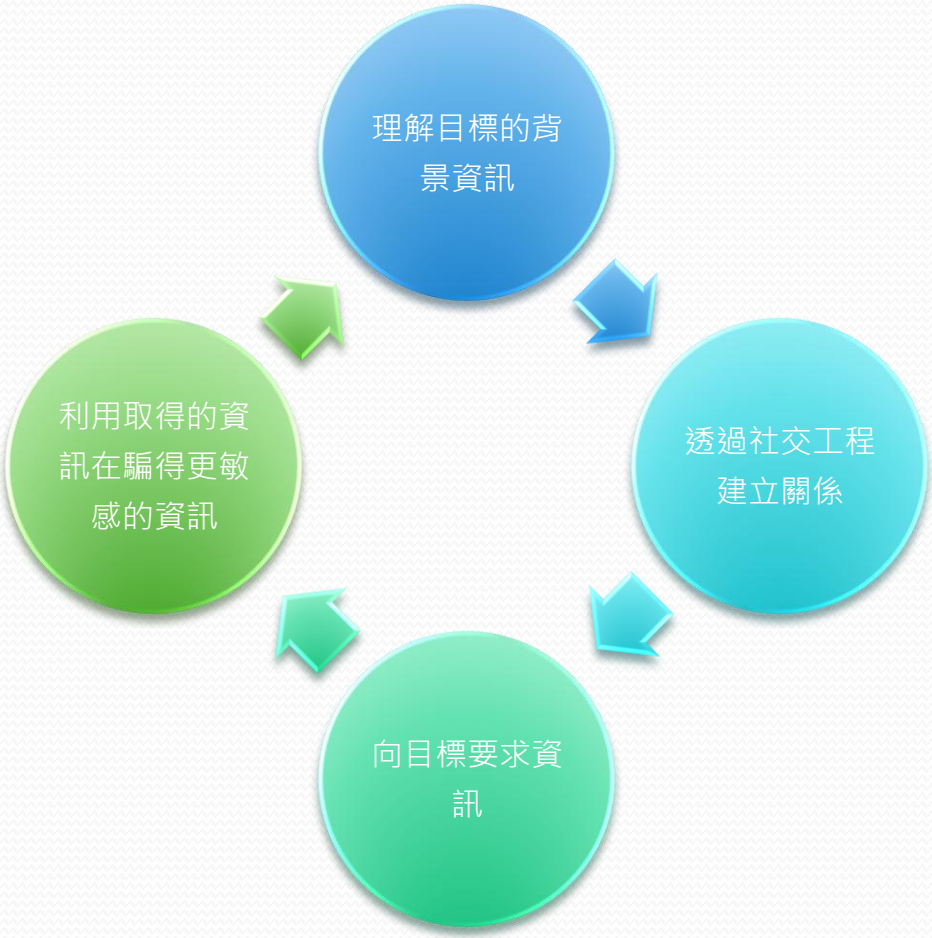
社交工程的危害與防治方式

陳永芳

什麼是社交工程?

- 社交工程，英文為Social Engineering，在資訊安全管理中，指利用人性弱點、人際交往上的漏洞?非法獲取資料的行為，這是近年來造成企業或個人極大威脅和損失的駭客攻擊手法。

