# Security Zone

To facilitate enhanced protection on your e-banking security and protect customers against evolving digital fraud risks, the bank will implement enhanced security measures in alignment with the Hong Kong Monetary Authority's new anti-digital fraud initiative "E-Banking Security ABC" launched in 2025. These will provide you with enhanced assurance on your e-banking services.

## What is "E-Banking Security ABC"?

### A – Authenticate in-App

When you log in to Mobile Banking for the first time or log in with an unbound mobile device, you must complete the security settings via facial recognition or other two-factor authentication methods:

- Activate Device Binding
- Activate Mobile Token

When you log in to Internet Banking or authorize designated transactions*, Mobile Token/ Security Device will replace SMS One-Time Password (OTP) to serve as two-factor authentication tool for transaction authorization.

*Designated transactions include but not limited to:

- Reset Password
- Investment Service
- Transfer to an unregistered payee
- Registering Payee
- Increase the transaction limit
- Register Small-Value Fund Transfer
- JETCO Cardless Withdrawal Service
- Update Customer Information
- NCB WeChat Account Binding Service

**B – Bye to unused functions**

You can choose to disable two higher risk functions anytime via Mobile / Internet Banking:

- Online registration of third-party payees service
- Online increase of transfer/remittance limits service

**C – Cancel Suspicious Transfers**

In case you are initiating fund transfer to suspicious accounts, an anti-fraud alert will pop up and display for a period of time, which provides you with more time to review the stated risks of the transaction.

## Security Upgrade Tailored for You—More secure Internet Banking services

### ☑ "Two-Step" for Security Setting

Step 1: Activate Device Binding

- You can have only 1 bound device as trusted device.
- Complete authentication with facial recognition or other authentication methods, instead of SMS One-Time Password (SMS OTP). By adopting more stringent authentication method, you may enjoy a higher level of security.

Step 2: Activate Mobile Token

- By activating Mobile Token on your frequently used mobile device, authenticate your transactions anytime, anywhere.
- If you have not yet applied for a Security Device as the two-factor authentication tool, please activate Mobile Token now, which allows you to authorize transactions in a more convenient way.

Note:

i. The device binding and Mobile Token take 6 hours to become effective upon successful authorization. Afterwards, customers may authorize transactions with the Mobile Token serving as the two-factor authentication tool. Within the aforementioned 6-hour period, Mobile Banking services remain. A cooling-off period allows you to have sufficient time in reviewing and detecting suspicious e-Banking account activities. Risk of suffering loss can then be reduced.

ii. Subject to the need for security control measures, customers may be required to enter an SMS One-Time Password (OTP) for transaction authorization.

## ☑"Enhanced Protection" on Internet Banking Login

Customers with a Mobile Token/ Security Device must log in to Internet Banking with two-factor authentication. By taking an extra step for logon, you may enjoy a high level of security.

## ☑"Designated Transaction Authentication "Level Up"

Mobile Token/ Security Device will replace SMS One-Time Password (OTP) to serve as the two-factor authentication tool for authorizing designated transactions, which helps prevent your SMS from being phished and intercepted.

## ☑Bye to Higher risk functions

You may deactivate the online registration of third-party payees service and the online increase of transfer/remittance limits service at any time via Mobile Banking/ Internet Banking.

# Security Upgrade Tailored for You—More secure Internet Banking services

## ☑"Two-Step" for Security Setting

### 1st Activate Device Binding

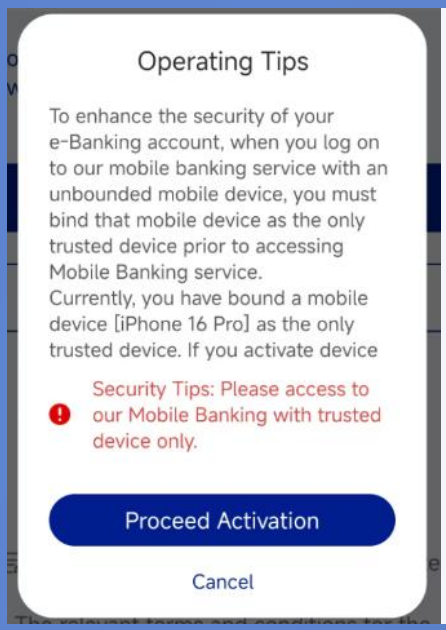
You must activate the device binding through the following default authentication methods according to the types of identity documents they had used for account opening:

