電子郵件內之警告內容與資訊素養高低是否能有效抵禦社交工程之攻擊行為?

粘敬宣[1]　陳慶文[2]
高雄第一科技大學資訊管理研究所
u9924820@nkfust.edu.tw

電子郵件內之警告內容與資訊素養高低是否能有效抵禦社交工程之攻擊行為?

粘敬宣
高雄第一科技大學資訊管理研究所
u9924820@nkfust.edu.tw

摘要

在此一資訊爆炸的時代，資訊安全議題廣泛的為人們所討論、研究。通常，企業、政府、個人與組織皆發展許多軟硬體方面以抵禦駭客的攻擊。因為目前的駭客不僅僅具有強大的資訊軟硬體技術，更具備了社交工程方面的手段如口語溝通、引誘、仿造身份、貪婪與規避懲處等心理上的弱點來向使用者發動網路釣魚、通話式的詐騙等等攻擊行為，並竊取個人資料、企業組織與政府部門機密資訊等等。

本研究主要探討社交工程中的網路釣魚其中一項手段，此手段是利用電子郵件或網站詐騙機密資訊。測試方式是，我們會利用網路釣魚的方式將電子郵件寄給有資訊背景與素養的學生，並在電子郵件中加入社交工程的警語觀察這些學生是否會被騙取個人資料，茲發現以下結論：

一、 在電子郵件內加入對社交工程的警告標語對社交工程的攻擊行為無顯著性的抵禦效果。

二、 一般來說資訊素養會隨著在學年級增加而遞增，但年級越高之學生卻不一定能夠有效辨別社交工程的攻擊而被竊取個人資料、資訊。

三、 若已經有被社交工程所詐騙的經驗，若再次遇到類似的社交工程攻擊手段依舊上當的機率會高於百分之五十。

最後本文加以探討、分析如何能夠避免社交工程在電子郵件中的攻擊行為。

關鍵詞：社交工程、網路釣魚、資訊素養。

第一章 緒論

第一節 研究背景

由於現今資訊科技基礎建設日趨完善，資訊科技設備已經成為現代人類生活不可或缺的一部分，並且網際網路日新月異的變動，使得資訊隨手可得、社會資訊素養逐步提升。近年來，電子郵件使用頻率因為網路外部性因素也呈現了爆炸性的成長，導致許多例如竊取與洩漏個人資料、詐騙手段與犯罪行為等社會議題的發生，類似此種議題的專有名詞我們將它稱之為"社交工程"，也就是以影響力或者是說服力來欺騙他人並取得自己所需、有用的資訊。在此方面，使用社交工程這類人是不需要具備有頂尖的電腦通訊技巧，只需要對疏於防範且對詐騙沒有足夠的了解的人們來下手就能夠取得個人資料、公司財務資料與帳號密碼等重要資訊。因此在使用者觀點方面需要了解如何防範社交工程的的詐騙行為與個人資料的保護是現今電子郵件上所必須注意、了解的一大目標。

而使用社交工程攻擊的種類分成許多方法，包含現今最為流行的電話詐騙之外，還有包括 1.電子郵件內的惡意連結與隱藏病毒、2. 網路釣魚、3. 圖片與影片中隱藏的惡意軟體程式、4. 偽裝的修補程式與軟體、5. 即時通訊軟體的病毒與詐騙。

目前主要社交工程攻擊方式主要方法為取得個目標的背景資訊，接著透過任何方式如 email、電話或者即時通訊軟體與受被害端交談並建立起與受害端的信任關係，再利用這些資訊向上探索取得自己所需的資訊與資料。因此不管是利用何種通訊方式，社交工程主要是利用詐騙的技巧，讓受害端將資料、資訊與機密文件提供給加害端的方式即是社交工程。

