資訊安全與社交工程教育訓練

圖書資訊館，網路通訊組
劉則明

Outline

- 教育部 - 惡意郵件開啟分年目標
- 100 年度演練時程及方式
- Question
- 資訊安全概念
- 駭客攻擊手法
- 社交工程的定義
- 社交工程造成極大威脅的原因
- 社交工程案例
- 常見的社交攻擊手法與目標
- 社交工程攻擊的流程
- 社交工程的可疑徵兆
- 防範社交工程攻擊的方法

教育部 - 惡意郵件開啟分年目標

等級	適用單位	99 年度目標	100 年度目標
A 級	教育部、 台大醫院、 成大醫院	開啟率 <10% 點閱率 < 6%	開啟率 <10% 點閱率 < 6%
B 級	大學、 區域網路中心、 縣 (市) 教育網路中心	開啟率 <10% 點閱率 < 6%	開啟率 <10% 點閱率 < 6%

100 年度演練時程及方式

	演練時程	演練方式	備考
國家資通安全會報演練	1~12 月不定期演練	寄發電子郵件	
學術機構分組【教育部】演練	第 1 次演練 :5 月 第 2 次演練 :9 月	寄發電子郵件	

Question 1

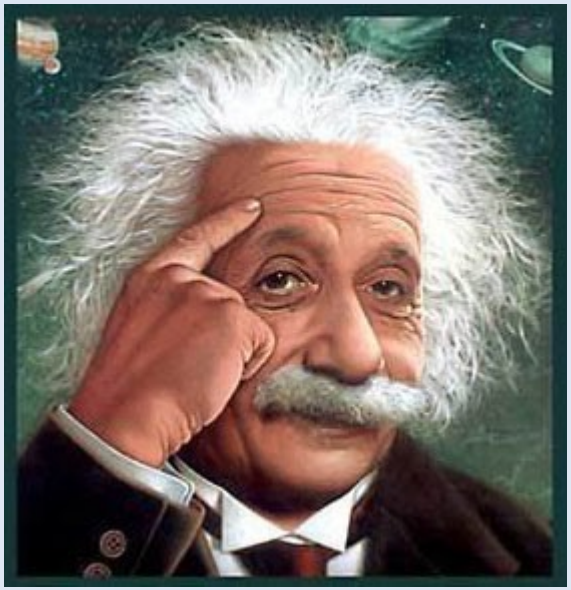
Scenario：
有一家公司引進了目前最好的安全技術，員工們也都訓練有素，下班前會把所有的公司機密都鎖起來，並請來保全業界最好的保全公司來保護這些機密。還遵從了專家所提出的安全建議，也安裝了各種受推薦的安全產品。

Question：
這家公司的安全是否真的無虞了呢？哪裡有可能會出現安全性問題？

Answer

安全還是堪虞

輕忽大意的員工



- 只有兩件事是永恆的，一是宇宙，一是人類的愚蠢，而我對前者不敢確定。 - Albert Einstein

Question 2

- 我不是資訊人員，所以資訊安全與我無關。
- 我不是系統管理人員，所以駭客不會找上我。
- 我所使用的軟體都是正版的而且有安裝防毒軟體，所以我的系統是安全無虞的。
- 為了不會忘記密碼，登入系統的密碼我一律使用我的身份證號碼作為密碼。
- 我管理多個帳號密碼，為了管理方便所以我把帳號和密碼設定成一樣。
- 我在單位裡的級職是最低的，所以不會成為攻擊目標。
- 對於主管於電話中或 E-mail 裡要求我提供系統的登入帳號及密碼，我會不加思索的提供給他。

資訊安全概念

- 沒有任何一套產品或系統可提供 100% 的安全防護。
- 資訊安全的管理是建立在風險管理的基礎上。
- 任何系統最薄弱的一環是人，安全警覺訓練是投資報酬率最高的安全對策。
- 資訊安全、人人有責。

駭客攻擊手法

- 收集基本資料
- 尋找可能利用的弱點並測試所發現的弱點是否可供利用
- 滲透
- 逐漸擴大入侵後的權限
- 進行入侵的目的
- 擴大入侵後的成果
- 清除入侵證據

