NCB Security Tips

Upgraded Security Measures | Anti-Fraud Tips

Upgraded Security Measures You Should Beware Of “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 payments

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.

Anti-Fraud Tips

Beware of Fraudulent Calls, SMS, Emails

- Stay vigilant of any bogus calls, fraudulent websites, emails, SMS, mobile apps and social platform accounts purportedly to be from the Bank. You are also reminded not to rely solely on the incoming call display, email address, website address, SMS or message content to identify the caller/sender.
- The Bank will never ask you to provide sensitive personal information (including user name of your Internet/Mobile Banking, login passwords, one-time passwords, security codes and transaction confirmation codes), via phone calls, phone messages, emails, SMS, etc., nor notify you of account irregularities via pre-recorded messages.
- If in doubt, please contact our 24-hour Security Hotline at (852) 2616 6628(press “9” after language selection) for verification, or request the assistance through contacting the 24-Hour Enquiry Hotline 18222 of the Anti-Deception Coordination Centre, Hong Kong Police Force.

Beware of Phishing

- Avoid logging in to Internet Banking via wireless network (i.e., Wi-Fi) which is public or not protected with password.
- You should not log in to Internet/Mobile Banking through third-party websites/applications, hyperlinks, QR codes or attachments embedded in any emails, SMS or instant messages.
- Please download Personal Mobile Banking App and NCB e+ App through the official application stores (such as Google Play, App Store, and Huawei AppGallery HK, etc.). Do not download or install any applications from unknown sources. If in doubt, you should stop operation immediately.
- Unless you are assured that you are accessing to the Bank's website, you should not provide any particulars related to your Internet Banking services. If in doubt, please contact the Bank.
- Stay vigilant to anything abnormal when logging in to Internet Banking (e.g. unusual pop-up screens, unusually slow browser response, multiple requests for password input etc.). In case of any doubt, you should not follow the on-screen instructions nor enter any information. You are advised to close the browser and contact the Bank immediately.

Security Tips for Online Transactions

- Please check your account’s transaction activities and transaction notifications regularly, and contact the Bank immediately in case of any unauthorized transactions detected.
- You may call the Bank’s 24-hour Security Hotline (852) 2616 6628 when discovering any unusual or suspicious transactions/activities in your accounts, and request immediate suspension of your Internet Banking service.
- You should review your transaction limits regularly and make necessary adjustment (such as lowering fund transfer limits) that fit your security needs.
- Before entering authentication factor for transaction authentication, you should verify the transaction details carefully, such as transaction type, amount and currency, etc. In case of any enquiries, please contact the Bank immediately.

Security Tips for Authentication Factors

- Please change your login password regularly and set a strong password; and avoid using the same password for accessing other services.
- Please do not provide any sensitive personal information (including user name of your Internet/Mobile Banking, login passwords, one-time passwords, security codes and transaction confirmation codes) to anyone (including the Bank staff, the Police and callers).
- If you once shared your login password with third parties, please contact the Bank and change your password immediately.
- Please keep your authentication factor(s) (for example, login password and authentication token) properly. Do not write or save the password on any devices.
- To protect your ATM Card PIN, when entering PIN for accessing to Self Service Banking, please cover the keypad with your hand. If you notice any suspicious device, please do not use.
- If you have lost or disclosed your password/ authentication factor(s), or suspected that your password/ authentication factor(s) has/ have been used by an unauthorised party, or found any unauthorised transaction(s) associated with your account, please contact us immediately.

Want to learn more?

Please refer to the Bank's website>Security Information