社交工程攻擊步驟

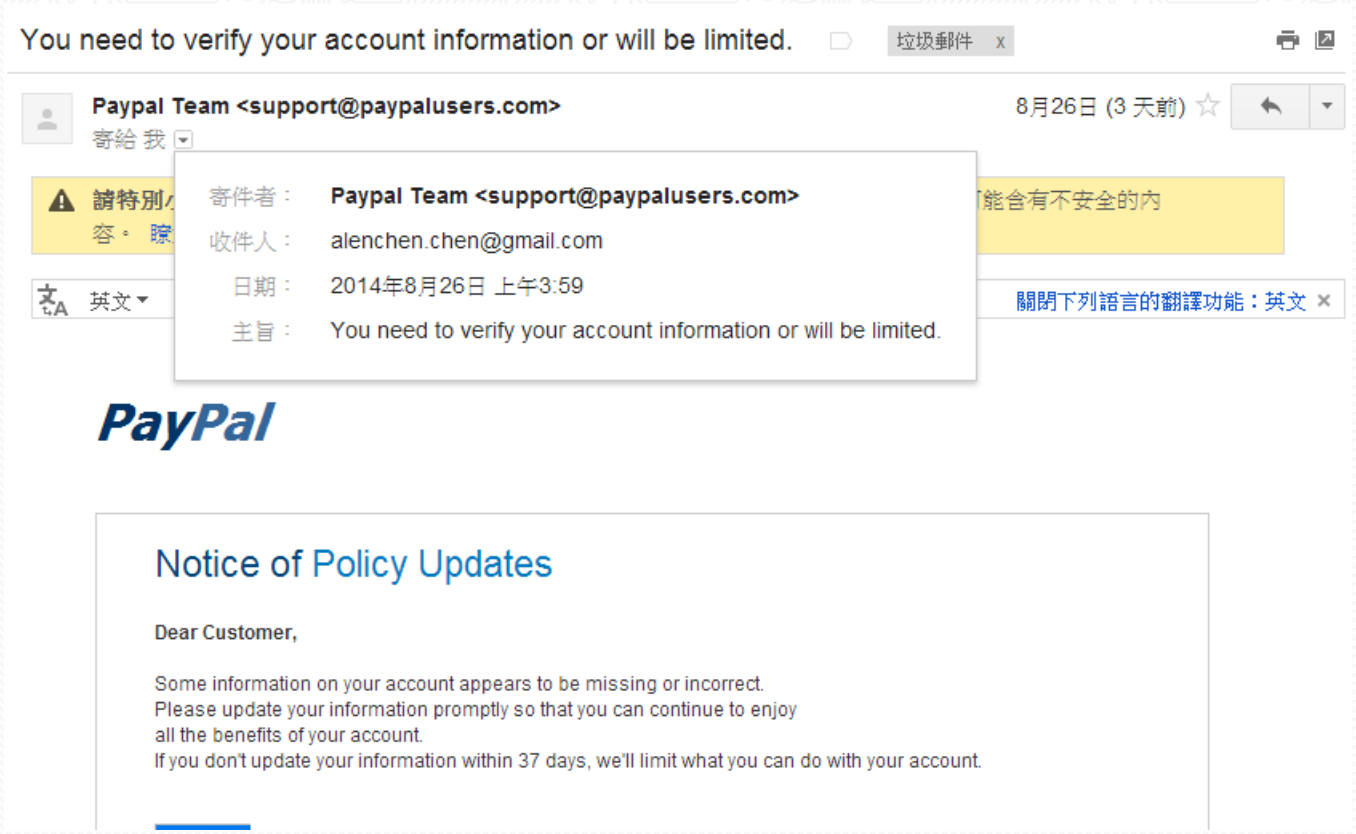


社交工程利用的元素

- 友誼：
  - 利用在朋友之間的彼此的交情關係。
- 電子郵件：
  - 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，
- 廢棄物：
  - 經由搜尋廢棄物搜尋可能有用的資訊。
- 窺視：
  - 未上鎖的文件櫃及未收好的文件
  - 未鎖定的電腦螢幕
- 信任：
  - 透過交談與受害人建立信任，然後向受害人要求資訊 。
- 時間：
  - 攻擊者的重要元素。

近年常見的社交工程攻擊型態

這封信...哪裡怪怪的?


You need to verify your account information or will be limited.
垃圾郵件 x
Paypal Team <support@paypalusers.com>
寄給 我
8月26日 (3 天前)
寄件者： Paypal Team <support@paypalusers.com>
收件人： alenchen.chen@gmail.com
日期： 2014年8月26日 上午3:59
主旨： You need to verify your account information or will be limited.
英文
關閉下列語言的翻譯功能：英文
PayPal
Notice of Policy Updates
Dear Customer,
Some information on your account appears to be missing or incorrect.
Please update your information promptly so that you can continue to enjoy
all the benefits of your account.
If you don't update your information within 37 days, we'll limit what you can do with your account.

網路釣魚-1

- 利用email來欺騙
  - eBay、Paypal、 以及Citibank是三個最常被利用的目標。
  - 使用者收到一封標題是Paypal帳戶資訊更新的郵件，其信件內容裡有提供一個仿冒Paypal網頁的連結並要求使用者由此連結登入Paypal網頁去輸入帳號及密碼來更新使用者資訊，這個仿冒網頁便會記錄使用者帳號密碼，接著再 將網頁導向真實的Paypal網頁，令使用者在不知不覺中就被盜取了密碼。