因此為了防範社交工程這類型的詐騙行為，人人應該建立與加強正確的防範觀念以及保護個人資料避免洩漏的行為。加強方式不外乎是教育訓練與平日個人資料的保護與日常宣導。

第二節 研究動機

目前詐騙行為層出不窮，許多企業避免公司機密與個人資料的外洩，皆舉行教育訓練與加強平日的宣導。但舉行了教育訓練與加強宣導後，多少還是會有許多企業機密與個人資料的洩漏。因此在加強與舉行了教育訓練與平日的提醒、宣導後是否具有對社交工程的防範的效果是值得我們探討的。本文主要研究為具有資訊背景的人在接受與加強了教育訓練或者平日的宣導、郵件內的警告後，是否還是會有人提供個人資料給加害端。因此不僅僅要舉行教育訓練與加強宣導外，更要具備相當的危機意識與警覺心，企業方面則要制訂出相關規定與正確的資訊傳遞、取得的權力或相當的授權制度才是正確的防範方法。

第三節 研究目的

日常生活中我們常常會收到許多郵件包含了惡意連結、病毒等等，通常稍微

具有資訊素養的使用者並不會去開啟或者點選,但若信件內容有提供對使用者有利益的獎項則多少稍微有人會去點選、開啟。在本研究中是對某大學資管系大學部二、三、四年級為實驗對象,針對這些學生來寄出郵件,並且利用社交工程的方式技巧性的取得這些具有資訊素養的大學部學生的個人資料,接著在幾周內利用信件內容提醒學生們個人資料的保護與詐騙行為的防範,並在同時再利用社交工程方式再一次取得學生的基本資料。

而本研究主要研究目的如下:

1. 以實際寄出電子郵件方式來查看具有資訊素養的學生是否容易洩漏個人資料。
2. 在電子郵件中加入警告標語與提醒避免個人資料的內容是否能有效避免社交工程的攻擊。
3. 觀察具有資訊素養的學生是否當年級越高越能夠避免受交工程的攻擊與危害。
4. 當具有資訊素養的學生在有了第一次受騙上當經驗後是否還會在上當並提供個人資料。

第二章 文獻探討

第一節 社交工程

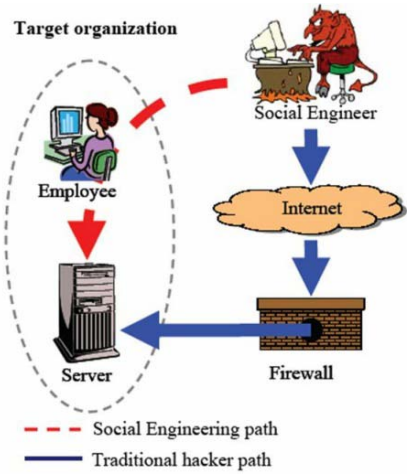
本節將探討社交工程之定義,社交工程指的是利用人類心理上的弱點、網路或電話中的溝通與交談、電子郵件中的超連結或圖片等釣魚方式來讓們掉入駭客的陷阱,使駭客能夠取得其所需資料稱之。通常駭客總是利用許多不同的方法來獲得寶貴的資源,而這些資源的來源不外乎是企業、個人或是其他團體等等對駭客有用、有利的資訊資源;而駭客所使用的方法不外乎是利用高超的電腦軟硬體知識來入侵計算機系統、企業內外部網路等等,但近年來發現有些惡意攻擊者雖然在電腦軟硬體技術上沒有非常精進,但是卻利用人類心理層面上的弱點或者是騙取人們的信任進行欺騙來取得其所需資源,這些惡意攻擊者所用的方法我們稱之為社交工程。

一、 社交工程定義

社交工程(social engineering)顧名思義,即為利用眾人疏於防範的詭計讓人們掉入陷阱,而此陷阱主要以交談、欺騙與假冒等等不當方式來取得大眾與企業的資料與機密。

通常社交工程主要是來利用操控人類的心理的一種犯罪行為,使受害的一方提供資料與機密檔案。而社交工程技巧通常是指用已蒐集資訊或電腦系統存取權限的詭計。常見的社交工程技巧都是以電話與網際網路為犯罪的主要途徑,包含了電話偽裝特定人員、垃圾郵件、電子郵件欺騙受害者、將電子郵件中的檔案植

入惡意程式、即時通訊的交談與詐騙等等的網路釣魚方式。因此社交工程的攻擊方式不是利用複雜、精進的電腦軟硬體技術，而是利用某些方式騙取人類的信任或是利用人類心理層面上如規避上司處罰的弱點來進行欺騙並獲取資訊。而企業對於一般的駭客卻是花費許多成本在軟硬體的保護上，卻忘了警惕、教育員工們如何防範社交工程的行為。因此社交工程是利用企業網路中最脆弱的一個環節，也就是使用者端的員工方面來下手，而不是直接攻擊企業網路或電腦硬體系統。下圖說明了駭客攻擊企業的兩種方式：



