企業或機關應加強宣導資安議題並建置防範措施，員工則應確實遵守資訊安全措施與相關程序，時時提高警覺。

# 從人性的弱點談社交工程的資安議題

◎魯晏汝

某天下午，忙裡偷閒的小如正一邊聽著音樂，一邊和朋友聊MSN。突然，她收到好友小明傳來的MSN訊息，點開一看內容是「你現在有空嗎？」小如馬上回覆說：「沒事呀，怎麼了？」小明回應：「你可以幫我買1,000元的麥卡（my card）嗎？只要到便利商店跟店員說你要買點數卡，然後把卡片上的儲值序號告訴我就可以了，錢，我之後會給你的。」不疑有他的小如心想「只是買點數卡嘛，小事一件」，於是很乾脆地答應小明了。小明見到小如答應後便緊接著說：「可以麻煩妳現在去買嗎？我急著要用，我在線上等妳回來。」小如知道小明急著要用後，便立刻去附近的便利商店買了1,000元的my card，然後趕快回來將儲值卡的序號告訴在MSN上等待的小明；沒想到小明得到小如回覆的序號後，就馬上下線找不到人了。

小如這時心想「奇怪！怎麼跟平時的小明不太一樣，最少應該說聲謝謝或說些客套話，沒想到就這樣離線了。」過了幾天，在朋友聚餐時見到小明，也不見小明有任何要還錢的跡象，好像這件事從來沒發生過一樣。內向的小如也不好意思主動開口向小明要回這1,000元，但卻很在意這1,000是否能拿回來，於是就一直把這件事擱在心上。一個月後，小如和姐妹淘小華在下午茶的聚會上，小如就把這件事說給小華聽，請小華幫她評評理，順便問問小華有沒有什麼好方法幫她把這1,000元要回來。

不料小華一聽完小如的敘述後，直接對她說：「小如，妳被騙了！」小如很納悶地問：「被騙了！為什麼？不就是小明在MSN上跟我說要我去幫他買點數卡嗎，為什麼是被騙呢？」小華見狀便語重心長地說：「可是，妳確定請妳幫忙買點數卡的人，真的是小明本人嗎？」

以上這段故事，相信對很多人來說都不陌生，許多的人都有收過類似的訊息，這些稱為是「社交工程」（Social Engineering）。社交工程可說是利用人性的弱點，透過話術的影響力或說服力來騙取他人的個人隱私、組織機密，或是誘使從事某些交易、動作，以獲得有用資訊或不法所得的一種技巧。由於人性的因素可說是資安防護措施中最弱的一環，社交工程即是利用人性容易受騙上當的弱點，破解人性的防火牆，可說是近幾年來駭客最常用的攻擊手法。社交工程的攻擊手法有很多種，常聽到的像是上例中的MSN點數卡詐騙，此外還有像是電話詐騙、網路釣魚、圖片中的惡意程式、偽裝的修補程式等等；我們可就這幾種攻擊手法分別舉例說明。

**一、電話詐騙：**電話詐騙顧名思義就是透過電話進行的詐騙行為。例如常聽見的有「你的小孩被綁架了，現在正在我的手上，如果要救他的話就準備1,000萬元的贖金過來…」，或者是「我是某某檢察官，我們查到你的帳戶資料被盜用，請立刻依照我們的指示操作ATM…」、「我們是某某購物，你之前在我們這裡購買的商品因為選擇超商取貨，在付款時超商店員不小心誤選了分期付款，造成有循環利息；如果要停止的話請依照我們的指示操作…」。以上這些都是利用人性害怕的弱點，擔心不照做的話，親人可能會受害，或造成財務上的損失。

**二、惡意電子郵件程式：**利用社交工程的概念，將病毒、蠕蟲或惡意程式隱藏在電子郵件中。例如偽裝成朋友寄來的信件，標題為「我要結婚了」，附件放著「婚紗照.zip」要分享給收件者，但是點開壓縮檔後可能是副檔名為「.exe、.com、.bat、.scr、.pif、.lnk」的檔案。這些副檔名都是惡意程式常用的執行檔類型，一旦點開這些執行檔後，惡意程式會自動在電腦裡進行安裝，竊取電腦裡的資料或是網路銀行的帳戶帳號、密碼等資訊。

