

18th December 2024

Beware of phishing messages and fraudulent websites
to safeguard your electronic banking account

Bank of China (Hong Kong) (“BOCHK”) would like to alert customers and the general public to phishing messages and fraudulent websites which are intended to steal personal information and electronic banking credentials.

Fraudsters recently purported to be genuine buyers in Online Trading Platform and sent out phishing emails messages embedded with fraudulent website hyperlinks or QR codes which purported to be from Online Trading Platforms / Courier Services for deliveries verification, deals closure or payments collection. These phishing emails messages made different false claims such as falsely claiming that courier services required customers’ information for verifying the deliveries, or the platforms required customers to log into electronic banking account for closing the deals and collecting the payments, etc., and lured customers to click on the embedded hyperlinks or scan the QR codes in the messages and enter personal and electronic Banking credentials (including Internet Banking usernames, bank card numbers, login passwords, one-time passwords or mobile tokens) in the fraudulent websites.

The hyperlinks of these fake emails / QR codes and fraudulent websites will appear under different domain names or with slight variations from the official website addresses by adding a similar combination of letters, numbers or symbols, with intent to mislead and steal customers’ personal and for swindling customers out of money.

BOCHK reiterates that we would not ask for sensitive personal information such as bank account details, Internet Banking usernames, bank card numbers, login passwords, one-time passwords or mobile tokens, through phone calls, phone call recordings, emails, SMS messages, hyperlinks, QR codes, attachments, etc.

The Bank reminds customers to be vigilant against possible scams:

- Please carefully protect your personal information and electronic banking credentials (including Internet Banking usernames, bank card numbers, login passwords, one-time passwords and mobile tokens), do not disclose your personal information, electronic banking credentials and passwords, including the SMS one-time password and mobile token.
- When logging in or conducting transactions through electronic channels,



customers are advised to access their Internet Banking or Mobile Banking accounts by typing the website address of BOCHK (www.bochk.com) directly into the browser address bar, or through the BOCHK Mobile Banking Application downloaded from official App stores or the Bank's official website.

- Do not open email, SMS messages, attachments or click on the hyperlink from unknown sources. In case of doubt, please stop the operation and do not input any data. Please close the window and contact the Bank immediately and provide the suspicious hyperlink or screenshot (if any).
- If customers have provided personal information to suspected fraudulent websites, please immediately contact the Bank's Customer Service Hotline at (852) 3988 2388 (press 3, # and 2 after language selection), and contact the Police.
- Review transactions record frequently through internet banking, mobile banking or statements to check if there is any suspicious or unauthorized transaction.
- Starting from 28 January 2024, BOCHK will use "Registered SMS Sender IDs" : #BOCHK 、 #BOCHK_TXN or #BOCHK_CC to send SMS messages regarding login/transaction to customers' registered mobile phone number.
- If unusual login/transaction is detected on customer's electronic banking account, BOCHK will send customer a two-way alert SMS (through any of the following phone numbers: +852 622649931110 or +852 645063570006) to customer's registered mobile phone number. Please carefully verify the details in the SMS, such as transaction time, currency and amount before replying to that SMS.
- If customer have logged in/made the transaction, please reply with "1" after verifying that the SMS content is correct. If customer have not logged in / made the transaction, or the SMS content is incorrect, please reply with "9". BOCHK will follow up per the response, including immediate suspension of the electronic banking transfer function after receiving the reply of "9". If customer receive that SMS overseas, please contact BOCHK immediately and do not reply that SMS.

BOCHK will update the fraud alerts on the Bank's website from time to time. For details, please visit www.bochk.com/en/aboutus/fraudalert.html. For more security information about our electronic banking services, please visit www.bochk.com/en/security.html.