圖一：駭客攻擊的兩種方式(Hermansson, 2005)

二、 社交工程攻擊途徑

社交工程的攻擊手段不外乎是透過語音交談方式欺騙對方或者是電子郵件等方式來散布惡意軟體，因此社交工程攻擊途徑大致上可分為兩大類：1. 以硬體科技為基礎的詐騙、2. 以人類心理弱點為主的詐騙手段[3]。而社交工程攻擊者通常會將惡意軟體會隱藏在電子郵件內，這些惡意軟體不外乎是電腦病毒、蠕蟲、特洛伊木馬等等[8]，而這些惡意軟體通常隱藏在電子郵件內的超連結、圖片、影片、或者是附加文件內的文件之中。在 2007 年一月，曾經有個叫做"Storm worm"的蠕蟲病毒隱藏在全球許多的電子郵件之中，對重大的使用者造成相當程度的危害[2]。因此我們在開啟郵件裡面所包含的連結或者是媒體檔案時必須經過深思熟慮再行下載、開啟之動作。

另外在一項研究中發現，惡意軟體通常主要都是透過電子郵件來當作傳遞的途徑來達到社交工程攻擊的手段，也可以說社交工程攻擊的手段通常是依靠惡意程式來達成的[7]。因為使用者時常會不經意的忽略或違反組織內的資訊安全政策而開啟有惡意軟體的電子郵件，因此電子郵件是社交工程攻擊者最主要的攻擊方式。[7]。而這些含有惡意軟體的電子郵件常常由像是銀行、政府機關、企業與學校等等我們所信任的場所所發送出，因此一般使用者見到是自己信任的來源或者是自己親朋好友所發出的電子郵件會毫不猶豫的點擊電子郵件內的多媒體、超連結、文件檔案等等，如此一來便落入了駭客所設置的社交工程的陷阱。社交工程的風險時常被企業、政府、組織所低估，因此也忽略了員工的培訓計劃

與安全組織內部資訊安全政策的制定[5]。

而一般的網站也是駭客利用社交工程攻擊使用者的一個途徑，通常駭客喜歡在安全性較為脆弱的網站上嵌入惡意程式碼，等到使用者點選網站內的連結後，將會不知不覺的啟動惡意程式碼或者下載惡意軟體至使用者電腦中。或者駭客可以自行建置一個網站，並且在網域名稱上註冊一個與常見網站很相似的網域名稱，例如駭客可以註冊一個網域名稱像是 www.yahco.com.tw 來欺騙使用者，讓使用者以為自己已經連結到雅虎奇摩的首頁，殊不知進入的這個網頁駭客所建立與雅虎奇摩非常相似的假網頁。

近年來，因為網路的普遍，使得社群網站與部落格等等蓬勃發展。因此在社交工程攻擊途徑上又多了一種方法。此種攻擊途徑是利用社交軟體來作為攻擊的媒介，因為社交軟體目前被許多人所使用，並且可以透過網路的外部性來傳遞，因此駭客可以利用當紅的社群網站內的應用程式來攻擊使用者、竊取駭客所需資訊。例如駭客可以撰寫一個簡單的應用程式放置於當紅的 facebook 上，而使用者只要開啟、使用此應用程式及會下載惡意軟體至其電腦中。另外攻擊者也可以透過情緒的操縱來進行社交工程的攻擊，而情緒的操作包括恐懼、好奇、興奮、人性的貪婪、為了規避懲罰與認知的差異等等心理因素來影響、操縱使用者的心理[6]。因為人們通常用自己的判斷來信任他人，並沒有經過特別的求證與證明，而在此資訊爆炸、網路普及的時代，若要求證並信任他人是隨著網路的擴張而變得更加複雜[4]。

