking Login**

Input the Internet Banking No. / Username, password and verification code, and press "Login".

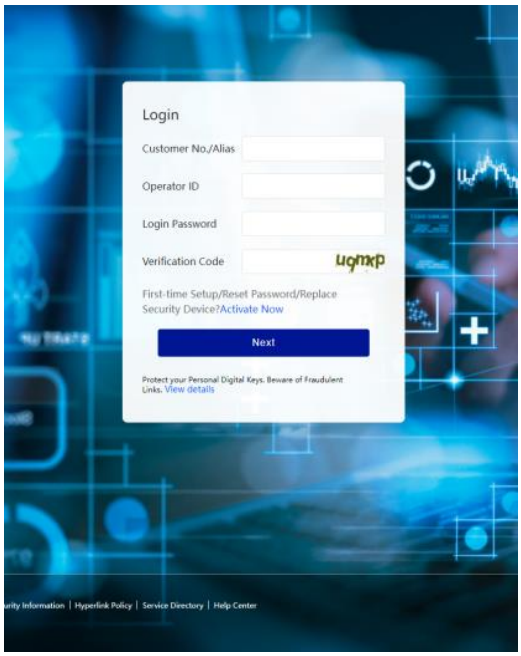


Customer may select "Biometric Authentication" for login.

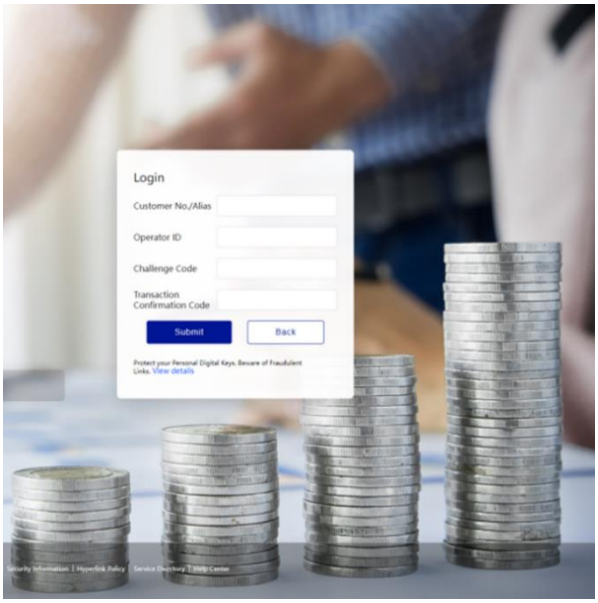


- **Corporate Internet Banking Login**

Enter Customer Number/Alias, Operator ID, Password and Verification Code to login.

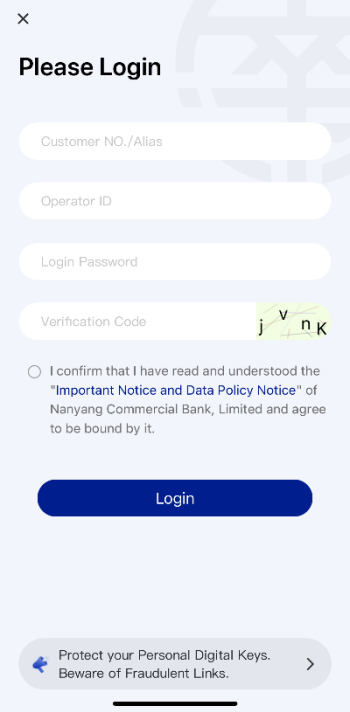


For customers who had enabled "2FA Login", customer shall obtain a "Transaction Confirmation Code" for login by entering the "Challenge Code" on "Security device".

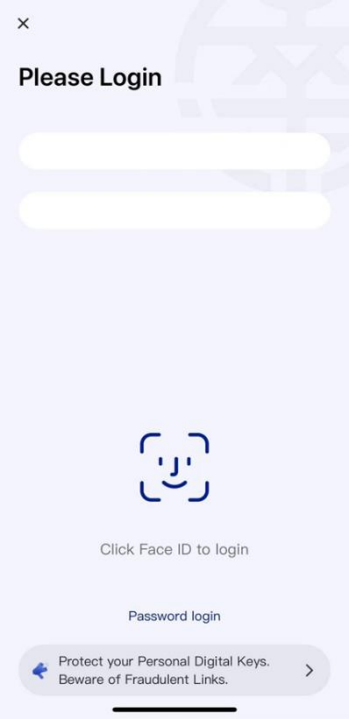


- **Corporate Mobile Banking Login**

Enter Customer Number/Alias, Operator ID, Password and Verification Code to login.



Customer may choose "Biometric Authentication" for login.



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 in various ways.
- Grammatical mistakes, typos or misspelling is found in the content of the phishing emails, SMS and/or instant messages sent from fraudsters.
- 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.

Your password and personal information should be well protected

- Please memorise your password. Do not write or store the password on any of the devices used for the e-Banking 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 or login information, 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 e-Banking 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 e-Banking 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) or activities 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 and e-Banking activity records via the e-Banking Banking.

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.

Take precautionary measures while you are using e-Banking Service

- Do not access the e-Banking Service using a shared computer (or shared mobile device) 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 e-Banking 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 Banking Services.
- Make sure no one can see your user name and password when you log into the e-Banking Services.
- Please check your last login and logout records every time you use the e-Banking 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.
- Please review your services' limits regularly and to make necessary adjustment (such as lowering fund transfer limits) that suits your own safeguard needs.