機關安全維護宣導—淺談資通安全最弱環節

＊「人」是資安的最弱環節

資通安全的整體安全強度，取決於系統中最弱環節，而政府機關及企業組織中，「人」往往是最容易造成資安事件的原因。近年重大資安事件層出不窮，政府機關及企業組織無不聞駭色變，紛紛提高了資安防護的經費與人力以對抗駭客入侵。但在資通安全領域有一句名言，「資通安全的整體安全強度，取決於系統中最弱環節」，而「人」就是被公認為是這裡所指的最弱環節，從日益猖獗的網絡釣魚詐騙似乎也印證了此一論點，不管是臉書、LINE，或是簡訊，總是有推陳出新的新詐騙內容。

＊假冒銀行發送簡訊客戶損失數百萬元

以近期的新聞事件為例，110 年 1 月底，駭客偽冒國泰世華網銀發送釣魚簡訊，內容為：「您的銀行帳戶顯示異常，請立即登入綁定用戶資料，否則帳戶將凍結使用」，訊息下方同時附上銀行網址要求民眾登入網路銀行。許多人驚見此訊息，心急立即點進此連結網站，而不幸被竊取其用戶代號及密碼，已有多位國泰世華網銀用戶上當；帳戶內資金被盜轉出去，短短 3 天內就有 21 人被害，損失金額高達 3 百萬元。對此，國泰世華銀行已在官網及 APP 上宣導相關資訊並暫時關閉 APP 部分功能，並強調「銀行不會主動要求用戶登入網路銀行來綁定用戶資料」。

＊網路釣魚常見手法

通常駭客若要成功進行網路釣魚，首先必須精心偽裝連結網址，常用手法如將字母「i」改以數字「1」取代，或是字母「w」改以連續兩個「vv」取代等方式，而此次國泰世華詐騙案所使用的偽裝手法就是將真實網址「www.cathaybk.com」改為「www.cathay-bk.com」，由於網址名稱太過接近，難怪用戶難

以察覺，點了連結後當然就會被導向偽裝的惡意網站。

＊防範網路釣魚之自救方式

若民眾收到任何要求登入網路銀行的通知，建議可先與銀行確認，切勿直接在簡訊上點擊連結。另為避免不小心點擊到來歷不明的網址，建議民眾可以養成記住常用銀行網址的習慣，或將銀行網址加入瀏覽器書籤，另外也可利用搜尋引擎找到正確網站，以減少被釣魚網站詐騙的風險。一旦懷疑自己可能已經中招，除儘速確認帳戶狀態外，另外應該趕快變更密碼，以搶在駭客前保護好帳戶資金。另外，若自己曾在多個不同網路服務中使用同一組帳號密碼，例如網路銀行、個人信箱、社群媒體及購物網站等，也必須一併更換，以避免駭客利用所竊取到之帳密資料進行多方嘗試。

~~節錄自清流雙月刊 110 年 9 月號~~

~~政風室 關心您