第二節 資訊素養

在網路普及、資訊爆炸的知識經濟社會中，培養國人具備有一定資訊能力已經是現代化國家的一個重要目標、主題。目前我國教育環境中，資訊教育是一項非常重要的議題，只要是培養學生們能夠有擷取所需資訊、分析與應用資訊、創新創造與思考、解決問題、團體溝通合作的能力與終身學習的態度。資訊素養(information literacy)是近年來出現的一個新名詞，也是一種知識管理上的策略，其意義為一種「使人們能夠有效的尋找、選擇、使用與評估傳統紙本或者資訊資源的技巧」。並且有學者也說明了，資訊素養式確認資訊、檢所及巡或資訊、組織及整理資訊、使用及創造資訊、評估的能[1]。

第三章 研究方法

第一節 資料來源與研究樣本

本研究樣本來源是國立某科技大學資管系大二至大四在學學生，主要研究探討資管系學生們資訊素養的程度以及日常防範社交工程的行為、口號是否能有效阻絕社交工程的攻擊，使得有資訊素養的人們不至於受到詐騙者的社交工程行為而喪失個人資料與機密文件、檔案。

本研究資料來源是利用 python 撰寫一支程式，而此程式是可以利用偽裝的信箱來大量寄信給大學部的學生。第一次信件內容是請學生點擊電子郵件內的超連結並填寫研究問卷，並且在填寫問卷後可以參加抽獎，但要參加抽獎的學生則必須填寫個人資料，因此第一次信件主要是騙取學生們的個人資料為主，主要是查看有多少學生們會為了抽獎而填寫問卷並且填入個人資料。而第二次寄信誘騙約是三周後，信件內容依然是點擊電子郵件內的超連結並填寫研究問卷，但在信件內有提及近年來的詐騙行為、模式與社交工程的危害，最後再填寫完問卷依然可以參加抽獎活動，而相同的若要參加抽獎則必須填入個人資料。因此第二次寄信主要是觀察在信件內含有部分的警告內容與提醒是否能對社交工程攻擊行為的防範有明顯的效果讓學生們不至於上當與受騙。

第二節 研究方法與研究架構

本研究方法是利用單一母體比例假設檢定與兩母體分配比例差檢定。單一母體比例假設檢定主要是針對"若有第一次受騙的經驗為條件，第二次也很容易受騙上當"來作的檢定方法。而兩母體分配比例差是針對"信件內容的警告標語是否有用"與"年級越高資訊素養程度越高"來作的檢定的方法。

一、 警告標語的影響

通常社交工程皆是利用人性與心理上的弱點來騙取檔案與資料，時常讓人覺得防不勝防。因此常見的社交工程防範的方法不外乎在電子郵件內寫上警告社交工程的標語、不開啟不明電子郵件、不點選來路不明超連結、不提供個人資料機密資料與不下載違法軟體等方式。因此本文研究在電子郵件內加入了警告標語是否能夠降低社交工程攻擊成功的機率。因此我們發展出如下假說：

假說一：電子郵件內含有警告社交工程的標語能夠明顯的防範社交工程的攻擊。

二、 年級高低與資訊素養的影響

本研究的研究樣本是某國立科技大學資管系大二至大四學生為主。主要利用大量發信來觀察資管系大二至大四學生有多少人會受到社交工程攻擊而提供個人資料與機密。因此本文亦觀察資管系二年級、三年級與四年級是否會因為年級較高而有著較高的資訊素養，並且資訊素養較高的年級是否較不容易上社交工程的當。最後發展出如下假說：

假說二：年級越高，資訊素養越高，越不容易上社交工程的當。

三、 受騙經驗的影響

本研究主要實驗對象為大學部二年級(含)以上的學生，並且主要實驗次數為兩次，也就是說在一個月內寄了兩封必須填入個人資料的信件，第一封信件尚未提及詐騙與社交工程的危險；而第二封信的信件內容有提及詐騙與社交工程的危險，主要觀察學生們是否會上當並且填入個人資料。而本研究也觀察在第一次受

