Security tips for Mobile Banking

For details of mobile device malware scam please refer to Latest / Important Security Information

Notes for downloading Personal Mobile Banking Apps

- 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 (TLS). 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.
- We have obtained the certificate issued by Sertigo 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.
- The bank provides customers with the login records for Mobile Banking (personal and corporate); customers can check the recent login records after logging in Mobile Banking (for Personal Mobile Banking, please visit Security > Login Log; for Corporate Mobile Banking, please click “Me” on the main page), which covers the login time, the relevant geographical location and the device type, and that shall facilitate early detection of unauthorised e-banking activities.

Customer 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 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 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 (such as Google Play, App Store, and Huawei App Gallery HK, etc.) 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.

Notes for conducting transactions through Mobile Banking

- 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 after logging in Mobile Banking. 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 deleting the relevant data at your own discretion.

- If your fingerprint or Face ID record of your designated mobile devices has been changed, 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.