校園資安與社交工程剖析

麟瑞科技
區域銷售事業處 副處長

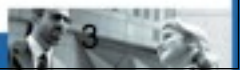
張晃崚 CCIE #13673, PMP

Agenda

- 社交工程分析
- 個資竊取技術
- 正確的防護觀念

社交工程的陷阱

- 一般大衆疏於防範的詭計
- 以影響力與說服力套取他人機密資訊
  - 交談
  - 欺騙
  - 恐嚇
- 詐騙集團



社交工程技巧

- 操控人類心理
- 利用階級、新聞、天災、八卦、金融稅務、謠言、購物等等方式
  - 歐巴馬放棄就職？
  - 麥可傑克森死亡內幕？
  - 求職回絕信

什麼是社交工程?

❖社交工程之典型範例

- 加州理工學院(CalTech) to 麻省理工學院(MIT)

開課囉！ ★寒假考前衝刺班★ 現正招生中！
天然靈芝禮盒 | 胡桃鉗DVD | 全國名師到你家

TTV》新聞》

網路劫標客 相仿帳號發信騙錢 數字1小寫L 肉眼難辨成漏洞

報導記者：郭于中 941206

網路拍賣詐騙手法又翻新，一位民眾在網路上向取名flora的賣家購買手機，沒想到，收到的得標信，卻是署名f一ora，由於一跟英文字母小寫的L，實在太過相近，被害人沒發現，就把錢給轉出去，對於類似的詐騙手法，連網路拍賣業者都說還沒聽說過。

網路上琳瑯滿目的拍賣

** 卡哇依教主 ** 楊丞琳

超離譜 網售東森購物 8千筆個資

黑者層出包 卡號全都露 每筆5毛 2009年06月11日蘋果日報

新聞快訊 列印 留言(0) 引用(0) 推薦(0) 點閱(28263)

1 / 1

東森購物客戶資料遭人公然上網販售，客戶的信用卡卡號、卡到期日、身分證字號等資料全曝光。

【郭睿誠、侯柏青／台中報導】八千筆東森購物台消費者個人資料在網路上「全都露」，有民眾周一在網路上宣稱「輸錢賣信用卡資料」，強調是「東森購物流出」，客戶姓名、信用卡號、身分證字號等一應俱全，一筆賣零點五元，還提供兩個檔案、多達八千筆免費資料供有意購買者參考。《蘋果》經抽樣訪問確認資料無誤，東森購物接獲《蘋果》查訪後表示已向警方報案；消基會則呼籲民眾慎選其他更安全的交易平台。

擁有三百多萬會員、全國最大購物頻道的東森購物網，近年來客戶資料外洩疑案頻傳。署名「阿哲」網友周一在二手市場網站貼文《輸錢賣信用卡資料》，強調「東森購物流出」，他另於免費網路空間中放置兩個檔案，讓有意購買者參考，強調：「今年五月前每天均有絕無欺騙，預購來信表示購買日期及筆數。」《蘋果》循網址，發現果然不需使用帳號、密碼，只要鍵入驗證碼並等候約四十五秒，即可順利下載兩個Excel檔案，檔案裡約有八千筆個人交易資料，日期為去年八月十二日及十一月七日，包括客戶姓名、商品名稱、定單金額、付款方式、配送地址及消費者行動電話、市內電話、信用卡卡號、發卡銀行、信用卡有效期限、生日、身分證字號等。

盜取網拍帳號密碼

網路購衣 女竟被騙1500萬

自由時報 更新日期：2010/05/03 04:11

〔記者邱俊福、謝武雄、李容萍／綜合報導〕桃園縣一名彭姓女子，在網路幫小朋友購買衣服，沒想到被詐騙集團盯上，透過連環詐騙手法，將她帳戶內的1500多萬元詐騙一空，被害人得知車手被捕，情緒激動的要對方「還我錢來！」

騙稱匯款分期錯誤

警方調查，38歲的彭姓女子，3月下旬在桃園家中透過網路購物，沒多久，彭女接到佯稱銀行行員的來電，聲稱帳戶的匯款設定成分期，必須將金額轉入指定帳戶才能夠解除，彭女誤信為真，從當天起到4月7日，陸續轉匯出32筆存款到不同的指定帳戶，金額從幾千元到近百萬元都有，另彭女還領出兩筆各500多萬元的現金，交付給歹徒。

社交工程攻擊方法

- 社交工程攻擊之定義
  - 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法
  - 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊
  - 透過電子郵件進行攻擊之常見手法
    - 假冒寄件者
    - 使用與業務相關或令人感興趣的郵件內容
    - 含有惡意程式的附件或連結
    - 利用應用程式之弱點(包括零時差攻擊)