網路釣魚-2

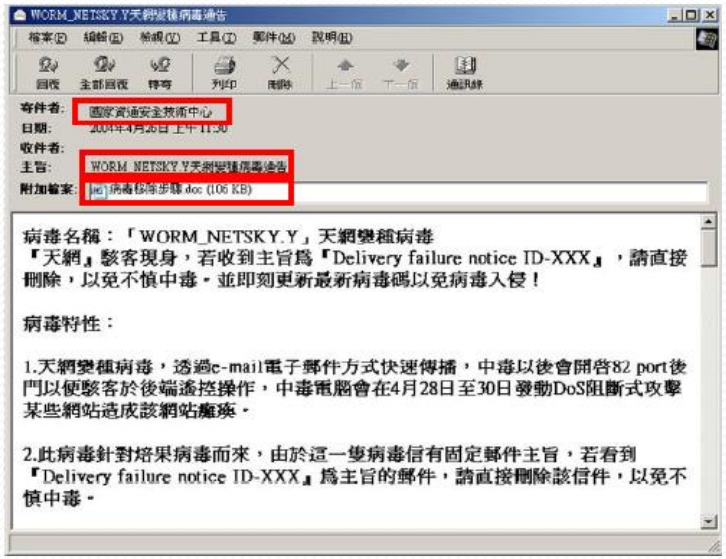
- 電子郵件隱藏電腦病毒
  - 駭客利用社交工程的概念，將病毒、蠕蟲與惡意程式等隱藏在電子郵件中，這些看似朋友所寄來的郵件，卻是應用社交工程的電子郵件陷阱
  - 例如過去造成重大損害的I LOVE YOU蠕蟲，就是一種利用社交工程散播的電腦病毒。

網路釣魚-3

- 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

網路釣魚-4

- 偽裝修補程式
  - 另一種社交工程的欺騙手法，就是偽裝成軟體修補更新程式，因為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。



網路釣魚-5

- 吸引您加入會員可以免費...
  - 影音下載、抽獎、特惠價...

因為多數人習慣用一組「相同的密碼」來為各個不同網站設定密碼

網路釣魚(Phishing) 案例

- 網路釣魚最常運用的管道有三，包括「電子郵件」、「假網頁」與「即時通訊軟體」等
- 黃姓男子盜用中國信託之網頁並建立註冊網站網址www.china-trust.com.tw民眾誤信登錄帳號密碼，向使用者要求一些之前就已提供給銀行做為身份認證用的資料，讓使用者填寫個人機密資料，像是銀行帳號、身份證字號、出生年月日或帳戶密碼等。
- 駭客取得這些機密資料後，就可進行後續的轉帳或其他惡意行為，造成使用者莫大的損失黃嫌利用帳戶轉帳盜取存款

網路釣魚(Phishing) 案例

- 台灣最多人使用的Yahoo!奇摩拍賣網站，也出現了盜取帳號密碼專用的「釣魚網站」，網站做得幾可亂真，網路使用者一不小心沒注意看的話，很可能Yahoo!帳號、密碼就被騙走了。
- 這個詐騙網站做得還真像，不但網頁、活動、廣告BANNER都有模有樣的，而且連網站網址都只差「.」跟「-」的分別，要是平時只顧著看特價商品，沒注意到網址不太一樣，一個不小心帳號密碼就被偷走了！
- 網址參考：
  - http://tw.bid.yahoo.com/
  - http://tw.bids-yahoo.com/