騙上當以後，就算有了第一次受騙上當的經驗，在第二次是否依然會為了得到抽獎獎品而填寫個人資料上了社交工程的當。因此發展出如下假說：

假說三：有了被社交工程詐騙的經驗者，往後就比較不容易受到社交工程行為的詐騙而上當。

第三節 研究假設

本研究包含三大項假說，主要目的包含觀察電子郵件內含有警告標語是否能夠有效防範社交工程的攻擊、是否隨著年級的遞增資訊素養也隨著增加，並且能夠有效避免社交工程的攻擊與有了被詐騙的經驗以後，是否依然還會掉入社交工程的陷阱中。本文發展的研究假設如下表：

表一：研究假設表

假設項目	假設內容
H_1：信件內警告標語對社交工程攻擊有顯著的防範作用。	在電子郵件傳遞時，於郵件內容中加入警告社交工程的行為與危險性，這些警告標語對社交工程攻擊有明顯的防範作用。
H_2：年級越高資訊素養越高，越不易受騙上當。	隨著年級的遞增，年級越高的同學越不容易受到社交工程此類手段詐騙其機密與個人資料。
H_3：若第一次被社交工程手法欺騙條件下，在第二次就算有警告的方式亦會上當。	由於人性貪婪，都會想要輕鬆獲得抽獎機會與獎品。因此就算曾經有過社交工程詐騙的經驗，再次上當的機會會大於分之五十。

第四章 資料分析

第一節 實驗敘述

本文實驗共分為兩次，第一次與第二次樣本大小皆為相同的 288 人。然而第一次受騙上當的人數有 99 人，第二次上當人數有 87 人；其中，第二次上當的 87 人之中有 55 人是在第一次也有上當受騙的，也就是說，有 55 位學生第一次與第二次皆上當並且提供個人資料。另外一年級第一次上當人數為 51 人，二年級第一次上當人數為 30 人，三年級第一次上當人數為 18 人；在第二次誘騙方面，第二次一年級上當人數為 34 人，二年級第二次上當人數為 26 人，三年級第二次上當人數為 27 人。整理後如下表：

表二：實驗結果統計表

	第一次上當	第一次未上當	第二次上當	第二次未上當	重複上當
一年級	P1a = 51	62	P2a = 34	79	25
二年級	P1b = 30	69	P2b = 26	73	18
三年級	P1c = 18	58	P2c = 27	49	12
總人數	288		288		55

第二節 資料分析

假說一：信件內警告標語對社交工程攻擊有明顯防範作用。

H_0：警告語在防範社交工程上無顯著性差異 $P_1 - P_2 \leq 0$

H_1：警告語在防範社交工程上有顯著性差異 $P_1 - P_2 > 0$

其中 P_1 表示三個年級第一次上當人數與總人數的比例；所以 P_1 為 $\frac{99}{288}$，P_2 表示三個年級第二次上當人數與總人數的比例，因此 P_2 為 $\frac{87}{288}$。

顯著水準 α 我們將之決定為 0.05，而統計方法是用兩母體分配比例差之假設檢定，因此是用 z 檢定來做為我們的檢定統計量。最後我們得出檢定統計量 Z_0 為 0.3018，可以明顯的知道 0.3018 不在拒絕域內，因此我們不拒絕 H_0，也就是說，我們認為警告語對防範社交工程沒有顯著性差異。

假說二 A：二年級學生資訊素養比起一年級學生較無顯著性差異。

H_0：二年級學生資訊素養比一年級學生還低 $(P_{1a} + P_{2a}) - (P_{1b} + P_{2b}) \leq 0$

H_1：二年級學生資訊素養比一年級學生還高 $(P_{1a} + P_{2a}) - (P_{1b} + P_{2b}) > 0$

P_{1a} 表示第一次一年級學生上當的人數比例，P_{2a} 表示第二次一年級學生上當的人數比例，P_{1b} 表示第一次二年級學生上當的人數比例，P_{2b} 表示第二次二年級學生上當的人數比例。

顯著水準 α 我們將之決定為 0.05，而統計方法是用兩母體分配比例差之假設檢定，因此是用 z 檢定來做為我們的檢定統計量。最後我們得出檢定統計量 Z_0 為 2.349，可以明顯的知道 2.349 是屬於拒絕域內，因此我們拒絕 H_0，也就是說，