**三、網路釣魚：**網路釣魚泛指利用社交工程或技術性的手法，引誘使用者點擊（click）假網頁。例如偽造為拍賣網站或是電子郵件信箱，誘騙使用者輸入帳號密碼，進而竊取其帳戶資料；由於其和原網頁相似度極高，很容易誤使他人受騙點擊。常見的散布手法還有廣告信件（利用聳動的標題或是知名大廠的名義發送郵件，通知收件人必須登入連結重新驗證身分，進而竊取使用者輸入的個人資料）、網址置換（偽造網站的網址，乍看之下網址與原本官網相同，但實際上可能將英文的O置換為數字的0，英文的Ｉ換成數字的１）、縮網址（利用部分網站提供縮網址的服務，將假網頁的縮址貼在各大BBS或論壇中，誘騙使用者點擊）等等。

**四、圖片中的惡意程式：**透過明星或色情照片散布惡意程式，也是常見的社交工程攻擊手法之一，利用使用者的好奇心，點選圖片後就會感染病毒，造成重大損失。

**五、偽裝修補程式：**另一種常見的社交工程攻擊手法就是偽裝成知名軟體的修補程式（例如微軟更新修補程式），因為一般使用者並不會認為這是來路不明的程式，往往直接下載並安裝這類程式。安裝後這些惡意程式非但不能修補系統漏洞，反而有可能在使用者的電腦裡安裝遠端控制的木馬程式，竊取使用者電腦裡的資料或是側錄其鍵盤輸入的帳號密碼等資訊。

在了解常見的攻擊手法後，更重要的是要知道該如何防範。在企業中，只要員工對於社交工程的安全防範措施沒有足夠的認知或是警覺度不高，無論資安措施做得如何完善，惡意人士都可以輕易地竊取個人帳號資料、財務資料，或是公司的重大資訊。所以企業應不定時宣導及安排員工教育訓練，提高員工的警覺心及危機意識，只要出現類似的社交工程攻擊手法，都應保持警覺並小心求證。此外，員工也應遵守公司的安全政策與程序，不開啟來路不明的電子郵件或網頁；如有必要，在提供任何資訊前，也應確認要求者的身分並經過相關的授權程序。最後是建立通報作業程序，當發生疑似社交工程攻擊時，應立即與相關單位聯繫並完整通報。

社交工程主要是利用人性的弱點做攻擊，所以很難做到完全的防範。使用者只能時時提高警覺，不點選來路不明的網址及檔案，遇到任何要求時，也要盡可能地確認是否為真。只要時時具備高度的警覺心並保持危機意識，那麼社交工程攻擊一點也不可怕。

**（作者服務於特力股份有限公司人力資源部）**

▲Top

委外代工簽訂保密契約及交付機密資料時，該注意那些事項？如果對方違約，又該負那些責任？

# 委外代工製作的資訊安全

◎魯明德

隨著景氣好轉，公司的業務也越來越多。某天，小潘的主管小強告訴他，公司剛剛拿到國內某安全機構的保密手機生產訂單，但是，所有參與生產的工作人員都要簽訂保密合約。小潘頓時感到納悶，保密合約到底是什麼？要保什麼密？為什麼要簽保密合約？於是菜鳥小潘鼓起勇氣問了他的小強主管；但是，小強只跟他說就是要簽，不必問什麼理由。小潘得不到答案，決定趁著跟司馬特老師見面的機會，要好好地問一下。

這天，小潘與司馬特老師又在校門口的咖啡廳見面，二人在焦糖瑪琪朵還沒上桌前，小潘乘機趕快提問，於是就把當天的情形敘述一遍，並且問司馬特老師：「為什麼幫人家代工，還要簽保密合約？」這時焦糖瑪琪朵也上桌了，司馬特老師喝一口後便緩緩道來。

現在很多產業都朝向專業分工，只會把核心能力放在自己的公司，其餘的部分會找專業廠代工（Outsourcing），即使像鴻海這麼大的公司，也不是所有的零組件都在自己的工廠製作。而核心能力之所以稱為核心，自然就是別人不會的；但是，相同技術領域的業者，其技術背景相似，當看過別人的設計後，就有可能學會，甚至將技術洩漏出去。

