資料來源：內政部警政署 165 反詐騙諮詢專線

標題：跨國網路犯罪猖獗 企業匯款當心駭客攔截

發布時間：2013/3/11 下午 03:04:33

案例一：北部某一從事汽車零件出口之國際貿易公司，貨款均由美國客戶以 TT (telegraphic transfer) 電匯方式匯至該公司在臺開設之銀行帳戶，雙方並透過 E-mail 進行聯繫。102 年 2 月底，該公司收到美國客戶以 E-mail 通知即將匯款美金 50 萬，數日後竟發現客戶將貨款改匯至一英國銀行帳戶。經向美國客戶查證，美國客戶稱是依照臺灣公司的 E-mail 指示，臺灣公司始發現雙方往來之 E-mail 遭駭客入侵。駭客入侵該臺灣公司與美國客戶間之 E-mail 後，以類似該臺灣公司的 E-mail 帳號與美國客戶聯絡，致美國客戶陷入錯誤，將貨款改匯至嫌犯指定之英國銀行帳戶，因而遭受巨額金錢損失。

案例二：北部某一工業顧問公司之電子郵件信箱於 102 年 2 月遭駭客入侵，直接以該公司之 E-mail 與美國客戶聯繫，致美國客戶陷入錯誤，將貨款 19 萬美金匯至嫌犯指定之馬來西亞銀行帳戶，公司因而遭受巨額金錢損失。

案例三：網路駭客攔截某一機械公司所發給客戶的 E-mail，郵件尚未到達客戶端前，駭客便直接攔截並竄改郵件內容及匯款帳戶資料。再假

借該公司名義，寄件給客戶；幸好客戶端警覺不對，主動聯繫是否有更改銀行帳戶事宜，才免於受騙。

犯罪手法介紹：

刑事警察局國際刑警科、刑事研究發展室自 101 年 7 月起接獲多起民眾報案，駭客入侵電腦後，破解電腦使用之保護措施或利用電腦系統之漏洞，得知民眾電子信箱之帳號密碼，因而得以入侵電子郵件，篡改郵件內容，變更臺灣公司之匯款銀行及帳號，致國外客戶陷入錯誤，造成貨款被駭客攔截的案例。截至目前，發線受害者有我國人、比利時籍、印度籍、沙烏地阿拉伯籍及波蘭籍等。

網路駭客手法說明如下：

一、註冊相似度極高之網域名稱：駭客利用網路申請註冊網域名稱(Domain Name)之便利性，利用極為相似之字母或數字，如英文字母小寫 l 與數字 1，n 與 h 等極為相似之符號以假亂真，使國外客戶難以辨別使用者(user)名稱之後真偽，或維持使用者(user)名稱，直接以相似度極高之網域名稱(Domain)代替。例如：駭客將 1isaling@hotmail.com 之英文字母 l 竄改成數字 1，形成 lisa1ing@homtail.com;或將 lisalin@yahoo.com 之網域名稱變更，篡改成 lisalin@ymail.com。

二、植入木馬程式：駭客利用暗藏的惡意或木馬程式，包括遠端遙控功

能及鍵盤側錄程式（keyloger），側錄民眾上網時所輸入之帳號密碼，並搜尋電腦所有磁碟是否存有憑證檔案，再將憑證及鍵盤操作紀錄之帳號密碼遠端傳送回駭客的主控台，因而得以輕易破解電腦保護措施，取得民眾電子信箱之帳號密碼，入侵電子郵件後竄改郵件內容。

三、進行客製化犯罪行動：犯罪集團入侵電子郵件信箱後，會針對公司做極為詳盡的資料蒐集，包括監控臺商與客戶間之對話，包括客戶之姓名、公司電話、電子郵件帳號及銀行帳號等，再利用非法取得之資料，運用社交攻擊手法，更進一步取得各種如網路銀行、行動電話等客服及語音電話服務所需之個人身分驗證資料，以「假冒客戶」通過客服人員所提問之身分驗證資訊，籍此「套出」更多個人隱私資料，進行各種假冒身分之犯罪詐騙行為。

民眾防制作為

一、注意密碼設定：由於網路的便利性，無形中產生許多漏洞，如大多數的網站都會提供會員「密碼提示」功能，而民眾多半會設定與個人相關的資料做為密碼提示，如「生日」、「手機號碼」、「媽媽的名字」等，而犯罪集團會針對個人蒐集詳細的資料，即可利用密碼提示猜到密碼，建議民眾在設定密碼提示時，不要以個人相關資料做為密碼提示的問題或答案，而且密碼設定至少要有英文、數字與特殊符號等，且經常更換密碼，以免帳號密碼遭盜用。

二、檢查郵件寄件者：將滑鼠游標移到寄件者名稱上，看看顯示名稱與寄件者名稱是否相符，尤其須特別留意電子郵件使用者名稱(user name)及網域名稱(domain)是否有異。

三、加強客戶端之安全檢核機制：請國內企業多加注意，如能多幾個方式和客戶端再次確認匯款銀行及帳戶之正確性，將能多一份保障，以避免造成重大財損。例如：匯款前以電話或傳真向客戶確認匯款銀行及帳戶，如須變更原使用銀行帳戶，或客戶接獲變更匯款銀行帳戶通知，均必須再三確認，以避免駭客入侵篡改匯款銀行資料。

四、使用正版軟體：企業電腦安裝正版軟體，隨時或定期上網修補系統程式漏洞，確保企業電腦安全，並確認企業電腦安裝正版防毒阮體，以提供一定程度的安全防護，例如，掃瞄、解毒、刪除病毒等並即時阻絕外來病毒、木馬程式的入侵及警示瀏覽網頁時的一些安全性威脅。

本局再次籲請社會大眾，注意企業電腦使用行為，以防範電子郵件遭駭客入侵後攔截國外匯款。多一分安全檢查，少一分財產損失。