

31 August 2023

### **Statement on fraudulent websites and phishing emails**

Bank of China (Hong Kong) Limited (“BOCHK”) would like to alert its customers and the general public to the following fraudulent websites and phishing emails, which purported to be from BOCHK.

Fraudulent websites:

[hxxps://lambdagolf.com/l/cn](http://lambdagolf.com/l/cn)

[hxxps://lambdagolf.com/l/en](http://lambdagolf.com/l/en)

[hxxps://agaogludericilik.com/g/cn/](http://agaogludericilik.com/g/cn/)

[hxxps://agaogludericilik.com/g/en/](http://agaogludericilik.com/g/en/)

[hxxp://todaysaccountant.com/alaire/cn](http://todaysaccountant.com/alaire/cn)

[hxxp://todaysaccountant.com/alaire/en](http://todaysaccountant.com/alaire/en)

[hxxps://nipm.gov.lk/shm/cn/](http://nipm.gov.lk/shm/cn/)

[hxxps://nipm.gov.lk/shm/en/](http://nipm.gov.lk/shm/en/)

[hxxps://mwt.kebbistate.gov.ng/token/auth/username.php](http://mwt.kebbistate.gov.ng/token/auth/username.php)

[hxxps://mwt.kebbistate.gov.ng/token/en/username.php](http://mwt.kebbistate.gov.ng/token/en/username.php)

[hxxps://www.bataguassu.ms.gov.br/token2/auth/username.php](http://www.bataguassu.ms.gov.br/token2/auth/username.php)

[hxxps://www.bataguassu.ms.gov.br/token2/cn/username.php](http://www.bataguassu.ms.gov.br/token2/cn/username.php)

Phishing emails:

WASSIN.DRIDI@ UIT.UNIVERSITY

wassim.dridi@ uit.university

khorton@ sgis.org

norbert@ itech-namibia.org

vincenzo.baniak@ sp2.slupsk.pl

siege@ captifs.fr

500047@ caraga.deped.gov.ph

llynes@ brownbagmarketing.com

00342257@ red.unid.mx

ESKATS@ REALI.ORG.IL

jennifer8013@ hotmail.com

Joe8092004@ hotmail.co

info@ essemme.ch

norbert@ itechanibia.org

KHORTON@ SGIS.ROG

WASSIN.DRIDI@ UIT.UNIVERSITY

wassim.dri.i@ uit.university

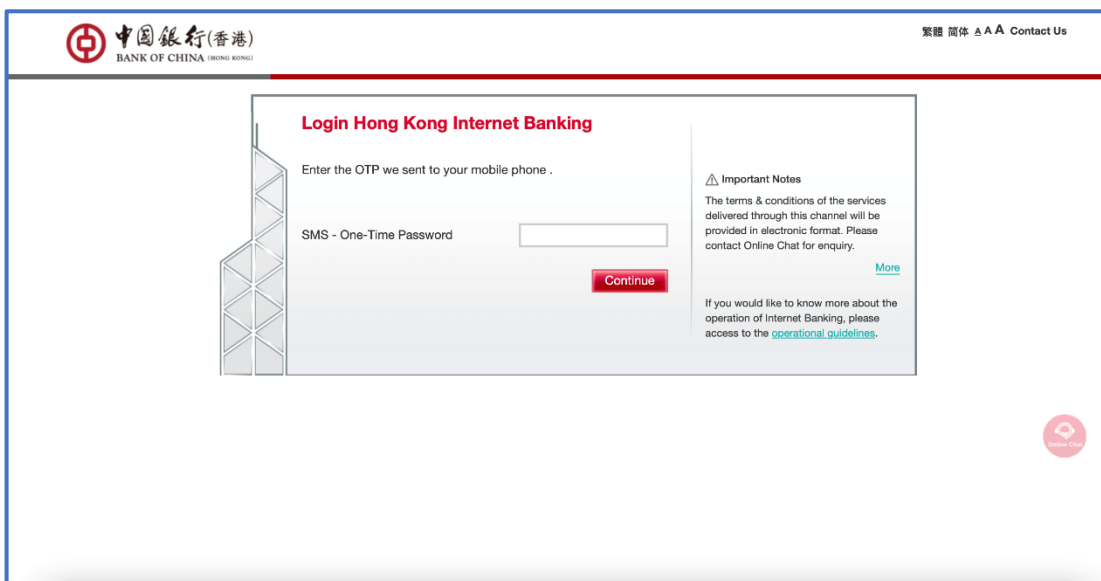
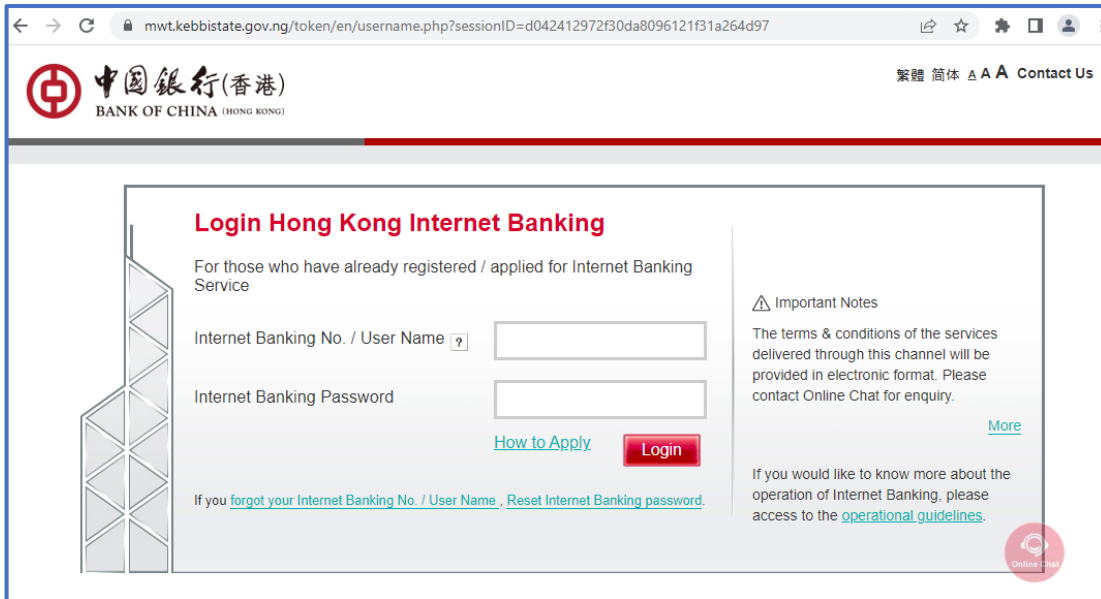
morbert@ itech-amibiadrgd