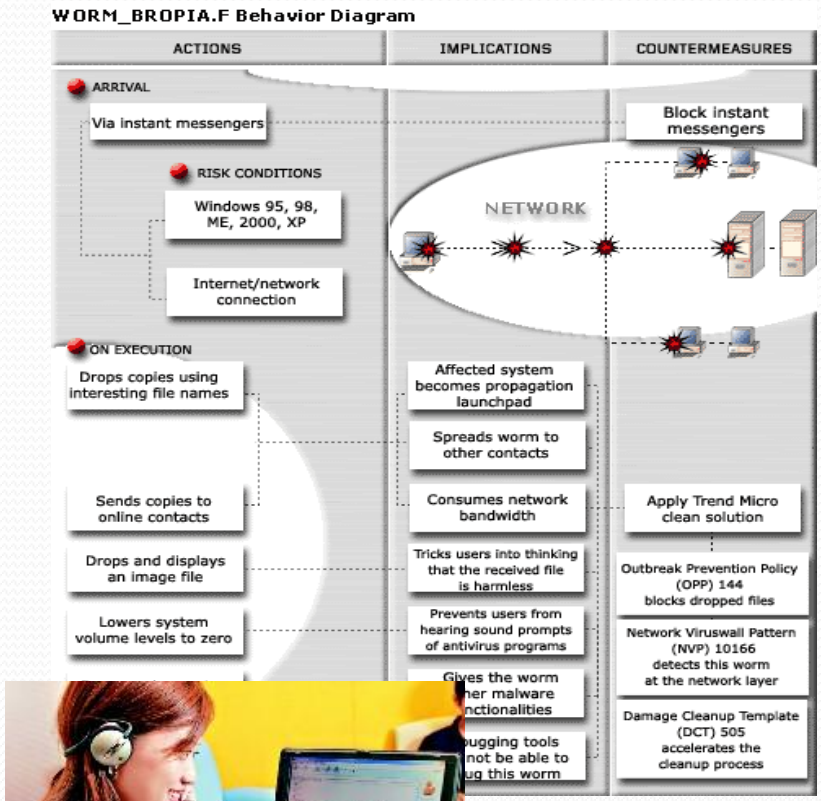
「釣魚網站」+「關鍵字廣告」手法

USB 社交工程法

- 遺失風險
  - USB 碟會有遺失的風險，在容量越來越大的現在，每次遺失都可能會造成大量資料外洩；預防方法嘛... 除了儘量不要掉以外，大概就是用加密技術了吧？
- 借用風險
  - 利用 windows 預設會跑 autorun 的特性，在 USB 碟裡面設定一些 spyware 或是跑程式搜集你電腦裡面的資訊，甚至有人會把東西藏在 iPod 裡面，藉口要充電，實際上則是在搞些奇怪的勾當。
- 連「撿到」都可能有風險
  - 原理和上一招一樣，但是直接把 USB 碟丟在容易被人發現的角落。如果你在地上撿到 USB 碟，你會怎麼做？應該是假設這個是同事的、然後想說看看裡面有沒有什麼檔案可以幫你物歸原主的吧？恭喜，中獎 ！

即時通訊成為社交工程新途徑

- 近年來，社交工程傳播惡意程式的途徑擴大至各種即時通訊軟體。
- 2005年2月，一個使用MSN大量散播 的病毒造成嚴重災情，這個電腦病毒會利用MSN自動傳檔給MSN連絡人上的朋友，亞洲各國皆傳出災情，包括台灣的案例也有千起以上。
- LINE也...



社交工程攻擊有效防範方法

資安認知教育

- 重視員工教育訓練與平常的宣導

認識可疑徵兆

- 不應該輕信他人
- 應該保持小心求證的戒心

社交工程有效防範方法

遵守安全政策與程序

- 不開啟不明電子郵件
- 確認資訊要求者身分及確認是否經過授權

通報作業

- 遇到疑似攻擊應立即通報

個人防範方法

- 不隨意點擊電子郵件、通訊軟體、社群分享的超連結
- 個人密碼管理好
  - 高複雜
  - 多不同
  - 常更換

謝謝您的參與！

課後加映

密碼設定的重要性

新聞報導

好萊塢女星遭駭　裸照瘋傳

http://www.cdnews.com.tw　2014-09-01 14:02:50

沈子涵/整理

法新社洛杉磯31日報導，美國媒體報導，好萊塢一線女星珍妮佛勞倫斯（Jennifer　Lawrence）以及流行樂小天后蕾哈娜的裸照疑似遭到駭客竊取後外流，這些照片今天在社群媒體上瘋傳。

珍妮佛勞倫斯在推特的推文中說：「有人為了剝奪他人隱私而費盡苦心，這真是太怪了。」

新聞報導

Gmail傳500萬帳密外流　使用者不求人2招自保

正文　網友評論　友善列印

【超犯規】美顏、長腿、蜜桃奶...好妹，不推嗎？

ETtoday科技雲　讚 62,631　6.2萬　2　24　讚　分享　推薦

科技中心／綜合報導

繼Apple爆出icloud遭駭，造成百位名人裸照外流，現在又驚傳Google(谷歌)電子郵件Gmail高達500萬個帳戶密碼也被有意人士盜取，並在昨(10日)天被公布於俄羅斯網站上流傳，吸引各界高度注意。雖然Google強調公司絕對將用戶資料安全放在首位，但現在也出現用戶自救的方法。

▲傳出Gmail有高達500萬個帳密遭洩，大部分是英語、俄語、西班牙語系使用者。（圖／翻攝自網路）

這一切...都是...
因為密碼設定不良

不太優的密碼

- 單一種文字、或數字(複雜度太低)
  - 連續或相同的數字
  - 英文名字或單字
- 使用同一個密碼
- 容易忘記的密碼

問題是...