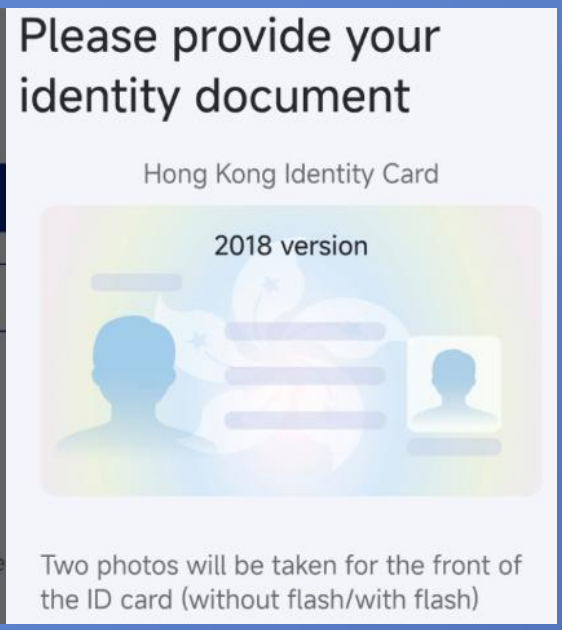
- **Holder of Hong Kong Identity Card:**

Step1: After logging on to the Mobile Banking via a new mobile device, click "Proceed Activation" according to the on-screen instruction

Step2: Capture the front of your Hong Kong Identity Card. (Go to Step 3 if you had once completed relevant identity document verification via our Mobile Banking successfully).

Step 3: Take a selfie for verification. After completing the facial recognition authentication, the device binding activation is then complete.

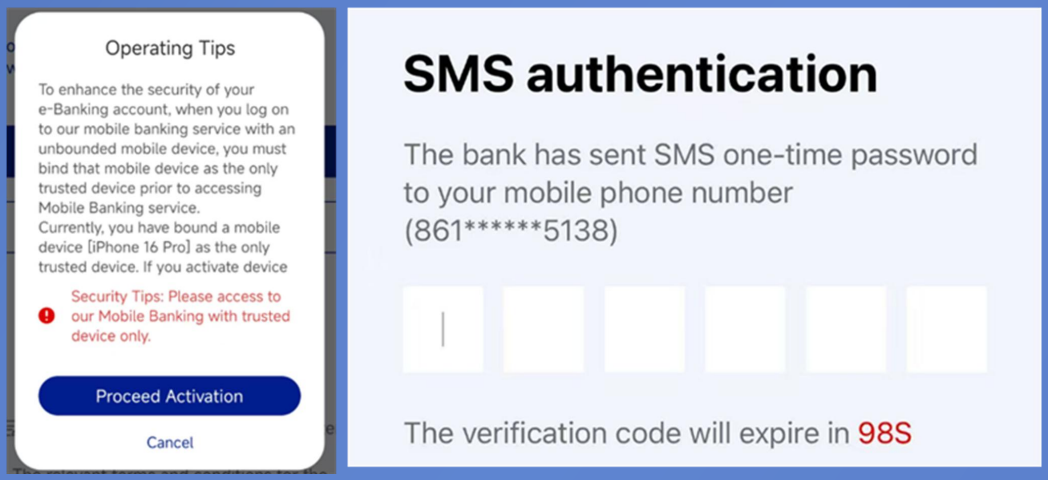


- **Holder of the People's Republic of China Resident Identity Card:**

Step1: After logging on to the Mobile Banking via a new mobile device, click "Proceed Activation" according to the on-screen instruction.

Step2: Input SMS One-time password for authentication. The device binding activation is then complete.

