

27 April 2021

Important Notes on Phishing Emails and SMS Messages

Bank of China (Hong Kong) (“BOCHK”) would like to alert its customers and the general public to phishing emails / SMS messages which have the intention of stealing customers’ personal information and swindling customers out of money.

Fraudsters recently sent out phishing emails or SMS messages, embedded with fraudulent website hyperlinks that purported to be from Postal Service / Airline Companies / Courier Services for verification or fee payment. These phishing emails or SMS messages made different false claims such as falsely claimed that customer’s package could not be delivered with extra postal / courier fee required, and requested customer to click on the embedded hyperlinks in the messages and enter personal and credit card information.

In an attempt to mislead customers, the hyperlinks of these fake emails / SMS messages and fraudulent websites will appear under different domain names or with slight modifications or variations of the official website addresses by adding a combination of letters, numbers or symbols to steal customers’ personal and credit card information, for various illegal use including **the binding of Mobile Payment & Services (e.g. XXX Pay)** for unauthorized local or overseas transactions, or **with the direct use on online transactions**.

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

The Bank reminds customers to be vigilant against possible scams:

- Please carefully protect your personal information. Do not disclose your personal information and passwords, including the SMS one-time password;

- Do not open email, 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.
- Do not input any information into unknown mobile applications or websites;
- If customers have logged in to the aforesaid fraudulent websites and provided personal information, 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 provided any password, please change the password immediately.
- If customers have received any email or SMS message on suspicious binding or use of Mobile Payment and Services or e-banking, please contact the Police and the Bank immediately.

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 BOCHK's electronic banking services, please visit www.bochk.com/en/security.html.

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



Phishing Emails:



Dear Customer,

Your package is waiting for delivery. Please confirm the payment
[REDACTED] on the link below, the online verification needs to be done in
the next 14 days before it expires:

[Follow my package](#)

This email is provided for informational purposes only and does not guarantee delivery of the shipment. Unable to reply to this email. Your e-mail address will only be used for the announcement of the parcel of the above shipment and will not be saved for advertising purposes. If you no longer wish to receive the package announcement, please click here [\[REDACTED\] Notification Service](#)

[Website](#) [Contact](#) [Impressum](#)





Book a pair of flight tickets for 100 HKD*; -

██████████ GOV.HK/ONLINE-GATEWAY-Number:

333299 Our reference number: 6859/ 0444

██████████hk order of 2 x "GOV.HK-POST ██████████"

██████████ ██████████ Airways Limited® ██████████
██████████ ██████████ mail.com

Dear ██████████ [mail.com](#),

Our company is celebrating 80 years since we have sold our first ticket. We th
celebrate and to honor our customers that support us by booking with our co

You and a couple of lucky ones have been selected to take advantage of this
100 HKD* we are giving away a voucher that can be used to book two tickets
with your loved one.

Can't wait? [Click here to get started.](#)

The voucher is available for one year from the date it was issued.

The link will be available for 48 hours so better hurry.

This is an automated notification email. Please do not reply to this message.



Phishing SMS Message:



█-Ship



由於欠缺資料 我們無法交付您的包裹 編號
EB008363309HK █ post.cc
█



Fraudulent Websites:

The image shows two side-by-side screenshots of a web browser. The left screenshot displays a payment form titled "Payment details" with the following fields: "Name On Card" (redacted), "Card number*" (redacted with a VISA logo), "Expiration date*" (redacted), and "CVV code*" (redacted with a card icon). A checkbox is checked, indicating acceptance of terms and conditions. A green button at the bottom says "Pay and continue >". The right screenshot shows a blue header bar with a redacted area and a menu icon. Below it, a large text message reads "Redirection to the request please Wait...." with the instruction "Please do not close this tab" and a circular loading spinner.





Protect Your Card Online

Protect your card against unauthorized use online **-at no additional cost**. For details, [click here](#)

To use your card, please complete this page. You'll the confirm your own card online.

Amount : 50 HKD\$
Commerce : [Redacted] Post

The code you entered is not valid or has expired. We have sent you a new code. Please enter the code within three minutes.

SMS KEY : (Required)

your request is being processed please wait..



Bank of China (Hong Kong) Limited