

2 March 2021

### **Statement on phishing SMS messages and fraudulent websites**

Bank of China (Hong Kong) (“BOCHK”) would like to alert its customers and the general public that fraudsters recently sent out phishing SMS messages embedded with fraudulent website hyperlinks that purported to be from BOCHK. Those phishing SMS messages falsely claimed that customers’ account settings were abnormal or their verifications were unsuccessful etc, and requested customers to click on the embedded hyperlinks in the SMS messages and enter personal information, such as Internet Banking number/username, Internet Banking password and one-time password sent via SMS on the fraudulent BOCHK websites. BOCHK declares that it has no connection with the phishing SMS messages and fraudulent websites. Meanwhile, the case has been reported to the Hong Kong Monetary Authority and the Hong Kong Police Force.

In an attempt to mislead customers, the hyperlinks of these fraudulent websites will appear under different domain names or with slight modifications or variations of the official BOCHK website address [www.bochk.com](http://www.bochk.com) by adding a combination of letters, numbers or symbols, such as described below:

[https:// www.bochkee.com](https://www.bochkee.com)

[https:// www.bochkem.com](https://www.bochkem.com)

[https:// www.bochkeo.com](https://www.bochkeo.com)

[https:// www.bochkep.com](https://www.bochkep.com)

[https:// www.bochkeu.com](https://www.bochkeu.com)

[https:// www.bochkew.com](https://www.bochkew.com)

BOCHK reminds customers to be vigilant against possible scams. BOCHK reiterates that it will not request customers to provide any sensitive personal information, including account numbers, Internet Banking number/username, Internet Banking password and one-time password, through hyperlinks, QR codes or attachments embedded in SMS messages, e-mails or on websites, and will not contact customers via pre-recorded voice messages. Customers must not login to their banking accounts or provide personal information (including password) through SMS messages, e-mails, hyperlinks, QR codes or attachments. If customers receive any suspicious SMS message claiming to be sent by BOCHK requesting to click on the hyperlink to provide any personal information, please be alert and call BOCHK immediately to verify the authenticity of the SMS message.

When 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](http://www.bochk.com)) directly into the browser address bar, or through the BOCHK Mobile Application downloaded from official App stores or reliable sources. Customers should not access such accounts or provide personal information (including passwords) through hyperlinks, QR codes or attachments embedded in SMS messages, e-mails or on websites. 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](http://www.bochk.com/en/aboutus/fraudalert.html). For more security information about BOCHK's electronic banking services, please visit [www.bochk.com/en/security.html](http://www.bochk.com/en/security.html).

Anyone who has logged into the aforesaid fraudulent websites and provided their information should immediately contact BOCHK Customer Service Hotline at (852) 3988 2388 (press 3, # and 2 after language selection).

Below are the screenshots of the fraudulent websites (Chinese only):





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

登入香港網上銀行

已登記 / 辦理網上銀行服務

網上銀行號碼 / 用戶名稱

網上銀行密碼

驗證碼 **7865**

「交易驗證碼動碼」將於10分鐘內傳至您的手機！

確定 取消

登入

© 中國銀行(香港)有限公司。版權所有。 您的最佳選擇 YOUR PREMIER BANK

Bank of China (Hong Kong) Limited