我們認為二年級學生的資訊素養是比一年級學生來的高的。

假說二 B：三年級學生資訊素養比起二年級學生較無顯著性差異。

H_0：三年級學生資訊素養比二年級學生還低 $(P_{1b} + P_{2b}) - (P_{1c} + P_{2c}) \leq 0$

H_1：三年級學生資訊素養比二年級學生還高$(P_{1b} + P_{2b}) - (P1c + P_{2c}) > 0$

P_{1b}表示第一次二年級學生上當的人數比例，P_{2b}表示第二次二年級學生上當的人數比例，P_{1c}表示第一次三年級學生上當的人數比例，P_{2c}表示第二次三年級學生上當的人數比例。

顯著水準 α 我們將之決定為 0.05，而統計方法是用兩母體分配比例差之假設檢定，因此是用 z 檢定來做為我們的檢定統計量。最後我們得出檢定統計量 Z_0 為-0.265，可以明顯的知道-0.265 不屬於拒絕域內，因此我們不拒絕 H_0，也就是說，我們沒有顯著證據證明三年級學生的資訊素養是比二年級學生來的高的。

假說二 C：三年級學生資訊素養比起一年級學生較無顯著性差異。

H_0：三年級學生資訊素養比一年級學生還低 $(P_{1a} + P_{2a}) - (P_{1c} + P_{2c}) \leq 0$

H_1：三年級學生資訊素養比一年級學生還高 $(P_{1a} + P_{2a}) - (P_{1c} + P_{2c}) > 0$

P_{1a}表示第一次一年級學生上當的人數比例，P_{2a}表示第二次一年級學生上當的人數比例，P_{1c}表示第一次三年級學生上當的人數比例，P_{2c}表示第二次三年級學生上當的人數比例。

顯著水準 α 我們將之決定為 0.05，而統計方法是用兩母體分配比例差之假設檢定，因此是用 z 檢定來做為我們的檢定統計量。最後我們得出檢定統計量 Z_0 為 1.633，是不屬於拒絕域內，因此不拒絕 H_0，也可以說我們沒有顯著證據證明三年級學生的資訊素養是比一年級學生來的高。因為顯著水準我們將之設定為 0.05，最後檢定統計量 Z_0 為 1.633，與拒絕域 $Z \geq 1.645$ 差距不大，若我們將顯著水準設定為 0.1，則結果很明顯的是三年級學生的資訊素養會比一年級學生高。一般我們會將發生型一錯誤最大機率設定為 0.05 或 0.1，來控制型一錯誤發生的可能性；另外，我們也可以使用尼曼-皮爾森定理來找出給定 α 之下的最強檢定力。因此我們不能同時讓型一錯誤與型二錯誤一起下降，若想要較小的型一錯誤，則型二錯誤發生機率必會上升；反之亦然。

假說三：若第一次有被社交工程手法欺騙為條件，在第二次有警告的方式亦會上當。

H_0：有第一次上當經驗為條件，重複上當機率會低於 50% $(P_2 \mid P_{1a} + P_{1b} + P_{1c}) \leq 0.5$

H_a：有第一次上當經驗為條件，重複上當機率會高於 50% $(P_2 \mid P_{1a} + P_{1b} + P_{1c}) > 0.5$

P_2 表示第二次上當的機率，$P_{1a} + P_{1b} + P_{1c}$ 表示第一次三個年級的上當機率總合。

顯著水準 α 我們將之決定為 0.05，而統計方法是用單一母體比例之假設檢

定，因此是用 z 檢定來做為我們的檢定統計量。最後我們得出檢定統計量 Z_0 為 1.8847，是屬於拒絕域內，因此有顯著證據支持對立假設；也就是說就算有第一次受騙上當的經驗，第二次就算有警告標語會再受騙上當的機率也會大於 50%。

第五章 實驗結果、結論與建議

第一節 實驗結果

在第一次寄信引誘同學們上鉤時，並未在信件內提及警告內容，警告內容包含同學們社交工程與個人資料可能被竊取的風險。而第一次問卷問題設定為十題，獎項為學校內圖文部禮券五百元三張。第一次樣本總數共 288 人，上鉤人數一年級共 51 人、二年級共 30 人、三年級共 18 人，總上鉤人數為 99 人。