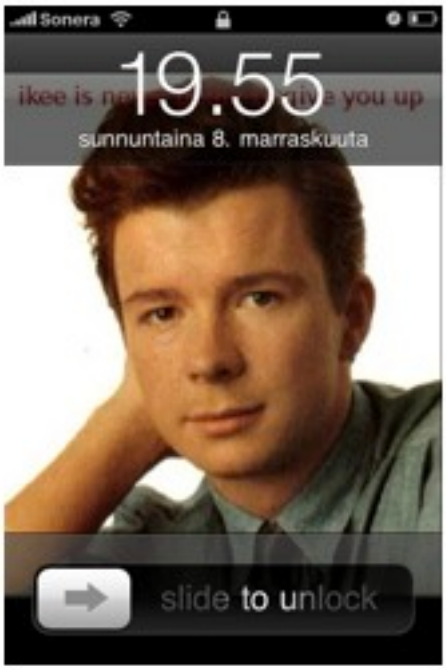
個資竊取方式

- 手機病毒
- 垃圾郵件
- Key Logger
- 網路釣魚
- HTML Injection
- Spyware
- Botnet
- Google hacking

日本 NTT DoCoMo iMode 手機案例

iMode使用者收到病毒寄發的惡作劇郵件，不知情而按下郵件裡面的超連結後，手機會自動撥號到110緊急報案電話

iPhone Virus



垃圾郵件

垃圾郵件不只有廣告

從 (from) RLC-T

主旨 (subject) [Spam] ringline.com.tw account notification

到 (to) RLC-T

回覆 · 轉寄 · 備存 · 刪除

1:47 PM

其他動作

垃圾郵件　非垃圾信

Dear Customer,

This e-mail was send by ringline.com.tw to notify you that we have temporarly prevented access to your account.

We have reasons to beleive that your account may have been accessed by someone else. Please run attached file and Follow instructions.

(C) ringline.com.tw

文字

setup.zip

八卦新聞主旨

收件者... centrell <centrell@cc.ncu.edu.tw>;

副本(C):

密件副本(B)...

主旨(J): 賈靜雯外遇真象

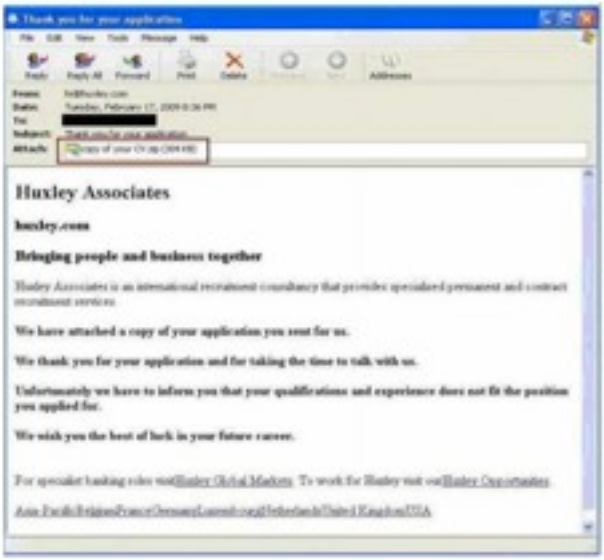
賈靜雯外遇真象

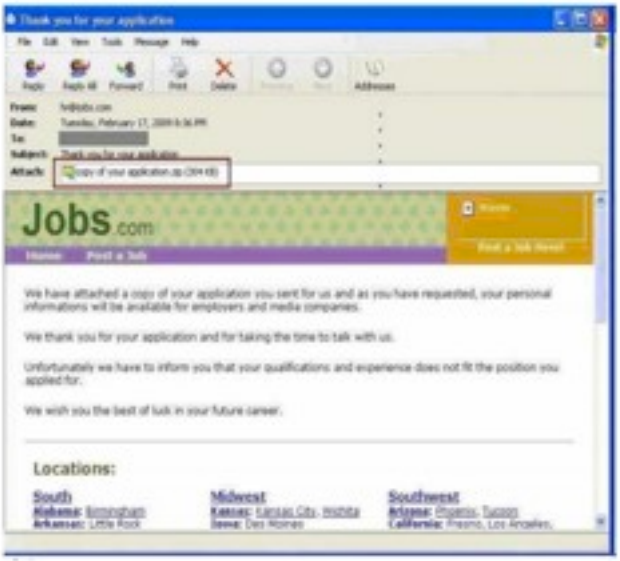
孫志浩舅舅劉正中爆賈靜雯3年前在南京拍戲時「發生不堪的事情」，曾與賈傳緋聞的黃磊昨以「見鬼了」形容自己無奈的心情。他說他與賈靜雯的緋聞純屬無稽之談，「我的為人大家也知道，怎會扯出這麼一筆爛帳。」

http://udn.com/NEWS/ENTERTAINMENT/ENT1/4837510.shtml

情色主旨(圖檔攻擊)

求職回絕信





假強風特報

小心！ 假強風特報 真電腦病毒

2009-03-18 | 中國時報 | 【李宗祐／台北報導】

「中央氣象局緊急通知—強風特報」？最近幾天如果接到上述主旨的電子郵件，最好直接刪除掉，千萬不要開啓，以免電腦病毒趁機入侵！氣象局昨日發布通訊安全緊急公告，呼籲民眾提防駭客假冒該局名義發送電子郵件，散播電腦病毒。

