

News Release

7 December 2015

HSBC WARNS AGAINST FRAUDULENT E-MAILS AND WEBSITES

HSBC would like to alert its customers to phishing e-mails which link to fraudulent websites (for example: <http://www.debiasi.it/HSBC.COM.HK/Z1ZE5154ZFEZEF15ZFE45R45Z54E>), suggesting customers, including HSBC customers, to provide, among other details, their personal and credit card information to reactivate their bank accounts.

HSBC would like to remind its customers that the Bank has not sent these e-mails to its customers and has no connection with the fraudulent sites involved. Below are examples of fraudulent e-mails and website.

Example of fraudulent e-mail

Dear HSBC Customer,

Our records show unnormal transactions have been made from your HSBC accounts in the past 2 months.¹ As such, **your accounts are now deemed dormant**. Dormant accounts are not eligible for HSBC phone banking or online services, nor can they be used to purchase HSBC Wealth Management products.

Re-activate your accounts by following this step **CLICK HERE** and Follow the instruction. Once you have all the details validated, you will have your account activated and in service once more.

Thank you for choosing HSBC!
Please call your Relationship Manager, visit any HSBC branch, call the HSBC Premier hotline on **400-840-3788** or the HSBC Advance hotline on **400-830-8887**, or click for more details.

© 2015 Copyright. HSBC Bank - Company Limited. All rights reserved

This information is issued by

The Hongkong and Shanghai Banking Corporation Limited

Registered Office and Head Office:
1 Queen's Road Central, Hong Kong
Web: www.hsbc.com.hk
Incorporated in the Hong Kong SAR with limited liability

HSBC 

Screen capture of fraudulent website

The screenshot shows a fraudulent website designed to look like the HSBC internet banking interface. At the top left is the HSBC logo. To its right are navigation links: Banking, Borrowing, Investing, Insurance, and Offers. Below this is a red horizontal bar. The main heading is "Account Verification" in red. A yellow alert box contains the text: "ALERT: This step is required for your account safety and we will call you after the verification." Below the alert are several input fields for user identification: User ID, Password, Dual-Password Logon, Email, Phone Number, Date of birthday, HK ID/Passport, and Account Number. Further down are fields for credit card number, Full Name, MM/AA, CVC, and 3D Password. A red "Continue" button is positioned below these fields. To the right of the input fields is a blurred image of a credit card. At the bottom of the page is a red footer bar with the text: "© The Hongkong and Shanghai Banking Corporation Limited 2002-2015. All rights reserved."

Customers are reminded to ensure they are connected to a valid HSBC site when they want to access the Bank's internet banking services. The Bank's internet banking site's domain is <http://www.hsbc.com.hk>. Customers should access their Personal Internet Banking accounts by keying in the website address at the address bar of the browser.

HSBC is working with the relevant authorities to shut down the fraudulent site. If customers are concerned they may have disclosed their personal details to suspicious parties, they should call the HSBC Personal Banking service hotline at +852 2233 3000 or report to the Police.

ends/more

Notes 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 around 48 million customers through four global businesses: Retail Banking

and Wealth Management, Commercial Banking, Global Banking and Markets, and Global Private Banking. The Group serves customers worldwide from over 6,100 offices in 72 countries and territories in Asia, Europe, North and Latin America, and the Middle East and North Africa. With assets of US\$2,549bn at 30 September 2015, HSBC is one of the world's largest banking and financial services organisations.

ends/all