網路安全的社交工程

陳嘉玫

電腦網路除了帶來便利的生活外，也伴隨著各種網路犯罪手法的快速成長，已對個人資料、財產、公司系統等產生極大的威脅。

什麼是社交工程

定義　隨著電腦科技的進步，電腦網路已成爲社會發展與人們日常生活中不可或缺的重要工具，舉凡訂票系統、醫療系統、購物網站、社群網站等，都需要電腦網路才能使用。因此，人們在食、衣、住、行、育、樂等方面已與電腦網路密可不分。但是電腦網路除了帶來便利的生活外，也伴隨著各種網路犯罪手法的快速成長，已對個人資料、財產、公司系統等產生極大的威脅。

儘管不斷研發出新技術來加強資訊防護，但整個資訊系統環節中，最脆弱的部分就是「電腦使用者」。因爲只要有「人」，就必然有弱點，因此近年來「社交工程」（social engineering）成爲最常用且難以防範的攻擊手法。

社交工程是利用人性的弱點進行詐騙，是一種非「全面」技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行爲。例如駭客通常藉由電話、電子郵件或假扮身分，問些看似無關緊要的問題來進行社交工程。這些手法的特性是攻擊者並不需具備高深的駭客技術或攻擊工具，僅利用人缺乏警覺性或有好奇心的弱點，就可輕鬆騙取個人資料、系統帳號密碼等重要資料，令人防不勝防。

社交工程是利用人性的弱點進行詐騙，是一種非「全面」技術性的資訊安全攻擊方式，藉由人際關係的互動進行犯罪行為。

就算擁有高科技的資安設備、高效能的防護系統，只要需要人為操作，就有遭受社交工程攻擊的危機。

案例　2010年1月網路巨擘谷歌（Google）帳號遭駭客入侵事件，在國際間引起喧然大波。探究其攻擊手法，不外乎駭客一開始先鎖定特定人士，接著運用多重管道寄送夾帶惡意附件檔案的社交工程手法，搭配IE零時差漏洞，造成谷歌內部員工一時不察下載惡意檔案。

這惡意檔案一旦執行後，便自動安裝後門程式，從被感染的系統上竊取機密資訊並傳送給遠端的駭客。據說那一次的攻擊不僅造成重要的原始碼資料遭竊取，另一項重大損失是密碼系統，該密碼系統掌握全球數百萬用戶登入谷歌的電子郵件與商業應用等服務，影響甚大。

據網路安全專家表示，谷歌在網路硬體和軟體的防禦系統上所投入的資源相當龐大，網路安全防備系統也算相當完善，但是仍避免不了遭受社交工程的攻擊。由此可見，就算擁有高科技的資安設備、高效能的防護系統，只要需要人為操作，就有遭受社交工程攻擊的危機。

攻擊目的　駭客利用社交工程的目的，主要有以下幾種：攻擊目的一誘使被害人安裝破壞性的惡意程式，而造成系統破壞或網路癱瘓；廣告目的一藉由社交工程不斷開啓惡意廣告；金錢目的一網路犯罪大多數都是以金錢爲目的，利用社交工程竊取而來的機密個人資料與系統帳密，可以直接盜取金錢或至黑市中販賣。根據賽門鐵克（Symantec）2010年4～6月情報季刊，黑市論壇中的個資交易比率與價值，其中排名第一的是信用卡資料，占28%。

攻擊管道與手法

攻擊管道　電話一社交工程手法最早使用的管道是以電話爲媒介，假冒各種身分，利用公司員工容易相信與缺乏警覺性的人性弱點，誘騙出帳號、密碼等機密資料。

排名	項目	百分比	價格（美金）
1	信用卡（credit cards）	28%	1～30
2	銀行帳戶（bank accounts）	24%	10～125
3	電子郵件帳戶（email accounts）	8%	5～12
4	電子郵件位址（email addresses）	5%	5～10／MB
5	信用卡背磁條內容（credit card dump）	4%	無定價
6	R57及C99軟體（R57 & C99 shells）	3%	2～5
7	完整ID（full identity）	3%	3～20
8	郵件程式（mailers）	3%	1～5
9	攻擊用工具程式（attack toolkits）	3%	5～20或每月120
10	付款服務（cash-out services）	2%	200～100或50～70%

