匯思

所有文章

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。

鑑於近期發現到的騙案，以下我會以答問形式說明一些涉及木馬程式的事項。

Q1 **騙徒如何利用木馬程式來攻擊網絡用戶？**

A1 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。

Q2 **用戶可採取哪些防範措施，避免遭到木馬程式攻擊？**

A2 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。

Q3 **互聯網用戶如何辨察得出個人電腦已遭植入木馬程式？**

A3 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

Q4 **木馬程式攻擊是否同樣可以影響附有交易簽署功能的保安編碼器(即設有數字小鍵盤的保安編碼器，見下圖)？**

A4 網上銀行客戶使用附有交易簽署功能的保安編碼器時，須於保安編碼器輸入有關交易的特定資料(如收款人戶口號碼)，再由保安編碼器發出一次性密碼，作爲確認交易之用。然而，騙徒可能利用各種技倆，誘使客戶在保安編碼器輸入某組號碼(很可能是騙徒犯案用的戶口號碼)，藉此截取由保安編碼器發出的一次性密碼，然後經網上銀行從受害人戶口轉帳到騙徒的戶口。因此，網上銀行用戶必須緊記，一般而言網上銀行登入手續**不會**要求客戶將電腦畫面顯示的任何數字輸入保安編碼器內。換言之，用戶一旦發現登入網頁要求他們把數字輸入附有交易簽署功能的保安編碼器，便可假設那是一個虛假網站，並應立即通知銀行。

Q5 **網上銀行騙案風險增加，使用網上銀行服務是否仍然安全？**

A5 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。

附有交易簽署功能的保安編碼器

助理總裁(銀行監理)
鄭發
2013年4月24日