大 眾 銀 行（香 港）
PUBLIC BANK (HONG KONG)
（馬來西亞大眾銀行附屬公司 A subsidiary of Public Bank Berhad, Malaysia）

Date: 29 May, 2013
日期：2013 年 5 月 29 日

Dear Customer,

Trojan Horse Attack on Internet Banking Services

At the request of the bank's regulator, Hong Kong Monetary Authority (HKMA), the bank would like to draw your attention to the recent discovery in Hong Kong of a number of suspected Trojan Horse fraud cases, chiefly relating to business or corporate internet banking services.

Internet users should stay vigilant when using their computers. If you find the website of the bank suspicious or encounter unusual logon screen, you should NOT enter any information (including user ID, password and one-time password (OTP)) to the website and should report to the bank immediately. Enclosed please find the extract of HKMA's inSight Article on "Trojan Horse Attack on Internet Banking Services" for details.

For enquiries, please visit the bank's corporate website at http://www.publicbank.com.hk or call the bank's E-Banking Support Hotline at (852) 2541-9206.

Public Bank (Hong Kong) Limited

親愛的客戶：

網上銀行服務 - 慎防特洛伊木馬程式

因應監管機構 - 香港金融管理局（「金管局」）之要求，本行敬希 貴公司垂注，最近於本港發現之多宗與木馬程式有關之騙案，主要涉及企業網上銀行服務。

互聯網用戶使用電腦時應時刻保持警惕。 貴公司若發現銀行網站有任何可疑之處，或登入網頁時有異樣，便不應輸入任何資料(包括用戶名稱、密碼及一次性密碼)，並應即時與銀行聯絡。隨函附上節錄自金管局之「匯思」文章 「網上銀行服務慎防特洛伊木馬程式」以供 貴公司參考。

如有查詢，請瀏覽本行網站 http://www.publicbank.com.hk，或致電本行電子銀行服務熱線 (852) 2541-9206 查詢。

大眾銀行（香港）有限公司

Extracted from "inSight" published by Hong Kong Monetary Authority

Trojan Horse Attack on Internet Banking Services

You may have the experience of receiving fishy emails purported to be from your friends asking you to open a file or to provide personal data, but your friends later confirmed that the emails were not sent by them. In such cases, most likely your friends' computer had been infected with a Trojan Horse, and if you did follow the instructions in the emails, you might have become a victim too.

Recently a number of suspected Trojan Horse fraud cases, chiefly relating to business or corporate internet banking services, were detected in Hong Kong. It is believed that computer users, when logging on their internet banking account, were lured into inputting their logon credentials (e.g. logon ID, password, and one-time password (OTP) generated from the security device) to a fake web page. The information so "stolen" was then used by fraudster to initiate fraudulent fund transfer transactions despite two-factor authentication was required, as OTP was already disclosed to the fraudster.

The use of Trojan Horse for internet fraud has been around for some years. Where computer users fail to protect their computers from malwares such as Trojan Horse, fraudsters will still be able to do the trick, regardless of the level of internet security provided by banks. Here the HKMA would like to remind bank customers that it is very important to vigilantly protect their computers to safeguard against internet banking fraud.

How could Trojan Horse be used to pose risks to internet users?

Through the use of Trojan Horse planted in an internet user's computer, a fraudster can capture screen displays and keystrokes, steal information stored in or even take control of the user's personal computer.

What precautionary measures could be taken to avoid becoming a victim of Trojan Horse attack?

Internet users should stay vigilant when using their computers in order to minimise the chance of being infected with Trojan Horse or any other malwares, or at least to detect them if the computers are already infected. If customers find the website of the bank suspicious or encounter unusual logon screen, they should **NOT** enter any information (including user ID, password and OTP) to the website and should report to the bank immediately.

How could an internet user detect whether a Trojan Horse has been installed in his/her personal computer?

