HSBC

28 December 2016

News Release

SHOPPERS SHOULD TAKE EXTRA CARE TO PROTECT THEMSELVES ONLINE DURING BUSY FESTIVE PERIOD – HSBC

With more and more people shopping online and the New Year period the busiest of the year, shoppers should take basic steps to protect themselves from the increasing threat of online crime.

From phishing to spoofing, there are many different names for cyber scams – but they all rely on criminals encouraging victims to download malicious software or hand over personal information which then enables them to steal money, data and even identities. Some of the tactics fraudsters use include sending emails and text messages (SMS) containing bogus links; setting up fake websites; hacking insecure wireless networks; and phone calls pretending to be from a bank.[1]

Nguyen Duc Thinh, Head of Branch Network North, Retail Banking and Wealth Management, HSBC Vietnam, said:

"With millions of people across Vietnam going online every day to shop, bank and browse, especially during the holidays, we are calling on consumers to be vigilant as they rush to take advantage of seasonal promotions which have been widely offered by merchants including e-commerce ones. It's more important than ever that people don't forget to stay safe shopping online. Taking some basic steps will help people avoid cyber-crime risk.

"In the same way that you wouldn't walk down your shopping streets with your wallet wide open, don't share personal information or bank account details on social media, or in emails, and never reveal your PIN number. At the same time, make sure your computers and smartphones are protected with the latest updates, anti-virus software and have automatic locks enabled with password protection."

Various steps online shoppers can take to protect themselves include:

- Not over-sharing on social media and other websites – criminals use personal information such as birthdays, addresses and phone numbers to hack into accounts
- Watching out for fake emails, text messages (SMS) and websites – reputable companies will never send unsolicited emails asking their customers to verify their personal and security details

- Never divulging bank PIN number to anyone - banks never ask for cards (and PINs) to be returned via a courier
- Making sure wireless networks are secure by turning on all the privacy settings and password protection
- Using passwords to automatically lock and protect mobile phones or tablets
- Installing anti-virus software and downloading the latest security updates for computers, tablets and mobile devices
- Destroying paper documents carefully – some fraudsters go through rubbish bins to find useful information.[2]

HSBC works with leading experts to continually improve the security of its customers. Find out more about the different types of online attacks and how HSBC is working to protect customers via our country public website.

-ends-

Media contacts

Tran Ngoc Anh Thu +84 8 3520 6592 thunatran@hsbc.com.hk

Notes to editors

[1] HSBC, Online Security
http://www.hsbc.com/internet-banking/online-security

[2] HSBC, Online Security
http://www.hsbc.com/internet-banking/online-security

The HSBC Group
HSBC Holdings plc, the parent company of the HSBC Group, is headquartered in London. The Group serves customers worldwide from around 4,400 offices in 71 countries and territories in Europe, Asia, North and Latin America, and the Middle East and North Africa. With assets of US$2,557bn at 30 September 2016, HSBC is one of the world's largest banking and financial services organisations.

HSBC Vietnam

HSBC has been in Vietnam for more than 140 years – the bank first opened an office in Saigon (now Ho Chi Minh City) in 1870. HSBC was the first foreign bank to launch its locally incorporated entity on 1 January 2009 as HSBC Bank (Vietnam) Ltd. The bank's current network includes two branches and five transaction offices in Ho Chi Minh City, one branch and four transaction offices in Hanoi, and three full-service branches in Binh Duong, Can Tho, and Da Nang. HSBC is one of the largest foreign banks in the country in terms of investment capital, network, product range, staff and customer base.