中國銀行(香港)有限公司
BANK OF CHINA (HONG KONG) LIMITED

16th May 2023

Phishing Alert - Avoid Payment Card Scam

Bank of China (Hong Kong) ("BOCHK") would like to alert customers and the general public to phishing emails / SMS messages which are intended to steal personal information and payment card credentials (including credit cards and BOC cards).

Fraudsters recently sent out phishing emails or SMS messages embedded with fraudulent website hyperlinks which purported to be from Online Shopping Platform / Reward Scheme Platform / Postal Service / Courier Services / Government Departments / Banks for verification, reward redemption, refund, fee payment or information update. These phishing emails or SMS messages made different false claims such as falsely claiming that customers' information in the platform should be updated to continue the services, or customer's parcels could not be delivered and thus personal information should be updated or extra fee is required, or customer's account was overcharged or automatic payment failed and thus credit card information should be provided to handle immediately, etc., and lured customers to click on the embedded hyperlinks in the messages and enter personal and payment card information.

The hyperlinks of these fake emails / SMS messages 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. Senders' names appearing in the fake SMS messages may be as same as the genuine merchants, resulting in the fake SMS messages being displayed together with the previous SMS messages received from genuine merchants, with intent to mislead and steal customers' personal and payment card information for various illegal acts including **binding Mobile Payment & Services** for unauthorized local or overseas transactions, or to **directly use it on unauthorized online transactions**.

BOCHK reiterates that we would not ask for sensitive personal information such as bank account details, Internet Banking usernames, login passwords, one-time passwords or payment card numbers/security code, 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 payment card, personal information and payment

card information (including card number, expiry date, CVC code, SMS one-time password). Do not disclose your personal information, payment card credentials and passwords, including the SMS one-time password.

- Even though "AutoFill" function is available on mobile devices, before inputting the one-time password for any authorized transaction, please verify transaction details and message content carefully, such as merchant name, transaction type, transaction amount and currency, that whether it matches with the usage and the transaction.
- Ensure the website is genuine and reliable before inputting any information or conducting transaction.
- 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, or verify through official contact point of the genuine merchant.
- 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.
- If customers have received any suspicious message on binding Mobile Payment & Services or internet transaction, please contact the Police and the Bank immediately.
- Review transactions record of credit cards and BOC cards frequently through internet banking, mobile banking or statements to check if there is any suspicious or unauthorized transaction.
- If cardholders fail to take reasonable care to keep the credit card / BOC card, personal information and payment card credentials (including card number, expiry date, CVC code, SMS one-time password), or ignore BOCHK's transaction notifications, in accordance with the credit card agreement / credit card user agreement, terms and conditions, important notice of BOC ATM card and Conditions for Services, cardholders may be liable for the transactions and losses.

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.

The following are some examples on the screenshots of phishing SMS messages and fraudulent websites for reference:

中國銀行(香港)有限公司
BANK OF CHINA (HONG KONG) LIMITED

Phishing SMS Message:

Phishing Emails:

Bank of China (Hong Kong) Limited