淺談電子郵件社交工程演練

◎吳信東

資訊安全工作一直都是各公、私立機關、公司、學校的電腦部門最重要的工作之一，資訊安全除了仰賴價格不便宜的軟、硬體設備，如入侵防禦系統（IPS, Intrusion Prevention System)、防火牆系統、防毒軟體、郵件過濾系統及漏洞修補系統…等之外，更重要的是，所有的電腦使用者也必須要有高度的警覺心，對於任何可疑的檔案複製、超連結、電子郵件，以及上、下載傳輸資料，都要小心謹慎地使用，避免因為一時的疏忽，輕則個人的電腦資料遭毀損或竊取，重則整個機關、公司、學校的資料被竊取或毀損。要提高電腦使用者的警覺心，資訊人員便需要定期或不定期辦理各種資安工作演練。

電腦使用者之間互相傳遞或分享照片、檔案、訊息等，可以使用的工具相當多，常見的包括社群軟體（如臉書 Facebook)、Skype、Line 及雲端硬碟，而電子郵件可以算是歷史最久，也依然最普遍被使用的工具。各式各樣利用電子郵件的攻擊和威脅，如病毒郵件、釣魚郵件、炸彈郵件、內部異常濫發郵件等攻擊，也如影隨形存在至今。如何提醒電腦使用者不要開啟來路不明的電子郵件，或可疑的電子郵件，不僅成了資訊管理人員的重要工作之一，也是資安工作重要的一環。

為了訓練及養成電腦使用者不開啟可疑或來路不明電子郵件的習慣，資訊管理人員大都使用「電子郵件社交工程演練」方式，即利用假名字的寄件者，以吸引人閱讀的郵件主旨，誘惑收件人打開電子郵件，甚至點閱該郵件的附件，進而回傳至系統後台，統計有哪些電腦使用者點閱了多少封可疑的電子郵件；資訊人員便可針對警戒心較弱的同仁，加強教育訓練宣導，以提高資訊系統的安全度。

另外，社交工程演練的電子郵件，必須具備多樣性才足以吸引使用者開啟。以筆者服務的機關而言，最近一次的演練郵件，類型包括休閒、娛樂、情色、保健、財經、政治等方面，郵件主旨如「Candy Crush Saga 全關卡破關攻略」、「主播吳 0 潔睡衣半開」、「善存的新聞—有在吃的朋友看清楚了」、「Costco 十大必買」、「三流說風暴—七成網友認為陳○文發言失當」、「睡不好又打呼 罹患惡性腦癌風險提高 47%」等；其中被開啟點閱的信件，經過統計後，最高的是「善存的新聞—有在吃的朋友看清楚了」及「Candy Crush Saga 全關卡破關攻略」,顯見保健資訊和熱門的 Candy 遊戲，比較容易吸引電腦使用者開啟閱讀；而原先以為可以獲得較高開啟率的情色郵件，可能因為電腦使用者易產生警覺心，實際被開啟率反而不高。

電子郵件社交工程演練本來應該是一種長期性、持續的演練工作，這樣才能時時讓電腦使用者有所警覺，不會輕易開啟可疑的信件。但是在實務上，礙於機關資訊人力有限，所以通常只能擇定一段時間範圍內（例如1年2次或每季1次），進行彈性不定時演練；以筆者服務的機關而言，101年進行了2次演練，第1次演練人數為803位同仁，其中188位同仁開啟郵件，112位同仁點閱郵件附件或點閱超連結，開啟率及點閱率分別為23.41%及13.81%；第2次演練人數為823位同仁，其中158位同仁開啟郵件及80位同仁點閱郵件附件或點閱超連結，開啟率及點閱率分別為19.19%及9.27%；102年第1次演練結果，演練人數為827位同仁，其中152位同仁開啟郵件及36位同仁點閱郵件附件或點閱超連結，開啟率及點閱率分別為18.37%及4.35%。

由這3次演練成果比較，開啟率由23.41%下降到18.37%，點閱率由13.81%下降到4.35%，顯見透過機關內部經常性的宣導，再加上實際演練後，電腦使用者確實會產生警覺心，因此開啟率及點閱率均有進步；但開啟率在101年第2次演練由19.19%到102年第1次演練僅下降到18.37%，進步較小，分析其原因，可能是有部分新進同仁初到機關工作，對於可疑電子郵件的警覺心尚未建立，致機關整體進步有限，也顯示機關對新進同仁的電腦教育訓練還可以再加強。

為了讓開啟及點閱演練郵件的同仁有所警惕，機關可以適當地以各部門為單位，公布演練不合格的同仁名單，通常這樣所得到的警惕效果相當大；但也會有部分同仁較難接受演練未通過的結果，進而打電話或親自到資訊中心詢問，此時資訊人員可提供更完整的演練資訊，如開啟演練信件的電腦IP、開啟日期、開啟時間等，並再耐心說明演練的目的及資訊安全的重要性，藉此加強宣導。

防範惡意電子郵件社交工程演練，只是資訊安全工作其中的一環；整體資訊安全的工作相當繁雜，其他重點工作尚有：從作業要點的訂定開始，就必須考量資安預防及危機處理；資訊人員本身也要不斷充實各種資安新知，甚至是通過專業證照考試；如果機關經費足夠的話，可以申請資訊安全管理系統ISMS（Information Security Management System）的第三者驗證；另外如系統防護設備的購置、安裝及設定等。包括這些防護設備的持續維護及更新，都需要資訊人員長期不斷地投入。希望藉由本篇淺顯的短文，讓電腦使用者了解電子郵件社交工程演練的意義、重要性，及整體資訊安全工作的概略。（文摘自法務部調查局清流月刊103年2月號）