而在第二次寄信引誘同學們上鉤時，在信件內有提及社交工程與個人資料外洩的警告內容，第二次的總樣本人口數和第一次為共同的 288 人，問卷題目設定為 35 題、獎品內容為西堤與陶板屋餐券各一張(各價值五百元)，在回收問卷時發現一年級上鉤人數為 34 人、二年級上鉤人數為 26 人、三年級上鉤人數為 27 人。

經過兩次實驗後，交叉比對發現同時在第一次與第二次上鉤人數有 55 人，並且發現第一次上當人數與第二次僅僅相差 12 人，我們可以了解到在第一次沒有警告內容與第二次有警告內容的差別是不大的，因此雖然有警告內容，但第二次上鉤人數之中有 55 位同學在第一次有上鉤，因此可以發現只有第一次上當的人數有 44 人，只有第二次上當的人數是 33 人，也就是說警告內容對這重複上當兩次的這 55 位同學(上當的大部分同學)來說是可以被忽略的，因此在電子郵件方面的防護機制必須另外有更好的提醒方式或防範方法才能避免社交工程的攻擊。在實驗結果出來以後，另外有發現到年級越高，則上當人數越少，不管是第一次或者是第二次誘騙，上鉤人數三年級少於二年級，而二年級人數又少於一年級，但因為二年級與三年級學生參語的總人數較少，因此看出高科大資管系教育、教學多少讓學生有些資訊素養，但是只有顯著證據證明二年級學生資訊素養比一年級還高，沒有顯著證明三年級學生資訊素養比一年級學生高、亦沒有顯著證據證明三年級學生資訊素養比二年級學生還要高。

第二節 結論與建議

目前，也就是資訊安全非常重要的時代，不管是對企業、政府、個人、團體等等，資訊的安全都是必須達成的目標。因此在此時代，我們期望我們的資料、資訊與智慧財產能夠有所保障，並且不被不肖之人所竊取、利用。而目前雖然透過軟硬體的發展與測試行為使得電腦系統更為安全，但是駭客依舊能夠藉由簡單的社交工程行為來找出資訊安全的漏洞、竊取企業、政府等組織與個人的機密資料、資訊。在此時代，我們確定社交工程的惡意軟體是普遍且常見的，社交工程攻擊途徑通常不外乎是利用能夠通話的裝置或者將惡意軟體隱藏在電子郵件、網

站等等。我們需要了解到，社交工程攻擊的策略與途徑的改變可以說明社交工程攻擊的方法是會進化的，而且是愈來越複雜且精密，使得使用者更難防範、避免。而日常使用者也時常因為忽略了資料的安全性，並且駭客也利用大量垃圾郵件攻擊也是一種對使用者非常危險的組合，這樣的結合式攻擊方式使得日常使用者常常尚未查覺自己已經被被竊取機密資訊或者是個人資料，造成個人資料被利用、企業組織洩漏機密資訊。

在資訊時代的初期，通常駭客有非常專精的電腦技術來撰寫一些惡意軟體與程式，其目的就是用來攻擊與入侵使用者主機。而現今駭客不僅僅有專精的電腦技能來作為攻擊的用途，另外還可以透過人類心理層面的欲望、貪心、懦弱等等弱點與網路的普遍性、分享性來對使用者發動社交工程攻擊以竊取駭客所需資料與資訊。

然而在此方面的防範方式非常是有限的，，這些防範的方法也就只有局限於避免惡意軟體與網路釣魚的攻擊方式，卻較不能有效的避免社交工程的攻擊行為。

因為網路攻擊日新月異，因此目前資訊安全的政策已經不能完全地保護公司、組織的資產，因此在現今常見的社交工程的環境中，由於社交工程的攻擊行為與攻擊方式可以是隨著環境變化而複雜的，因此組織不僅僅要加強資訊安全的軟硬體設備，另外組織中人們必須隨時保持警惕與發展更新的資訊安全管理政策才能夠有效的防範社交工程的攻擊。所以在組織內必須時常倡導安全意識、制定組織內資料索取的權限、提升組織內的資訊素養、發展員工教育訓練與發展新的資訊安全政策。

所以我們可以了解到，組織雖然不能完全的避免社交功的攻擊，但是能夠透過倡導安全意識、制定組織內資料索取的權限、提升組織內的資訊素養、發展員工教育訓練與發展新的資訊安全政策來減低社交工程攻擊的成功率，而未來我們的挑戰就是尋找出能夠完全的避免社交工程攻擊的方法，並且減少社會上社交工程攻擊的犯罪行為。

