大陸台商
對於網路詐騙事件之預防與防制

文／姜志俊

一、問題緣起

最近海基會受理多起大陸台商遭受網路詐騙的陳情案件，無獨有偶，經濟部國際貿易局及內政部警政署刑事警察局亦分別受理甚多網路詐騙案件，並多次發出國際貿易詐騙事件警示。因此，如何預防網路詐騙事件，及發生網路詐騙事件後如何防制救濟，乃成為刻不容緩的重要課題。

二、詐騙事件舉隅

茲就海基會受理陳情的網路詐騙案件，略舉數例簡要說明如下：

(一)本公司於105年5月中旬收到客人的訂單後將PROFORMA INVIOCE傳給客人，隔天客人打電話詢問我們是否有請他把款項美金20,601元匯到另外一個中國帳戶，並將他收到的PROFORMA INVIOCE傳給我們看，發覺是非法人士使用我們公司的郵件並以公司同事的名義發信件告知客人我們換了銀行帳戶，而且還撥電話催促客人趕緊匯款。隔一個禮拜後客人發郵件詢問我司大約會走幾號的船，非法人士又使用本公司的郵箱回信給客人，並附上偽造的授權書給客人，告知他們匯款至他們指定的銀行帳戶確實是沒有問題的。

(二)本公司向大陸廠商A公司購貨轉銷美國，5/16發採購單，5/17的7:12還是由大陸廠商A公司的正確信箱發出的信，要求改新帳戶，5/17的8:06是由另一個信箱發出的信要求改新帳戶，內容與上一封一樣，5/18通知匯款新帳戶，7/22告知要求我方通知退回款改匯另一個帳戶，7/26通知我聯絡吳先生，因雙方講的東西兜不起所以沒再理他，給的資料是福建省，但實際聯絡對方在山東，經與吳先生電話聯絡過，並且有錄音，吳先生告知錢確實是他收到美金66,240元，且已轉走，但目前我方無法確認這人否為詐騙集團的人

或是人頭帳戶，7/27發覺書信內容很怪才跟廠商聯絡發覺受騙立刻報警，8/2第三方持續來信跟對方銀行請求退款並重新匯款。

(三)本公司於105年7月13日依照韓國客戶B公司的來信指示，將貨款美金303,974元匯入中國上海交通銀行的指定帳戶內，直至同年7月18日韓國客戶告知尚未收到款項，經本公司透過LINE將匯款資料傳給韓國客戶，被韓國客戶告知該帳戶並非該公司的匯款帳號，可能是駭客的帳戶。我們已經向台灣警方報案，但因款項龐大，對公司影響甚鉅，還請 貴處協處，能將款項早日追回。

三、詐騙手法

綜合上述三個詐騙案例，發現詐騙集團都是透過侵入電子信箱作案，歸納歹徒所用詐騙手法大致如下：

(一)犯罪集團入侵電子郵件信箱，針對公司做極為詳盡的資料蒐集，以「假冒客戶」通過客服人員所提問之身分驗證資訊，藉此「套出」更多個人隱私資料，進而從事各種假冒身分之犯罪詐騙行為。

(二)駭客利用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，o與O等極為相似之符號以假亂真，由於陳情人採用電子郵件溝通，很少再用電話溝通，使陳情人一時失察，難以辨別使用者名稱之真偽，以致誤上賊船，將貨款匯入詐騙集團帳戶。

(三)駭客利用暗藏的惡意或木馬程式，側錄廠商上網時所輸入之帳號密碼，並搜尋電腦存有之憑證檔案，將其傳回駭客主控台，而得以輕易破解電腦保護措施，入侵電子郵件後竄改郵件內容。

