電郵易遭駭客竄改遂行詐騙，企業應落實資安防詐教育訓練

國內利用釣魚郵件詐騙的手法持續不斷，其中針對企業進行的竄改商務電子郵件詐騙(Business Email Compromise, BEC)數量也大幅提升，加深了企業的資安風險。

企業進行國際貿易頻繁，與外國供應商或企業合作時常需要聯繫及匯款交易，使駭客有機可趁。駭客會以假冒合作的外國供應商或是高階主管之名義寄送電子郵件，意圖降低收件者戒心，誘騙公司或財務人員轉帳匯款。今年國內就有案例是駭客偽冒一間公司的財務長發送電郵給秘書，以信件內容及會議紀錄誘使秘書信任，進而轉帳至指定帳戶，使公司損失上百萬美元。

這類 BEC 詐騙常見手法是，駭客會先寄送釣魚郵件，以具誘惑性之文字內容誘發員工開啟郵件，並下載夾帶木馬程式、病毒的附件以便暗中竊取 Email 登入資訊。或是誘騙員工點擊惡意連結進入釣魚網站，利用以假亂真的網頁騙取信箱帳密。駭入員工的 Email 之後，駭客會收集並竊取員工來往郵件的內容資訊，接著利用收集到的資訊偽冒身分發送郵件，騙取員工匯款至指定帳戶藉以竊取企業的帳款。

資安廠商 Proofpoint 2020 年的研究報告指出，透過 Email 進行駭侵攻擊是駭客容易進行的攻擊手法之一，因許多企業內仍有不少資安教育訓練或資安意識不足的員工。秘書和會計等會接觸到匯款、交易的企業員工，常被駭客鎖定為竊取 Email 帳密的對象。

- 建議採取資安強化措施

1、建議如果收到聲稱是合作企業或高階主管的電子郵件，務必利用其他管道查明對方身分，或是向其所屬企業確認身分。

2、收到電子郵件務必確認電子郵件地址的正確性，駭客可能將郵件地址的英文字母小寫改成大寫或相似字等方式，偽冒成主管或合作夥伴。

3、不開啟不明寄件者或可疑標題的郵件，勿點擊郵件中的連結及附檔，進入可疑網站不隨意輸入帳密和個資，即使看起來像官方網站，也要確認網址的正確性，以免被駭客利用釣魚網站竊取帳戶資訊或被暗植木馬程式。

4、建議不論個人或企業都應定期將系統進行更新，安裝防毒軟體與防火牆，確保設備軟體處於最新版本，以免被駭客利用資安漏洞進行攻擊。

5、建議企業落實對員工的資安宣導，定期舉辦資安教育訓練及社交工程演練。疫情期間許多企業讓員工遠距在家上班，員工家中設備網路安全防護不足，也是企業應宣導及協助的部分。

本案來源台灣電腦網路危機處理暨協調中心網站