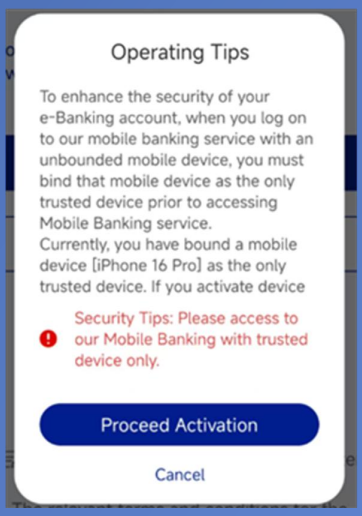


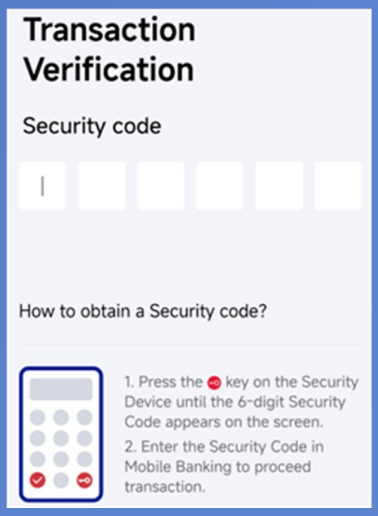

- **Holder of other identity documents:**

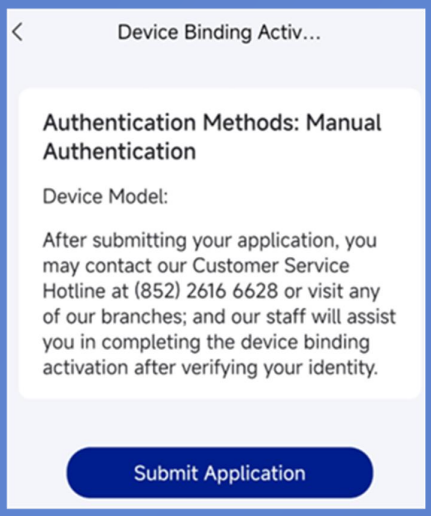
Step1: After logging on to the Mobile Banking via a new mobile device, click "Proceed Activation" according to the on-screen instruction.

Step2: If you have a security device, enter the 6-digit security code generated by the security device for authentication. The device binding activation is then complete.

If you do not have a security device, you are required to undergo the manual authentication process. Click "Submit Application" according to the on-screen instruction. Then you may contact our Customer Service Hotline at (852) 2616 6628 or visit any of our branches. Our staff will assist to complete device binding activation after verifying your identity.




Note:

i. If our Bank's facial recognition technology cannot verify your identity online, please contact our Customer Service Hotline or visit any of our branches for assistance. Our staff will assist to complete device binding activation after verifying your identity.

ii. If you fail the online identity verification for five times or above, you are required to complete device binding activation with manual authentication method. Upon submitting relevant request, you may then call our customer service hotline at (852) 2616 6628 or visit any of our branches for assistance. Our staff will assist to complete device binding activation after verifying your identity.

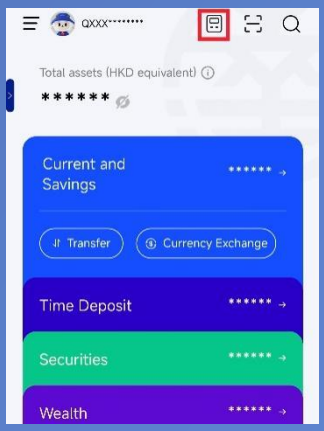
iii. If customers bind a new mobile device as a trusted device, the soft token of the old mobile device (if activated) will be automatically deactivated. Customers need to activate the soft token with the new mobile device again and it will take 6 hours to be effective.

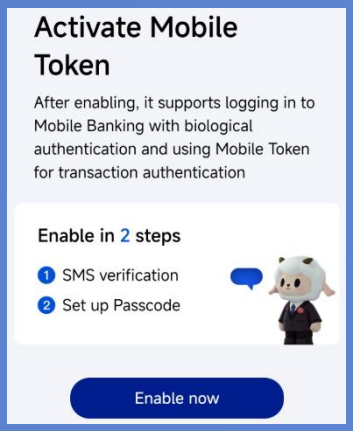
## 2nd Activate Mobile Token

By activating Mobile Token on your frequently used mobile device, authenticate your transactions anytime, anywhere.