最後本文作者建議在電子郵件的社交工程方面因為警告標語看似較為無法防範，因此在收到電子郵件時應該保持檢查寄件者的真偽、確認信件內容真實度、不隨便開啟電子郵件內的連結與附件等等習慣，並且加強危機意識與提高警覺性。若收到自認為可疑的郵件也可以採取許多保護措施，例如在非必要閱讀之郵件可直接刪除、開啟郵件內連結先確認網址與網域名稱、不隨意填入個人資料與機密資料、不要下載附件檔案為不知名的副檔名等措施。因此主要防範策略如下：

1. 組織、企業、政府開始執行對員工們的資訊安全培訓。
2. 驗證可疑的身份、郵件、電話是否是駭客的攻擊行為。
3. 安裝與維護防火牆、電子郵件過濾器、防毒軟體與反間諜軟體。
4. 明確的檢查網站與網址是否合法。
5. 不在社交網站、電子郵件與即時通訊軟體上傳輸機密資訊。

6. 不向任何人提供有關組織的資訊與組織內資訊安全架構。
7. 盡可能避免公開有關組織人事架構、組織結構圖。
8. 不允許員工在組織內硬體設備下載任何軟體。

第六章 參考文獻

1. 張臺隆 (2004)，中部地區國民小學校長資訊素養與實施資訊科技融入教學情形之研究，碩士論文，台中師範學院國民教育研究所。
2. Kanich C, Kreibich C, Levchenko K, et al. (2008), “Proceedings of the 15th ACM Conference on Computer and Communications Security. ”
3. Lena Laribee (2006), “Development of methodical social engineering taxonomy project,” Naval postgraduate school, Master's Thesis.
4. Luhmann, N. (1994), “Risk: A Sociological and Theory”
5. McDermott, J. (2006). “Social engineering - The Weakest Link in Information Security”
6. Raman K (2008), “Ask and you will receive,” McAfee Security Journal Fall, pp.9-12.
7. Sherly Abraham, InduShobha Chengalur-Smith (2010), “An overview of social engineering malware: Trends, tactics, and implications,” Technology in Society No. 32, pp.183-196.
8. Siponen M, Oinas-Kukkonen H. (2007), “A review of information security issues and respective research Contributions,” Database for Advances in Information Systems, No 38, pp.60-81.

Can warning signs and the level of information literacy within emails effectively resist the social engineering of the attacks?

Nien Ching Hsuan[1] and Ching-Wen Chen[2]
Department of Information Management, National Kaohsiung First Technology University of Science and Technology
u9924820@nkfust.edu.tw

Abstract

In the age of information explosion, information security has been an issue everyone concerns with. In general, organizations will develop anti-attack software for their users to defend hostile attacks by unknown hackers. However, hackers are not only capable in coding techniques for software development, but also have social skills such as oral communication, lure, counterfeit identity, greed, punishment avoidance and another psychological weakness to defraud or to phish users' personal information or other confidential information. This study focus on one of social engineering termed phishing, in which emails or websites are used to defraud people for confidential information, using a well-planned experiment.

In this study, an e-mail with social engineering warning signs is created and distributed unexpectedly to students, who are information majors and supposed to be capable in dealing with the issue of information security, to see whether they would be defrauded of their personal information. After these emails being distributed to target experimenters (students), we have found the followings:

1. An email with warning signs does not significantly prevent social engineering attack to target experimenters who are information majors.
2. It is believed that senior experimenters (junior and senior students) should have more information literacy than junior experimenters (freshmen and sophomore) do. However, it is not the case. In this experiment, senior experimenters didn't effectively identify social engineering attacks. Thus, they were still defrauded of their personal information.
3. The experimenters, who have been defrauded by social engineering before, would have more than fifty percent chances to be defrauded again by same social engineering attacks.

In the end, how to avoid and prevent social engineering attacks in emails has been explored and analyzed. Alternatives of avoiding being attacks by social engineering are also suggested.

Keywords: Social engineering, Phishing, Information literacy