四、問題防制

針對本文所述三個詐騙案件情形，可見台商在電子郵箱管理、與客戶業務往來查證及事後應變處理三方面，均有待注意與加強。

(一)在電子郵箱管理方面

企業必須管理好公司的電子郵箱，提高安全性和私密性，具體作法如下：

1. 加強電子郵箱保密工作：在國際貿易中，電子商務日益普及，外貿企業的商務溝通主要通過電子郵件進行，但是外貿企業必須認識到電子郵件雖然具有方便快捷的優點，同時還會存在一些容易被不法分子利用的漏洞。一些外貿業務員不分場合隨意發放自己的名片和自己的聯繫郵箱， 實際上這些隨意的做法給不法分子盜取郵箱重要商務往來資訊提供了機會。外貿企業在參加一些貿易洽談會時，要加強保密意識， 對企業的一些比較重要的聯繫郵箱要注意保密。
2. 電子郵件交流過程中要注意分辨真偽：外貿業務員疏於區分真假郵箱細微差別，一方面給企業客戶帶來經濟損失，另一方面嚴重損害了企業的信譽。如有個不法分子在廣交會上冒充客商身份獲取了某公司業務員的名片，並且之前還通過一筆小小的訂單拿到了該公司的各種印章， 在得知國外客戶準備預付定金時就立即註冊了非常相似的郵箱地址，騙取了國外客戶預付的定金。所以外貿業務員在使用電子郵箱時必須高度警惕。在電子郵件交流過程要仔細注意分辨真偽，對常用的客戶郵箱可以添加必要的備註說明或防偽標記。
3. 建議使用企業郵箱或付費郵箱：商務溝通過程中，最好使用企業郵箱或者付費郵箱， 這樣可以提高郵箱的安全性；或者根據不同的國外客戶，分別使用不同的專用郵箱，有別於在已發放名片上的郵箱地址。此外，不要點擊不明郵件或連結， 防止釣魚網站和木馬病毒。同時要選擇較好的防毒軟體，定期進行電腦殺毒並更換郵箱密碼。

(二)在與客戶業務往來查證方面

國際貿易往來中不要單純依靠電子郵件進行溝通，可以在貿易往來的關鍵環節進行多樣溝通方式，例如電話和傳真，儘量不要僅僅通過電子

郵件提供銀行帳戶等重要資訊，可與交易方約定只通過傳真或電話等較為可靠管道提供付款資訊， 並提醒對方在轉帳或匯款前後進行電話確認。此外，在涉及合同或款項交易時，儘量建立多種確認方式，尤其是在匯款前，一定要打電話或發傳真向對方確認，不讓不法分子有任何可乘之機。

(三)在事後應變處理方面

外貿企業應與國外客戶經常保持聯繫，一旦發現異常情況， 或貨款被騙，要及時向警察機關報案，並盡可能詳盡提供如對方銀行卡號等資訊，以利警察機關即時調查犯罪嫌疑人，並透過兩岸共同打擊犯罪及司法互助協議，要求大陸公安機關協助追緝歹徒。同時，應及時告知國內匯款銀行或國外客戶請其指示相關銀行凍結款項，儘量挽回損失。由於部分企業在國際貿易風險防範方面意識不強，不能及時察覺和發現電子郵件遭駭客侵入，導致不法分子屢屢得逞。加以國際貿易中通常採用外匯進行貨款的結算（一般以美元結算居多），合同交易金額較大，一旦被騙，損失非常慘重。電子郵件詐騙還涉及到國外客戶，如果對詐騙手法不夠瞭解，很容易導致雙方的不信任，嚴重干擾了國際貿易秩序，甚至引起國外客戶客訴索賠，因此，企業在從事國際貿易時，應對此類犯罪手段高度關注，防止企業遭受信譽及經濟的雙重損失。

五、問題預防

經濟部國際貿易局及內政部警政署刑事警察局，對於屢屢發生的國際貿易詐騙案件，經常於其官網或政令宣導時報提出警示，台商應針對被騙的發生原因對症下藥，茲提出下列建議以供參考：

(一)注意密碼設定：廠商設定密碼提示時，不要以企業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，且須不定時更換密碼，以免帳號密碼遭人盜用。

(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：除利用電子郵件與客戶往來外，更應增加其他聯絡方式和客戶端再次確認匯款銀行及帳戶之正確性，如此方能多一份保障，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，如有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軟體，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。

(五)注意加密處理：電子郵件屬低安全性之資訊交換格式，易遭竄改冒用，以電子郵件傳送訂單或出貨單等資料，應加密處理，以防止資料遭到竄改、偽冒。

(六)加強資安管理：強化公司內部資安管理，除系統程式的適時更新完善外，對員工接觸機密文件的授權機制及資安教育訓練，亦須同步加強，以減少駭客入侵機會，而造成公司財物損失。

(七)加強資訊蒐集：有關預防跨國網路詐欺事件，可責成公司專人定期至經濟部國際貿易局台灣經貿網（網址： http://info.taiwantrade.com/CH/），或內政部警政署刑事警察局（網址：http://www.cib.gov.tw/index.aspx），或資安人（網址：http://www.informationsecurity.com.tw/main/index.aspx）網站查詢，以利公司借鏡，俾免公司遭受損失。

（本文作者為翰笙法律事務所主持律師、海基會台商財經法律顧問）