The fraudulent websites and phishing emails intend to steal customers' data, such as internet Banking number/username, Internet Banking password and one-time password sent via SMS. BOCHK declares that it has no connection with the fraudulent websites and phishing emails. Meanwhile, the case has been reported to the Hong Kong Monetary Authority and the Hong Kong Police Force.

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 e-mails or on websites. For more security information about BOCHK's electronic banking services, please visit <http://www.bochk.com/en/security.html>.

BOCHK advises its customers to verify any emails that claim to be sent from BOCHK. Please delete suspicious emails and attachments immediately without opening them. Customer who has logged into the aforesaid fraudulent websites and provided personal 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:



[Refer friends](#)  
to open an account now!  
HKD 100,000,000

[Home](#) | [Contact Us](#) | [Logout](#)

[Banking](#) | [Bill Payment](#) | [Investment](#) | [Loans](#) | [Insurance](#) | [Credit Card](#) | [RMB](#) | [Wealth Management Connect](#) | [MPF](#) | [e-Statement/e-Advice](#) | [Upgrade / Open Service](#) | [Assistant](#) | [Setting](#)

My Account | **Security**

**Mobile Token** [Print](#) [Help](#)

Please complete this step

ID

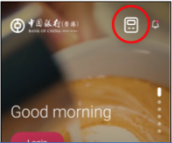
This transaction requires two-factor authentication.

Transaction Confirmation Code  (Please input the above numbers of "ID" which are underlined in RED into the Mobile Token to generate a 6-digit Transaction Confirmation Code.)

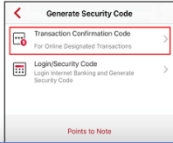
[back](#) | [Confirm](#) | [Cancel](#)

Please open BOCHK Mobile App on your phone and follow the steps below for authentication:


**Step 1:**  
Click "Mobile Token"



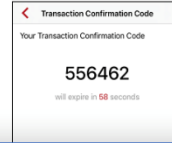
**Step 2:**  
Choose "Transaction Confirmation Code"





**Step 3:**  
Follow the instruction to enter specific ID information and use fingerprint or "Mobile Token" Passcode for confirmation



**Step 4:**  
"Txn Confirmation Code" will be shown on the phone. Please input "Txn Confirmation Code" on Internet Banking and follow the step to complete transaction.



