從日常網路使用行為談資通安全

◎魯晏汝

某個風光明媚的下午，公司員工正埋頭苦幹，期待下班後的美好週休假日。但小陳一行人這時正在會議室裡上著資安教育的課程，臺上的講師說明請大家來上這門課的原因：「各位知道為什麼你們要來上這門課嗎？因為之前公司發了封測試信，標題是時下最熱門的新聞話題人物富少爺的不雅光碟，大家因為好奇心點選了這封信，所以才要來上這堂課。」臺下學員聽到老師這麼說，每個人都很不好意思地低著頭，因為自己一時好奇開啟了這封信，感覺挺沒面子的。

老師又說，這次的電子郵件測試就是利用人性的弱點，發送一些能吸引人點閱的郵件標題，讓人因好奇心而點開電子郵件或附件，隱藏在裡面的惡意程式就會自動安裝在電腦裡，造成電腦裡的個人資料被竊取，或是鍵盤被側錄導致輸入的帳戶資訊外洩，這種利用人性弱點的手法稱為是「社交工程」。社交工程是近幾年來常見的駭客攻擊手法，因為人性的因素是資安防護中最弱也最難控制的一環，資訊系統的防護可以藉由安裝防毒軟體、架設防火牆等來防堵外界的入侵，但是人性的防火牆不管再堅固都有可能因為一時的不查而受騙，所以社交工程可說是利用人性的好奇心或是容易受騙上當來破解人性的防火牆。

像這次的案例，就是利用大家對時下熱門新聞的好奇，透過網路釣魚的手法來引誘使用者上當，一旦點選後就會被安裝後門程式，自動監控電腦操作的一舉一動，或是控制這臺電腦，將此電腦做為跳板，用以入侵其他電腦，造成資安防護上嚴重的漏洞。正因為社交工程是利用人性的弱點來做攻擊，所以很難像資訊系統一樣做到完善的防範，只能透過加強宣導及訓練的方式，提高使用者在網路使用上的警覺心，不隨便點選來路不明的網址，下載安裝檔案時要確認是官方軟體等。

老師說到這裡停頓了一下，看到學員們面有難色，決定再多舉一些常見的案例讓大家能夠更清楚一點。我們常聽到跟社交工程有關的還有像是收到朋友的信，主旨可能是「我的出遊照」、「我的小孩照片」等，點選進去後是「.zip」的檔案，解壓縮後可能的附檔名為「.exe、.com、.bat、.scr、.pif、.lnk」的檔案，這些都是常見的惡意程式執行檔；此外像是直接隱藏在圖片中的惡意程式，當收到這些含有惡意程式的圖片，不需解除壓縮，只要誤點圖片就會感染病毒，造成重大的損失。

經由這堂課，小陳一行人終於對「社交工程」有進一步的了解。其實日常生活中，我們常會收到朋友傳送的檔案或是 email 郵件，但由於傳送或寄件者是認識的人，大家往往都會直接點選開啟，為了確保安全，我們應先確認傳送者是否為朋友本人，及傳送的內容是否含有惡意程式，才能避免不必要的損失。

（文摘自法務部調查局-清流月刊）