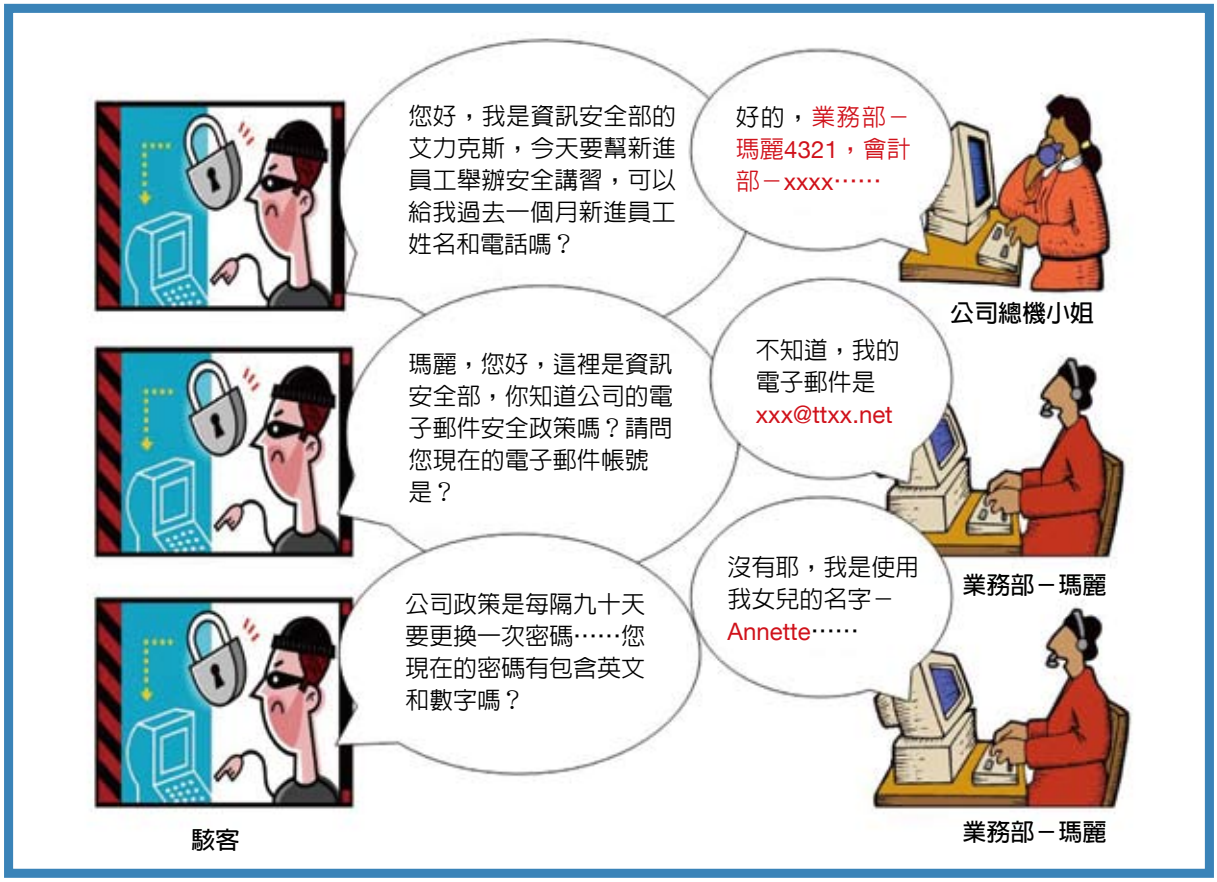
資料來源：賽門鐵克2010年4～6月情報季刊

案例一：2010年在美國拉斯維加斯舉辦的Defcon大會，進行以社交工程爲主題的駭客競賽，發現美國10家大型科技、石油和零售企業被隨機選中的五十幾名員工中，只有3位察覺有異，沒有提供任何回答就掛斷電話，其餘的竟毫無警覺地在電話中洩露公司的敏感資訊，這些資訊都能被駭客用來攻擊公司的電腦網路。