- 複雜的密碼容易忘
- 好記的密碼太好猜
- 每個不同容易混淆

解決方法

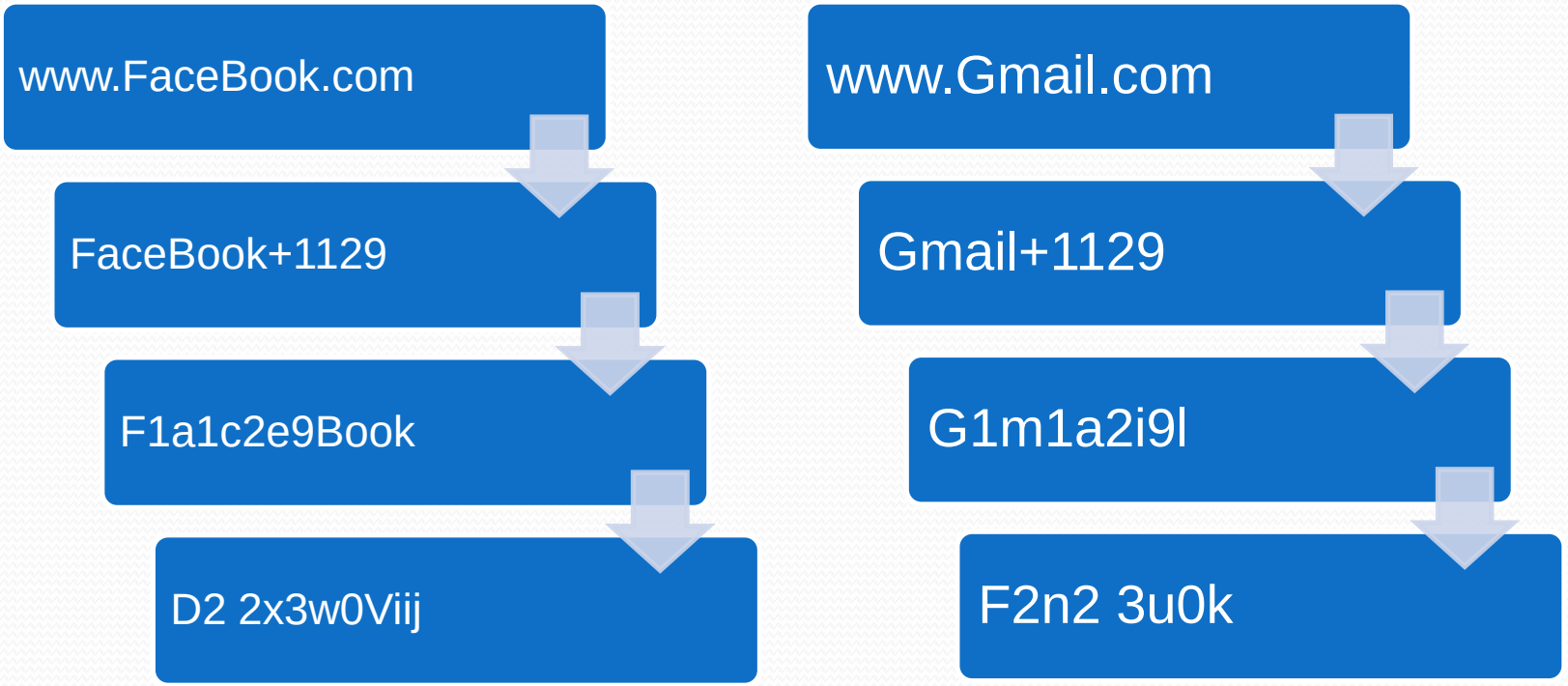
- 函數式密碼設定法
  - 一個固定的運算式
  - 依來源取得不同參數
  - 例如....

以提款卡密碼為例

- 密碼設：5234579

前7個數字依序加1、2、3、….7

網站密碼你可以...


www.FaceBook.com
FaceBook+1129
F1a1c2e9Book
D2 2x3w0Viij
www.Gmail.com
Gmail+1129
G1m1a2i9l
F2n2 3u0k

提醒您...

「一個固定的運算式」請自己想....別跟我的範例一樣....

P.S.以上範例不是本人密碼設定方式，如有雷同純屬巧合....