Step 1: After logging on to the Mobile Banking via bound device, click the "Mobile Token" at the upper right corner of the home page.

Step 2: Click “Enable now” and follow the default authentication methods for identity verification according to the types of identity documents they had used for account opening.




More preferred on physical security device? Check out here to apply for a  Security Device!

Method 1: Apply in person at any branch and you can obtain the “Security Device” immediately.

Method 2: Apply for the “Security Device” through the Customer Service Hotline (852) 2616 6628, and the Bank will mail the Security Device to your registered mailing address with the Bank. Please allow approximately three weeks for delivery. (Actual delivery time may vary)

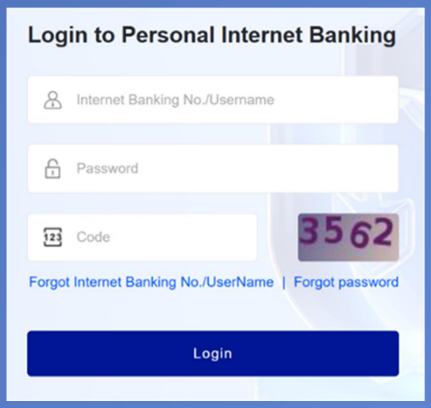
## ☑ Enhanced protection on Internet Banking Login

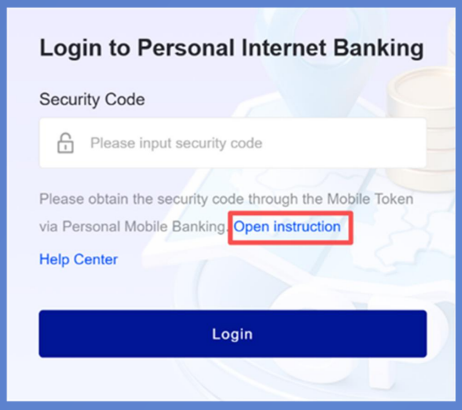
Customers with a Mobile Token/ Security Device must log in to Internet banking with two-factor authentication.

Step 1: Input the Internet Banking No./Username, password, and verification code, then click “Login.”

Step 2: Input the one-time security code generated by Security Device or Mobile Token, then click “Login.”

Step 3: After completing the verification, you can log in to use Internet Banking services.

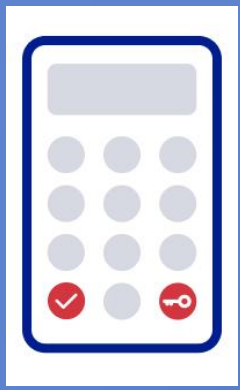


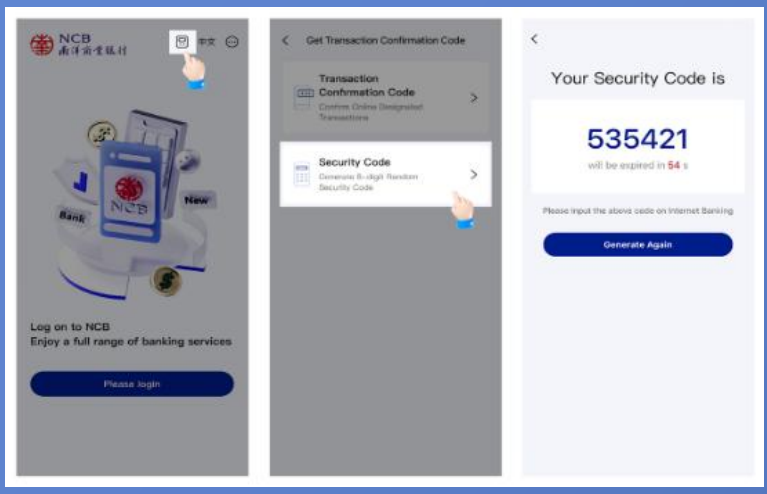

## ☑ Designated Transaction Verification "Level Up"

Mobile Token/ Security Device will replace SMS One-Time Password (OTP) to serve as the two-factor authentication tool for authorizing designated transactions, which help prevent your SMS from being phished and intercepted.