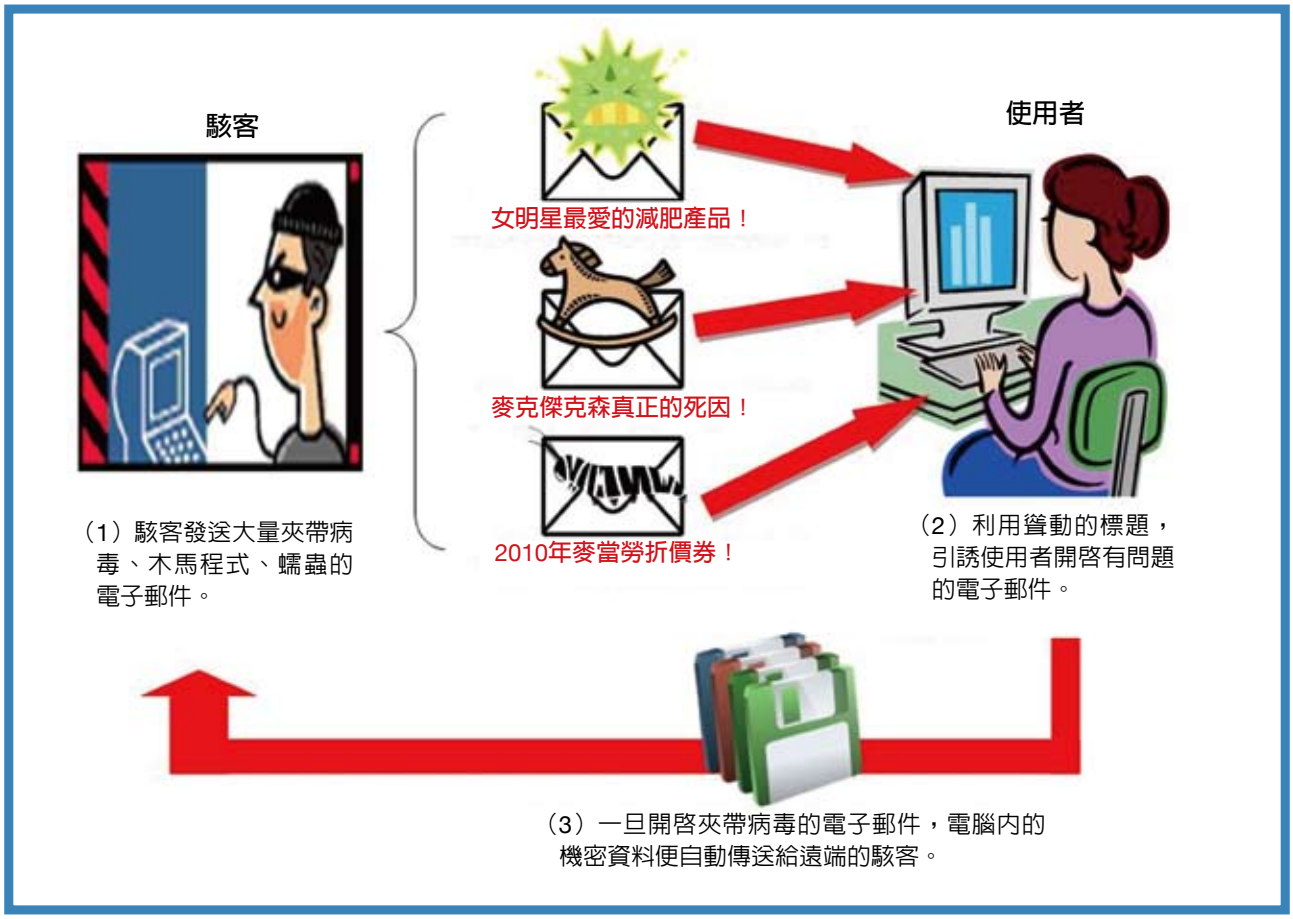
案例二：2006年美國FBI發現一個以行動電話交友騙術來入侵電腦的手法。駭客先透過電話簡訊的方式，感謝收訊人訂閱了他們的交友服務（當然是假冒的），並聲明這個交友服務每天兩美元的費用會合併在電話帳單中。如果收到簡訊的人要取消服務，可以連結到http://www.irrealhost.com取消。

當消費者連到這網站時，消費者會被要求輸入他們的手機號碼，同時會被詢問是否要執行一個程式來取消交友服務。當這程式執行後，消費者的電腦上便被植入後門程式，受害者的電腦中的檔案（host file）也會被修改，使得受害人無法連到防毒廠商的網站。同時受害人的電腦也會變成所謂的「殭屍電腦」（zombie）網路的一員，讓駭客可以遠端遙控這電腦。