Internet users should install anti-virus software and personal firewall in the personal computers. It is also important to keep the software up-to-date to cater for any new alerts identified. Other good habits include:

- be very cautious about opening attachments in e-mails from unfamiliar sources, and avoid visiting or downloading software from suspicious websites
- never access your internet services such as internet banking through hyperlinks embedded in emails, internet search engines, suspicious pop-up windows or any other doubtful channels (customers should connect to a bank website through typing the authentic website address in the address bar of the browser or by bookmarking the genuine website and using that for subsequent access)
- don't disclose logon passwords or OTP to any person through any means such as e-mail, over the phone or in person
- review your transaction records regularly and verify transaction details on the notification (e.g. SMS message) sent from the bank, and report to your bank immediately if you notice any suspicious transactions in your bank accounts or discover any suspicious web page
- follow the security tips published by your banks when conducting internet banking transactions

Given the increasing risk of internet banking frauds, is it still safe to use internet banking?

Internet banking services in Hong Kong are safe to use so long as both the banks and the customers have taken appropriate precautionary measures.

節錄自香港金融管理局之「匯思」

網上銀行服務
慎防特洛伊木馬程式

大家可能試過收到朋友的可疑電郵，着你開啓某個檔案或提供個人資料，但一經查證後對方卻表明從未發過那些電郵。由此看來，你朋友的電腦可能已受到特洛伊木馬程式(木馬程式)感染，如果你當時按電郵指示照做的話，便可能同樣成爲受害人。

最近香港發現多宗懷疑利用木馬程式，並主要涉及企業網上銀行服務的騙案。相信過程中騙徒誘使網上銀行用戶在登入戶口時將有關的重要資料(如登入名稱、密碼及由保安編碼器發出的一次性密碼)輸入虛假網頁，然後利用上述所得資料(包括一次性密碼)完成雙重認證，再進行網上銀行轉帳騙取金錢。

利用木馬程式的網上騙案已存在多年。如果用戶的電腦保安措施不足，令電腦受到惡意程式攻擊，則無論銀行方面的網上服務保安如何嚴密，騙徒仍然有機可乘。因此，金管局希望在此提醒銀行客戶，妥善的電腦保安措施對防範網上銀行騙案極爲重要。

騙徒如何利用木馬程式來攻擊網絡用戶？
騙徒將木馬程式植入互聯網用戶的個人電腦後，便可記錄互聯網用戶電腦屏幕所顯示的畫面及按過的鍵、盜取用戶個人電腦內儲存的資料，甚至遙距控制用戶的個人電腦。

用戶可採取哪些防範措施，避免遭到木馬程式攻擊？
互聯網用戶使用電腦時應時刻保持警惕，以防受到木馬程式或任何其他惡意程式攻擊；即使電腦已遭感染，用戶至少仍有機會察覺到異常的情況，並採取適當行動。銀行客戶若發現銀行網站有任何可疑之處，或登入網頁時有異樣，便**不應**輸入任何資料(包括用戶名稱、密碼及一次性密碼)，並應即時與銀行聯絡。

互聯網用戶如何辨察得出個人電腦已遭植入木馬程式？
互聯網用戶應在個人電腦裝設防病毒軟件及個人防火牆，並且不時更新，以便接收最新的病毒警告。用戶更應養成以下的良好習慣：

- 不應隨便開啓來歷不明的電郵的附件，並避免登入可疑的網站或從其下載任何軟件
- 切勿經電郵附上的超連結、網上搜尋器、可疑的突現式視窗或其他可疑渠道登入網上服務(如網上銀行)，而應在瀏覽器上端的網址欄親自輸入銀行的真實網址或將該網址記錄在瀏覽器書簽內，以連接到銀行網站
- 切勿透過電郵、電話或親身告知任何人自己的戶口登入密碼或一次性密碼

- 定期翻查戶口交易紀錄，並查核銀行通知(如手機短訊)的交易詳情，一旦發現銀行戶口有可疑交易或可疑網頁，應立即通知銀行
- 進行網上銀行交易時依循銀行的保安提示

網上銀行騙案風險增加，使用網上銀行服務是否仍然安全？

只要銀行及客戶雙方都採取適當的保安措施，本港的網上銀行服務是安全的。