



5 September 2019

HSBC WARNS AGAINST PHISHING EMAIL

The Hongkong and Shanghai Banking Corporation Limited would like to alert its customers to the phishing email purported to be sent by HSBC. The phishing email suggests that recipients should open the attachment.

HSBC would like to remind its customers that it has no connection with the phishing email involved. Customers are advised not to open the attachment in this email.

Below is the screen capture of the phishing email:

Phishing Email

[可能是垃圾邮件] HSBC - EXPORT BILL PROCEEDS PAID BACKTG316094CCC

HA HSBC Advising Service <tradeservice@hsbc.com>
To: Undisclosed recipients: Wed 2019-09-04 08:19 AM

ⓘ We removed extra line breaks from this message.

M0764200975917.xlsx
4 MB

Dear Customer,

As per previous arrangement, we attach DC/Amendment Advice (T01) and DC/Amendment Copy (T02) or Import/Export Global Trade & Receivables Finance advice(s), as applicable.

To open the file(s), please follow the instructions below:
1. Save or Detach the file into your preferred drive 2. Run Microsoft Excel 3. Open the file just saved to read or copy the advice/content.

Please note that whenever a DC and/or Amendment Copy is attached, it serves for reference only and is not a negotiable instrument.

The attached documents are intended for the assigned recipient only.

This is a system generated message and is only an acknowledgement that we have received the documents/claim. It does not constitute our acceptance of its contents.

Please do not reply to this email. If you have any enquiries please contact your local HSBC Global Trade and Receivables Finance office.

HSBC maintains strict standards and procedures to prevent unauthorised access to information about customers. HSBC will not contact you by email to ask you to validate customer information such as passwords or PINs.

HSBC does not have liability for any losses, damages, errors or omissions or late or non-arrival or disclosure to third parties of messages sent via email or other electronic means due to any reason whatsoever.

The Hongkong and Shanghai Banking Corporation Limited

Security tips

1. Install virus detection software and personal firewall on your computer. This software needs to be updated regularly to ensure you have the latest protection.
2. To prevent viruses or other unwanted problems, do not open attachments from unknown or non-trustworthy sources. If you wish to validate our email address please contact your local Global Trade & Receivables Finance office.
3. If you discover any unusual activity, please contact your HSBC Global Trade & Receivables Finance representative as soon as possible.

(See attached file: M0764200975917-T02.xlsx)

This e-mail is confidential. It may also be legally privileged.
If you are not the addressee you may not copy, forward, disclose or use any part of it. If you have received this message in error, please delete it and all copies from your system and notify the sender immediately by return e-mail.

Internet communications cannot be guaranteed to be timely, secure, error or virus-free. The sender does not accept liability for any errors or omissions.

"SAVE PAPER - THINK BEFORE YOU PRINT!"

If customers are concerned, they should call the HSBC Commercial Banking service hotline at 2748 8288 or report to the Police.

ends/more

Note to editors:

The Hongkong and Shanghai Banking Corporation Limited

The Hongkong and Shanghai Banking Corporation Limited is the founding member of the HSBC Group, which serves our customers through four global businesses: Retail Banking and Wealth Management, Commercial Banking, Global Banking and Markets, and Global Private Banking. HSBC serves customers worldwide from offices in 65 countries and territories in our geographical regions: Europe, Asia, North America, Latin America, and Middle East and North Africa. With assets of US\$2,751bn at 30 June 2019, HSBC is one of the world's largest banking and financial services organisations.

ends/all