電子郵件—駭客利用電子郵件夾帶病毒、木馬等惡意程式，信件標題再藉由熱門時事、養身保健或情色相關等聳動標題，引誘使用者開啓郵件中所夾帶的惡意程式。甚至僞冒寄件人，騙取使用者的信任，進而開啓郵件。



引用《駭客大騙局》書中的案例—利用電話進行社交工程的簡單案例。



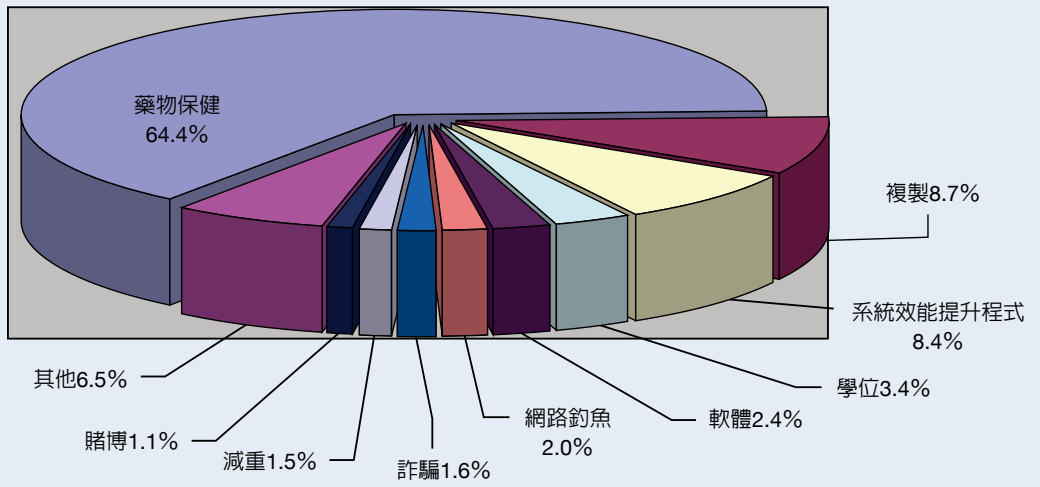
利用電子郵件進行社交工程的過程

據調查，目前全球每天流通的垃圾郵件約1,150億封，由於垃圾郵件數量愈多，使用者點閱的可能性愈大。雖然多年來垃圾郵件一直是利用惡意的電子郵件附件來感染使用者，但前年出現了大量使用社交工程的垃圾郵件，以方便網路犯罪者從中獲利。2010年第二季趨勢科技網路威脅報告統計指出，垃圾郵件的標題以「藥物保健」爲最大宗，占64.4%。