※ 其中以社交工程手法最容易進行資料的蒐集、弱點的測試及滲透的進行

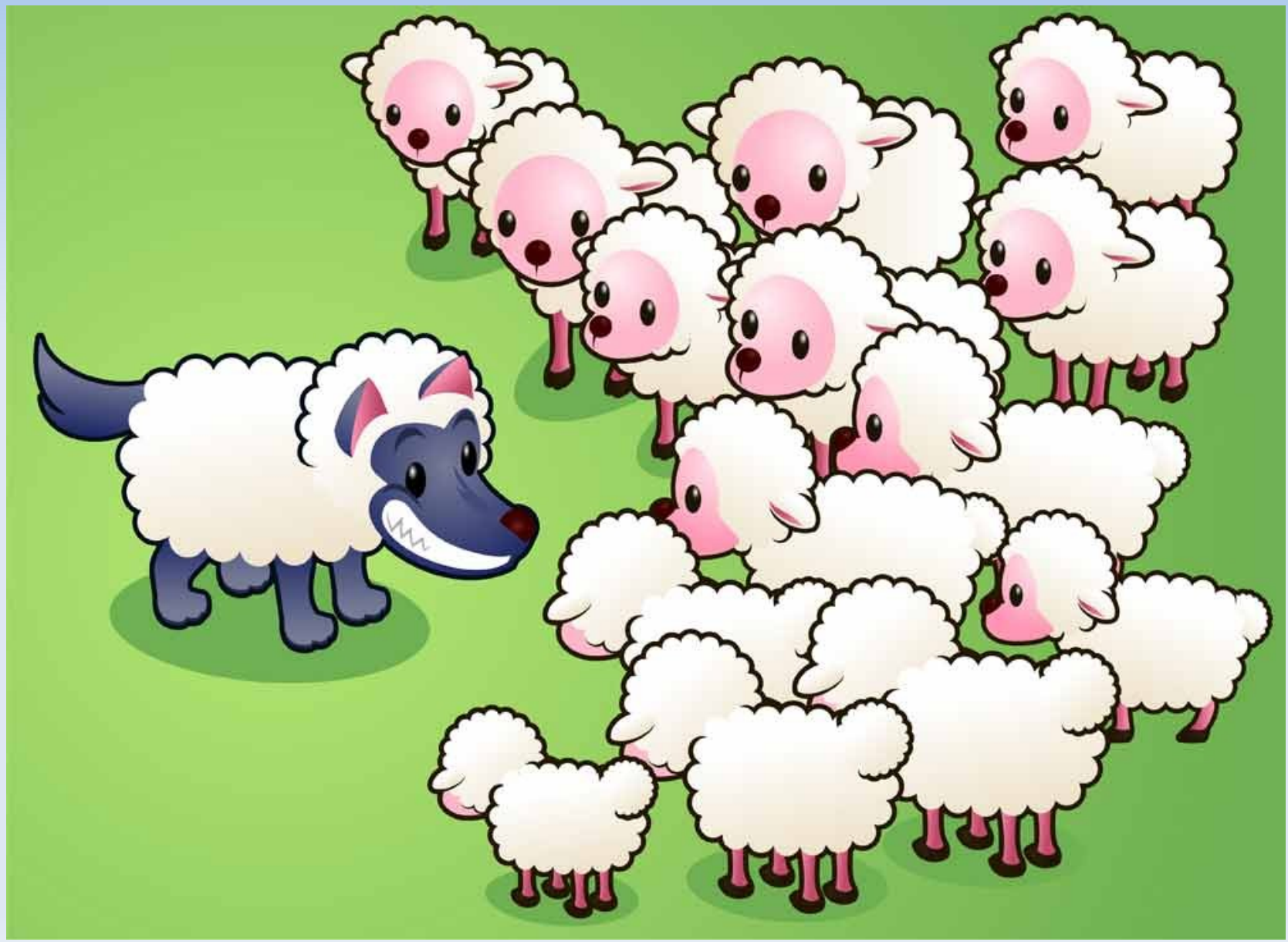
社交工程的故事

- 格林童話 - 大野狼與七隻小羊

大野狼與七隻小羊

- 大野狼先取得攻擊目標的背景資訊：
  - 羊媽媽留下七隻小羊在家裡單獨外出去找吃的東西
- 大野狼利用社交工程依序取得羊媽媽的特徵：
  - 聲音輕柔
  - 白色的腳
  - 沒有指甲
- 大野狼依據取得到的資訊，改變聲音、把腳染白及修剪指甲，於是突破小羊們的防備，讓小羊自動把門打開

接下來的後果 .....



社交工程的定義

- 網路世界的數位安全 (Secrets & Lies: Digital Security in a Networked World) 的作者 Bruce Schneier 曾提到所謂社交工程，全都是由人性方面，也就是利用所謂的”信任”來進行。
- 欺騙的藝術 (The Art of Deception) 的作者（ Kevin Mitnick ），更進一步的解釋到人類的天性就是很希望能幫助別人，因此也相當容易被欺騙。

社交工程的定義

- 以影響力或說服力來欺騙他人以獲得有用的資訊。
- 利用人性弱點或利用人際之信任關係來進行詐騙，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。
- 以人為本、騙術為主
- 技術門檻低
- 利用人的貪念、好奇心及缺乏警覺性

社交工程造成極大威脅的原因

- 不需要具備頂尖的電腦專業技術，只要員工對於防範詐騙沒有足夠的認知，就可以輕易地避過了企業的軟硬體安全防護，而騙取到各項帳號密碼、個人資料、財務資料或公司重要資料等資訊，對企業所造成的損害與威脅，完全不下於網路上的各種駭客攻擊。
- 社交工程利用人性容易相信而上當的弱點，避開了不容易破解的網路防火牆，只應用了簡單的溝通和欺騙技巧，便突破了企業的安全防護，而所花費的成本可能只有一、兩通電話的費用。

社交工程的幽默案例

加州理工學院 (CalTech) 有一尊 130 年歷史的加農砲

社交工程的幽默案例 count.