面對此種狀況，企業在委外合約上，就會要求外包商要簽訂保密協議（Non-Disclosure Agreement, NDA）；外包商在承受了保密的責任後，自然會將保密的責任再轉嫁給員工，要求員工負相關責任，不能把所知的技術洩漏出去。

而保密手機的設計、加密演算法…等，都涉及國家安全，如果外流，將會造成國家安全的損害，當然得要求得標的廠商確實保密，並將責任加諸其身，所以他（小強）自然會轉而要求員工遵守。

小潘聽完司馬特老師的說明，頻頻點頭。這時可口的千層派也上桌了，吃一口千層派後，小潘又接著問：保密合約的內容通常寫些什麼？司馬特老師吞下口中的千層派後，娓娓道來。

保密合約首先要載明保密的標的，接著明列簽訂保密協議者在取得機密資料後，可以做那些事，不可以做那些事，如果違約要負什麼責任等；此外，也會要求業者對其所屬員工負起相同的保密責任。

小潘趁著司馬特老師喝咖啡的空檔，又問：委託業者給了這麼多資料，我們怎麼知道拿到的資料那些是機密的？那些不是？司馬特老師喝口焦糖瑪琪朵後，接著說：當你要把機密資料交付給業者時，應該在文件上明確地註記機密等級並編號，並且要列冊讓接收者簽名，以釐清責任；如果資料不是一次給完，而是分批給，則在每次交付機密資料時，都要不厭其煩地造冊、清點、簽收。

小潘邊聽邊做筆記，並發表他的心得：這麼說來，外包合約是不是應該也要註明如果合約完成後，這些機密資料要交還給委託單位？司馬特老師點點頭，為了避免機密資料外洩，最好的方法就是把文件收回，這點一定要寫在合約中，以免日後有爭議。

小潘聽了司馬特老師的說明，心想：這個保密協議還真是有學問。這時他又想到法定權利都有一個期限，不知道保密協議有沒有失效的時間？於是，他又把握機會問司馬特老師。

司馬特老師喝了口咖啡後繼續說：保密期限要視個案來決定。小潘這時又迷惑了，心想：視個案決定不就是沒有標準了嗎？司馬特老師果然一眼看穿愛徒的心思，接著又說：因為每個個案的狀況都不一樣，所以，不能訂一個放諸四海皆準的準則，必須要保有適當的彈性。

以保密手機的案例來說，因為手機是3C產品，生命週期不長，２至３年就可能淘汰，而且加密演算法也會與時俱進，也許５至10年後，這些演算法都成為過氣的技術，而保密手機也都換新的了。因此，它的保密期限可以定在技術淘汰之後，當該技術及產品不再使用，也就可以不用保密了。

另外還有一種技術態樣，如果它是企業的營運必需品，它的思維又不一樣了；一旦這個資訊遭到外洩，勢必會影響未來的營運，那就必須在保密合約中約定永久保密。

小潘聽著聽著仍覺疑惑…，什麼資訊需要永久保密？他想起以前當兵期間，在簽辦公文、擬訂機密等級時，長官曾講過要符合國家機密保護法；但就算是國家機密保護法中規定列為絕對機密的資料，其保存期限最長也只有30年，時間到了就要解密，怎麼會有永久保密的資訊？

司馬特老師喝口咖啡後繼續說：國家資訊涉及人民知的權利，為了監督政府的施政、避免執政者濫權，所以要訂出解密的時間，讓人民知道政府在做什麼。但是企業就不一樣了，很多資訊一旦外洩，即可能影響營運。

如可口可樂的配方，就是它成為與百事可樂競爭的最大優勢。這個配方在1886年由藥劑師John Pemberton研發出來，配方的內容如果外洩的話，則任何人可能都可以做出跟可口可樂一樣口味的可樂。可口可樂公司於1892年成立後，擔心這個配方會落入他人手裡，於是將配方鎖在亞特蘭大（Atlanta）的太陽信託銀行（SunTrust Bank）的保險庫內，將近125年的時間，均未遭到破解。

小潘聽完司馬特老師深入淺出的解釋，頓時豁然開朗，原來保密協議還有這麼多學問啊！這個世界上真是處處是學問。隨著太陽下山，師徒也必須在咖啡的香味中，結束這次的下午茶約會。

**(作者服務於新心科技有限公司並任科技大學資訊管理系講師)**

▲Top