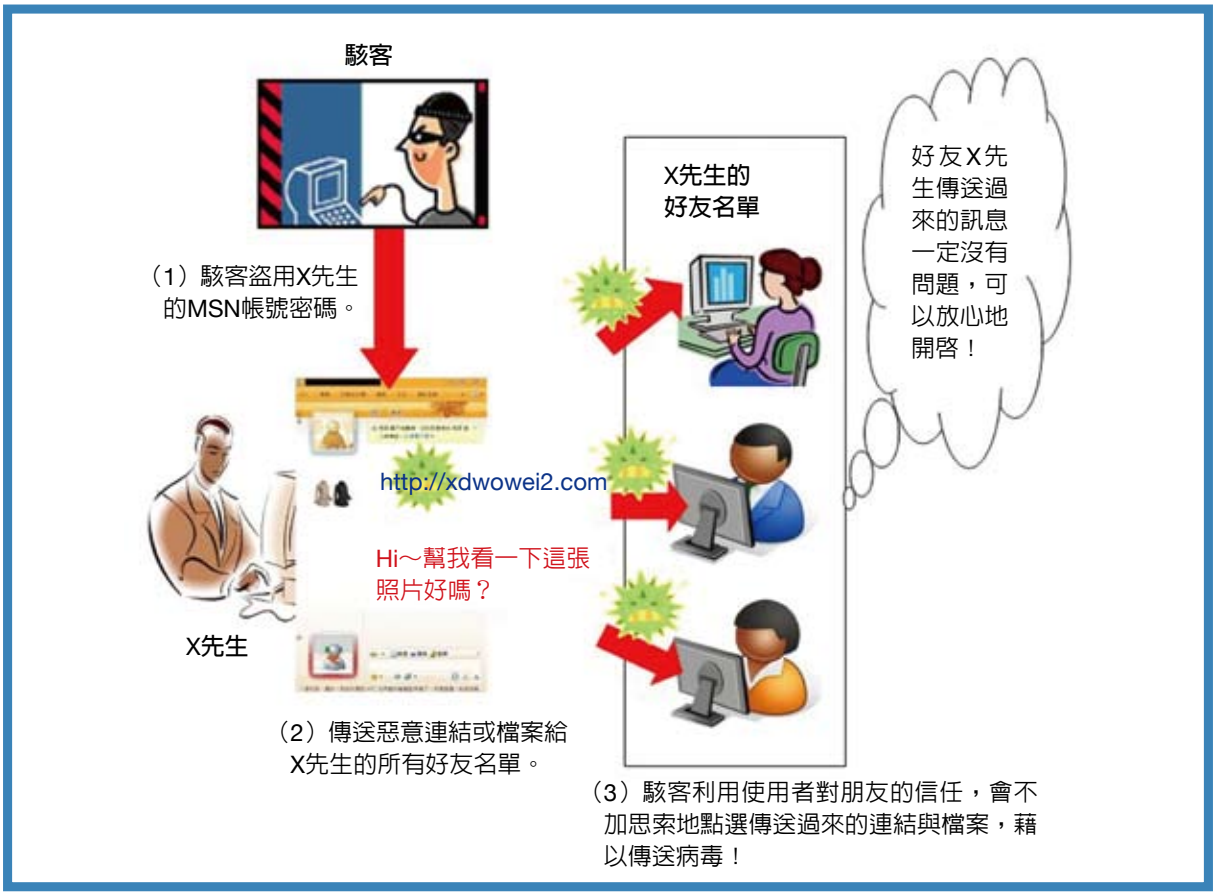
即時通訊軟體（instant message, IM）—即時通訊軟體病毒必須仰賴使用者之間互相傳遞。通常即時通訊軟體的使用者並不會接受來自陌生人的檔案或訊息，因此駭客必須先取得一個眞實使用者的帳號來發送病毒訊息。一般使用者收到來自朋友傳送的訊息，通常會毫無戒心地點選連結或下載檔案，進而感染病毒。而遭受感染的受害電腦又會自動傳送這病毒訊息給其他連絡人，藉以擴散病毒的感染範圍。

案例一：2007年5月，在西班牙有一個訊息，與使用MSN Messenger一樣的方式，只要接收訊息的人按下連結，據說會顯示出美國總統布希的動畫。但其實它會下載一個蠕蟲病毒到受害者電腦中。

案例二：2010年，台灣警方發現一種利用MSN的詐騙手法。歹徒首先竊取MSN帳號、密碼後，再以該帳號上線，假冒被害人身分與親朋好友閒話家常，建立熟悉感與信任度。爲避免被害人懷疑，歹徒第一次的攀談通常不會立刻提出額外要求，會耐心等待被害人第二次上線，才以有事無法出門或人在國外急著要用爲理由，要民眾到超商代買遊戲點數，並要求民眾把遊戲點數卡的卡號、密碼在MSN中告知歹徒。待日後協助代購民眾發現事有蹊蹺時，才發現原來是對方的MSN帳號遭人盜用並進行詐騙。



2010年第二季趨勢科技網路威脅報告統計指出，垃圾郵件的標題以「藥物保健」為最大宗，占64.4%。
（圖片來源：Q2 2010 Internet Threats Trend Report）



駭客利用MSN進行社交工程的過程

社群網站（social networking site, SNS）—Cellopoint Global Anti-spam Center最新的監控數據顯示，因爲社群網站的流行，駭客攻擊目標從傳統的電子郵件逐漸轉移至此，其中特別熱門的Facebook、Plurk、Twitter等網站就成爲主要目標。攻擊手法則結合木馬程式、僵屍網路、社交工程及郵件釣魚技術，成爲資安威脅新趨勢。

案例一：木馬程式Koobface以耶誕節主題影片爲誘餌，在2009年12月期間對Facebook用戶發動了一波垃圾訊息攻擊；另一個木馬程式ZBOT把攻擊目標鎖定Facebook用戶，攻擊手法是利用垃圾郵件把他們引誘至網路釣魚頁面中，企圖竊取個人資料。