[Refer friends](#)  
to open an account now!  
HKD 100,000,000

[Home](#) | [Contact Us](#) | [Logout](#)

[Banking](#) | [Bill Payment](#) | [Investment](#) | [Loans](#) | [Insurance](#) | [Credit Card](#) | [RMB](#) | [Wealth Management Connect](#) | [MPF](#) | [e-Statement/e-Advice](#) | [Upgrade / Open Service](#) | [Assistant](#) | [Setting](#)

My Account | **Security**

**Mobile Token** [Print](#) [Help](#)




Please complete this step


TOKEN ID

This transaction requires two-factor authentication.

Transaction Confirmation Code


Please follow the instructions below for authentication:

- Press  and hold it until  appears on the screen of Security Device.
- Enter the above numbers of "Token ID," which are underlined in RED on the Security Device.
- Press  to generate a 6-digit Transaction Confirmation Code.

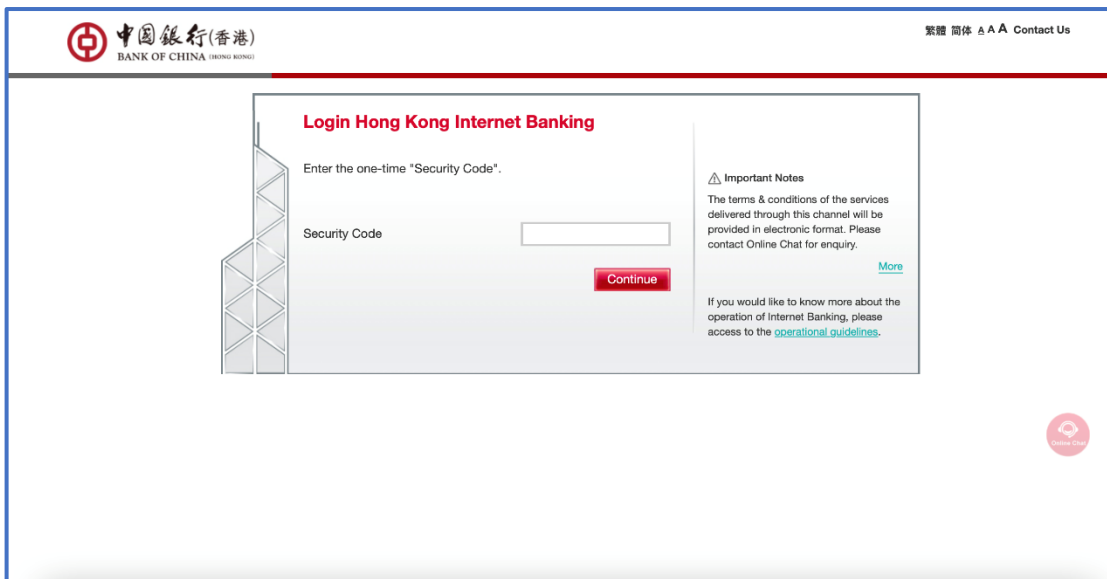
Remark: Please press  to correct inputs.

[Back](#) | [Confirm](#) | [Cancel](#)

**Display Screen**



[Conditions for Services](#) | [Important Notice And Privacy Policy Statement](#) | [Security Information](#) | [Hyperlink Policy](#) | [General Banking Service Charges](#)



Below are the screenshots of the phishing emails:



主題: 退款收據確認 [參考編號: 55236580107] / Confirmation of Refund Receipt

---

**退款 [55236580107]**

我地嚟信俾你知, 已成功處理並啟動退款 \$3,752.00 港幣, 將會退回到你賬戶。我地明白迅速處理退款既重要性, 並致力確保你既滿意。

為確認款項已經收妥並完成退款程序, 請跟隨以下步驟:

**登入**

我地誠實請求你喺24小時內完成呢個確認程序。  
如果我地喺 01/09/2023 前冇收到你既確認, 我地將會啟動程序將款項退還原發送者, 以免免任何不便。  
感謝你選擇中銀香港處理你嘅財務需求。我們重視你嘅信任, 期待繼續以卓越服務為你提供支援。

熱誠地

---

We're reaching out to inform you that a refund for [3,752.00 HKD ] has been successfully processed and initiated to be returned to your account. We understand the significance of a swift refund process and are committed to ensuring your satisfaction.

To confirm the receipt of funds and complete the refund process, please follow these steps:

**Login**

We kindly request that you complete this confirmation process within the next 24 hours.  
If we do not receive your confirmation by 01/09/2023 , we will initiate procedures to return the funds to the sender to prevent any inconvenience.

Thank you for choosing BOCCHK for your financial needs. We value your trust and look forward to continuing to serve you with excellence.

Best regards,

---

Bank of China (Hong Kong) Limited