美國麻省理工學院 (MIT) 的惡作劇學生把加州理工學院 (CalTech) 的加農砲偷到了 MIT，把它放在 MIT 的 Green Building 前，並將砲口朝向 CalTech 所在的 Pasadena。

社交工程的幽默案例 count.

同時在砲管上套了一個大尺寸的 MIT 金戒指。

社交工程的幽默案例 count.

這個偷竊行動等於橫跨了美國西岸到東岸。

社交工程的幽默案例 count.

在這尊砲旁邊豎立的一塊銘碑上，除了說明了這尊砲的”前一個擁有者”是 CalTech 外，也說明了這整個行動的進行方式。

常見的社交攻擊手法與目標

- 常見的詐騙與攻擊手法：
  - 假冒為同事或新進員工
  - 假冒廠商、客戶或政府單位
  - 假冒具有權威的人
  - 假冒系統廠商，表示欲提供系統修補程式或更新程式
  - 假冒好心人士，告訴對方如果電腦發生問題可以找他，然後製造問題，讓受害人打電話來求援...等。
- 社交工程攻擊常鎖定的目標：
  - 基層庶務人員
  - 新進員工

社交工程攻擊的流程

- 取得一個攻擊目標的背景資訊
- 與受害人建立信任
- 待建立信任後向受害人要求資訊
- 再利用這些資訊向其他或更高層人員欺騙

不斷重覆以上步驟，以達成最後目標。

Case Study

Scenario：

- 假設你接到一通電話，自稱是本校的主管，但是你從未聽過他的聲音。對方表示他正在前往教育部開會的途中。打電話的人說了個悲慘故事：他要帶去開會的筆記型電腦被偷了，而登入各個系統的帳號密碼都在那部筆記型電腦中，而他又要登入到系統中去查詢一些重要的資料。

Question：

- 假如你是那位接電話的人，你會不會如他所願，告訴他想要知道的資訊告訴他？

社交工程的可疑徵兆

- 對方強調是緊急事件
- 提出不尋常的請求
- 威脅對方如果不照辦會有嚴重的後果
- 拒絕告知回電號碼 …. 等

遇有上述情形時應提高警覺心。

防範社交工程攻擊的方法

1. 教育與訓練。
   - 教育組織內的員工，認識社交工程有哪些常見的可疑徵兆。
   - 教育組織內的員工了解並遵守學校安全政策與程序。
   - 實際模擬演練與測試。

防範社交工程攻擊的方法

2. 密碼政策。
   - 週期性的更換密碼。
   - 避免使用容易猜到的密碼。
   - 不要將密碼保存於紙張上或電腦中。
   - 禁止將個人密碼告訴他人。

防範社交工程攻擊的方法

3. 完整運作指引。
   - 確認身分（員工編號，姓名 ... ）。
   - 確認在職狀況（是否仍在職，單位部門，職稱...）。
   - 確認對方有取得資訊的需求及權限。
4. 實體的安全政策。
   - 進入具有資訊安全顧慮的空間，是否具有實體的管控。例如：進入機房是否需要刷卡，只有指定的人員進入機房可以開啟門禁。

防範社交工程攻擊的方法

5. 資訊的分類 。 將文件等級區分為:
   - 極機密
   - 特權使用
   - 內部使用
   - 公共使用 .... 等。
6. 適當的事件反應
   - 如遇到疑似攻擊事件時應向有關單位通報。

防範社交工程攻擊的方法

7. 政策檢查表。
   - 帳號的設定。
   - 密碼改變的政策。
   - 存取權限。
   - 紙張文件。
   - 實體存取限制。

網路社交工程的攻擊方法

- 電子郵件隱藏電腦病毒
  - 駭客利用社交工程的概念，將病毒、蠕蟲與惡意程式等隱藏在電子郵件中，這些看似朋友所寄來的郵件，卻是應用社交工程的電子郵件陷阱。
- 網路釣魚
  - 有一種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。

網路社交工程的攻擊方法 count.

- 圖片中的惡意程式
  - 明星或色情圖片也是許多惡意程式慣用的社交工程技巧之一，這些都是利用使用者的好奇心來散佈惡意程式。
- 偽裝修補程式
  - 一般使用者不會覺得這是來路不明的程式，卻沒有防範社交工程也會利用這個漏洞，而將惡意程式隱藏其中。使用者若安裝了這個檔案，不但不會修補作業系統的任何漏洞，還可能被安裝了遠端竊取資料的木馬程式。

網路社交工程的攻擊方法 count.

- 即時通訊軟體
  - 駭客利用盜取的即時通訊帳號將訊息、病毒、蠕蟲與惡意程式等傳送給帳號裡的好友，這些看似好友傳送過來的檔案，卻是應用社交工程的陷阱，例如 MSN 病毒、 MyCard 點數詐騙。