案例二：2010年2月，趨勢科技發現一個假借升級臉書黃金會員（Facebook gold account）的訊息，以金錢詐騙的社交工程手法。首先透過黃金會員可免費使用如影像交談、團體交談、布景主題（Beta版）等額外福利吸引網友下載。若網友按照指示進行，並邀請朋友一同來看這個好康，就必須先連結至一個詐騙網頁完成一個調查，網頁中要求回答完問題之後，要輸入個人手機號碼以便收到測試結果。

一旦輸入手機號碼，就代表同意支付9英磅的加入費用，以及後續每周9英磅的使用費。雖然這費用的支付已經列於服務內容及條款中，但網路詐騙者利用網友多半未詳閱條款的漏洞來發詐騙財。

網路釣魚—僞裝知名企業或機關單位寄發的電子郵件，通知收件人必須重新驗證密碼，或登入某網址輸入個人資料等，這種詐騙稱爲網路釣魚。收件人若未小心求證而連結了郵件中的鏈結，就可能下載惡意程式；或者在假網頁上輸入了帳號密碼或信用卡資料等，造成銀行戶頭被盜領或盜刷等嚴重後果。

攻擊手法　社交工程就是一種利用人性弱點的詐騙技術，藉由人與人之間的互動而形成的犯罪行爲，缺乏警覺性的使用者很容易掉入陷阱中。駭客經常使用下列手法誘騙人們的信任，進而竊取重要資料。

直接索取資訊—駭客佯裝資訊人員或僞裝委外

美國銀行網站與假冒的釣魚網站

偽裝知名企業或機關單位寄發的電子郵件，通知收件人必須重新驗證密碼，或登入某網址輸入個人資料等，這種詐騙稱為網路釣魚。

廠商的維護人員，甚至是上級主管，利用電話直接套出公司資料、帳號、密碼等機密資訊。

利用人性弱點—好奇：有一個案例是2009年流行天王麥可傑克森（Michael Jackson）驟逝的消息傳出後，不到一天的時間，資安業者已偵測到，駭客以「麥可傑克森是被冤枉的」爲主題發送惡意連結，引誘網友們點選；憐憫：利用「尋找失蹤兒」、「發揮您的愛心，一起響應賑災捐款活動」等標題的郵件，引誘使用者發揮憐憫之心，進而點選郵件；貪婪：利用人們貪小便宜的心態，以「恭喜您中獎了」、「分享好康優惠券」、「免費軟體下載」等標題，誘騙使用者點選；恐懼：網路犯罪者利用使用者對安全威脅的恐懼，慫恿不知情的使用者安裝間諜軟體，驅使使用者點擊連結以掃描電腦或取得移除威脅的軟體。

信任關係—利用一般人對熟人的信任感，認爲熟人寄來的信件一定不會有問題的心態，駭客假冒熟人發送訊息，誘使被害人失去警戒心而上當受騙。

案例：2009年台北市一位先生接獲昔日指導教授求助借錢的電子郵件，誤以爲老師人在國外需要幫助，火速以西聯匯款（Western Union Quick Cash）把錢匯至英國。事後透過電話向學校詢問，才發現教授根本沒有出國。而發信借錢的歹徒是以駭客入侵方式取得了教授Gmail信箱通訊錄資料，再假冒教授寄出借錢郵件。這位教授曾在幾天前接到一封冒充信箱管理發出的確認帳號信件，他填寫帳號、密碼、身分證號後回信不久，就發現一整天無法使用信箱，遭盜用的帳號也無法使用。

身分僞裝—駭客事先利用各種管道蒐集被害人的資料，再僞裝爲銀行行員、警察、客服人員等身分，因其掌握被害人的基本資料，很容易取得被害人的信任而大意交出帳號、密碼等機密資料。

案例：2007年有許多曾上網購物的民眾接獲自稱是網拍業者客服人員的來電，通知他網路購物付款時，轉帳設定操作不當，須至提款機操作。因個人資料、購物品項、金額核對都無誤，造成許多民眾上當匯出自己的存款。