If you have enabled Security Device, you may press the button at the bottom right corner of the Security Device. A 6-digit security code will then be displayed.



If you have enabled Mobile Token, you may open the Personal Mobile Banking App using the bound device (without proceeding login);click the "Mobile Token" at the upper right corner of the home page. By clicking "Security Code", a 6-digit security code will then be displayed.



## ☑ Bye to Higher risk functions

You may deactivate the online registration of third-party payees service and the online increase of transfer/remittance limits service at any time via Mobile Banking/Internet Banking.

- Deactivate the online registration of third-party payees service

1) Customers firstly activate Internet Banking services:

Mobile Banking
By accessing to login page of Personal Mobile Banking, select "Activate now". Check the box for "Deactivate the online registration of third-party payees service " on "Setup Account Details" page. After reading the warm reminder, select "Confirm" and proceed to identity verification. The concerned function is then deactivated.

Internet Banking
By accessing to login page of Personal Internet Banking, select "Activate Now". Check the box for "Deactivate the online registration of third-party payees service" on "Setup Account Details" page. After reading the warm reminder, select "Confirm" and proceed to identity verification. The concerned function is then deactivated.

2) Customers have already activated Internet Banking services:

Mobile Banking
By logging in to Personal Mobile Banking, select "All Functions" > "Registered Payee". Select "click here" at the alert message for function deactivation. After reading the warm reminder, select "Confirm" and proceed to identity verification. The concerned function is then deactivated.

Internet Banking
By logging in to Personal Mobile Banking, select "Transfer/Payment" > "Manage Registered Payee" > "Manage Registered Payee". Select "click here" at the alert message for function deactivation. After reading the warm reminder, select "Confirm" and proceed to identity verification. The concerned function is then deactivated.

Warm Reminder: Please note that after successfully deactivating the concerned service, you must visit our branch in person to complete the relevant verification procedures before you can complete (1) Registration of third-party payees service or (2) Reactivation of the concerned service.

- Deactivate the online increase of transfer/ remittance limits service

1) Customers firstly activate Internet Banking services:

Mobile Banking
By accessing to login page of Personal Mobile Banking, click "Activate Now". Check the box for "Deactivate the online increase of transfer/ remittance limits service" on "Setup Account Details" page. After reading the warm reminder, select "Confirm" and proceed to identity verification. The concerned function is then deactivated.

Internet Banking
By accessing to login page of Personal Internet Banking, click "Activate Now". Check the box for "Deactivate the online increase of transfer/ remittance limits service" on "Setup Account Details" page. After reading the warm reminder, select "Confirm" and proceed to identity verification. The concerned function is then deactivated.

2) Customers have already activated Internet Banking services:

Mobile Banking
Method 1: By logging in to Personal Mobile Banking, click "All Functions" > "Limit Management". Select "click here" at the alert message for function deactivation. After reading the warm reminder, select "Confirm" and proceed to identity verification. The concerned function is then deactivated.

Method 2: By logging in to Personal Mobile Banking, click "All Functions" > "Transfer Payment" > "Transfer" > "More Function" > "Small-Value Transfer Setting". Select "click here" at the alert message for function deactivation. After reading the warm reminder, select "Confirm" and proceed to identity verification. The concerned function is then deactivated.

Internet Banking

By logging in to Personal Internet Banking, click “Transfer/Payment” > “Transfer/Payment Setting” > “Transaction Limit” >“Transfer/Remittance” or “Small-Value Fund Transfer/Remittance”. Select “click here” at the alert message for function deactivation. After reading the warm reminder, select “Confirm” and proceed to identity verification. The concerned function is then deactivated.

Warm Reminder: Please note that the transfer/ remittance limits default as zero for newly activated e-Banking accounts. After successfully deactivating the concerned service, you must visit our branch in person to complete the relevant verification procedures before you can complete (1) Increase of transfer/ remittance limits service or (2) Reactivation of the concerned service. Online decrease of transfer/ remittance limit service remains.

Want to learn more?

Please refer to the Bank’s website>Personal Banking>e-Banking Services>Help Center

NCB 南洋商業銀行

中國信達全資附屬公司 Wholly owned subsidiary of China Cinda