假借調查爲由，實爲個資蒐集—不法集團經常假借問卷調查，利用填網路問卷送贈品的手法來欺騙客戶，實質目的是蒐集個人資料。

案例：2010年5月，賽門鐵克發現有駭客試圖假借一家著名快餐店的名義，向電腦用戶發放對其食品意見的調查電郵，再要求收件者在電郵中提供個人資訊以達到詐騙目的。賽門鐵克指出，用戶會被要求點擊電郵內所提供的連結，並聲稱用戶只要填妥問卷內的8條問題，便可以獲得80美元回贈。事實上，該連結只是連接至一個虛假網站，用以蒐集客戶的個人資料。

修補程式—假冒系統廠商或防毒軟體業者，寄送假的修補程式或更新程式的電子郵件，引誘使用者下載安裝。

案例：趨勢科技在2008年7月發現一款以繁體中文撰寫，夾帶聲稱是該公司推出的免費病毒移除工具「iClean解毒快手」程式的惡意郵件，在台灣地區流竄。該郵件附帶一檔名爲iclean20.rar的壓縮檔，並附有僞裝成趨勢科技網頁的解說文字，很可能導致不知情用戶執行後感染後門程式。趨勢科技警告用戶留意這攻擊手法，不要執行該附加檔。

社交工程的預防

社交工程的預防方法，包括：隨時具備危

機意識，對於任何詢問重要資料的人士，都需小心求證；單位內對權限應加以分級控管，非屬個人分內事宜，不應掌握帳號、密碼等特殊權限，防止因不了解安全等級而不慎外流重要資料；安裝防毒軟體，設定個人防火牆，並定期更新病毒碼；針對電腦應用程式應隨時更新修補程式；設定安全密碼（6～8碼，包括英數與符號字元），避免太簡單易遭破解的密碼；重要資料檔案要加密防護；相信直覺，當你感覺有一絲絲疑慮時，應相信自己的直覺，多方驗證，預防自己受騙（多一分求證，少一分損害）；碰到疑似社交工程行爲，應立即回報相關管理單位，並進行事件記錄。

防範電子郵件社交工程的方法　關閉預覽窗格，設定爲純文字讀取模式，避免開啓郵件內的超連結；確認信件來源，不要開啓可疑電子郵件（過於聳動的主旨、不正常的發信時間、陌生人或少往來對象來信、要求輸入機密資料等）；避免開啓可疑的附件檔案，如exe、dll、scr、bat、pif、com、vbs、lnk等；避免開啓與公務無關的電子郵件；避免在不安全的網站留下個人資料，包含電子郵件。

防人之心不可無

隨著資訊科技日新月異，社交工程手法也不斷翻新。目前駭客傾向採取目標式社交工程攻擊，先鎖定特定目標並蒐集相關資料，接著僞造電子郵件的寄件者來自內部員工或主管的郵件帳號等資料，信件主旨也假冒與公務相關，附件檔案進化爲平日常接觸到的應用程式格式，如Word、Excel、Powerpoint、Access、PDF、WinZIP、WinRAR等，再結合木馬程式、零時差漏洞、釣魚網站等先進惡意程式技術，利用精密的混合式攻擊手法，使用者很容易一時疏忽就掉入陷阱中。

預測未來社交工程的技巧，會趨向以更精密、更複雜的手法引誘使用者上鉤。預防社交工程，除了使用者須具備良好的電腦使用習慣外，俗話說：「防人之心不可無」，隨時保持高度的危機意識及警覺心，才能減少社交工程攻擊的傷害。

陳嘉玫
中山大學資訊管理系

深度閱讀資料

Kevin D. Mitnick & William L. Simon（2003），駭客大騙局（子玉譯），藍鯨出版社，台北。

Schneier, B. (2000) *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons Inc., Hoboken, NJ.

崔嘻，微網誌成社交工程陷阱新寵（含2007～2009主要事件一覽表），TREND 雲端運算安全趨勢BLOG部落格，http://domynews.blog.ithome.com.tw/post/1252/30017, 2011

Social Engineering: The Basics, http://www.csoonline.com/article/514063/social-engineering-the-basics?page=1, 2011

Social Engineering: Eight Common Tactics, http://www.csoonline.com/article/460135/social-engineering-eight-common-tactics?page=1, 2011

TREND科技公司技術通報，2008技術通報—目標式社交工程攻擊手法，http://tw.trendmicro.com/tw/support/tech-support/board/tech/article/20080821045654.html, 2011

預防社交工程，除了使用者須具備良好的電腦使用習慣外，還得隨時保持高度的危機意識及警覺心。