氣象局前天發現該局網站設置的民眾意見箱（webqry@cwb.gov.tw）發送出去的電子郵件中，有四、五十封電郵被莫名退回，信件主旨都是「中央氣象局緊急通知—強風特報」。追查發現，原寄信者的ＩＰ位址並非氣象局，且該局最近未傳送電子郵件給這些收件者，懷疑有駭客假冒該局名義發送電子郵件。

氣象局資訊中心爲追查冒名信件來源及駭客企圖，逐一打開被退回信件，赫然發現附件檔夾帶電腦病毒。

由於駭客冒用氣象局名義傳送電子郵件，並非針對該局電子報訂戶，而是發送垃圾郵件「散彈打鳥」，不知情民眾看到信件主旨及寄件者電子郵件帳號爲代表政府單位的「.gov」，多會不疑有它、打開信件。氣象局爲避免無辜民眾慘遭毒手，昨日發布資通安全緊急公告。

主動下載有毒附件

記者蘇湘雲／台北報導

調查顯示，有五成網友是主動下載有毒影音檔、開啓電子郵件，讓自己曝露於網路毒駭的問題中。（圖／Yahoo！提供）

總是抱怨網路毒駭事件層出不窮的使用者聽到以下消息，可能要先檢討自己爲何如此「手賤」囉！入口網站最新調查顯示，網路中毒原因的前三名分別爲「**下載有毒的音樂或影音檔案**」（**27.6%**）、「**帳號被盜**」（**26.7%**）及「**收到夾帶有毒檔案和連結的電子郵件**」（**24.2%**），除了帳號被盜，有五成以上的網友都是「**主動被駭**」，主因來至網路安全知識的不足，而誤入「毒」徑。

網友最容易點選「跟搜尋結果相關的網站」（42.3%）及「好友寄的信件或訊息」（29%）而上了有毒程式的釣鉤，誤入電腦被駭的危機。而另外依序還有「免費試玩或下載」（13.9%）、「火辣性感圖」（7.3%）及「折扣好康」（5.7%）等誘人資訊也會讓網友忍不住點選。

透過交叉分析也發現有趣的現象，**會被「折扣好康」內容吸引的女性網友爲男性的三倍，而「火辣性感圖」的內容吸引者則大多數爲男性網友。**

Key Logger

Solutions
Services
系統整合，資訊服務的第一選擇

www.ringline.com.tw

Key-logger 鍵盤側錄程式

- Key-logger程式可側錄所有自鍵盤輸入之字元，並將其存入一記錄檔(log file)之中
- 為持續記錄鍵盤輸入，key-logger程式相同於一般應用程式，須載入Windows registry，且須常駐於記憶體當中執行
- 駭客可藉由植入key-logger程式，側錄電腦使用者鍵入之網路帳號、金融密碼、甚至於個人機密文件；然後只須取得記錄檔(log file)，即可竊取各種電子資料

按鍵竊聽器的運作方式

使用者在已經被植
入竊聽木馬的PC上
登入網路銀行

身分證字號 H123456789

網路銀行密碼 ********

帳號和密碼得手！

網路身分竊犯在另
一部PC利用接收器
竊聽的所有按鍵

天堂虛擬寶物種類多 木馬盜"天幣"

天堂遊戲／國內首宗　木馬盜「天幣」　4學生落網 2001/9/10 11:53

記者鄭哲政／台北報導

令國內百萬網友痴迷的知名遊戲網站「天堂」，近來屢傳玩家虛擬裝備「寶物」、「天幣」遭竊案件，刑事警察局經深入調查，逮捕最姓大學生等4名學生嫌犯，刑事局表示，嫌犯利用一種能紀錄電腦按鍵使用情形的木馬程式，侵入網咖電腦取得他人帳號、密碼，進而盜走「寶物」、「天幣」、「遊戲點數」，甚至販售謀利。

刑事局偵九隊表示，網路遊戲已成爲青少年重要的休閒模式，但近來令國內百萬網友痴迷的「天堂」遊戲，卻不斷發生玩家的「寶物」、「天幣」遭竊，這些虛擬裝備都是玩家藉由打怪獸，一點一滴辛苦「練功」得來。

刑事局在連續接獲數十名網友報案後著手深入調查，追出有玩家爲了提升遊戲人物的等級，挺而走險盜用其他玩家的遊戲帳號、密碼，侵入竊走被害人的「寶物」、「天幣」，甚至販售謀利（目前行情是1萬台幣換100萬天幣）。警方經月餘調查後，逮捕到最姓、張姓、郭姓等4名學生，其中最爲大學生，其餘則是高中生。

最等人向警方供稱，他們是在「天堂」遊戲網站的討論區內看到「如何防止帳號被盜」的文章，內容表示部分玩家使用過的網咖電腦，會在暫存資料夾TEMP裡面留下全部的

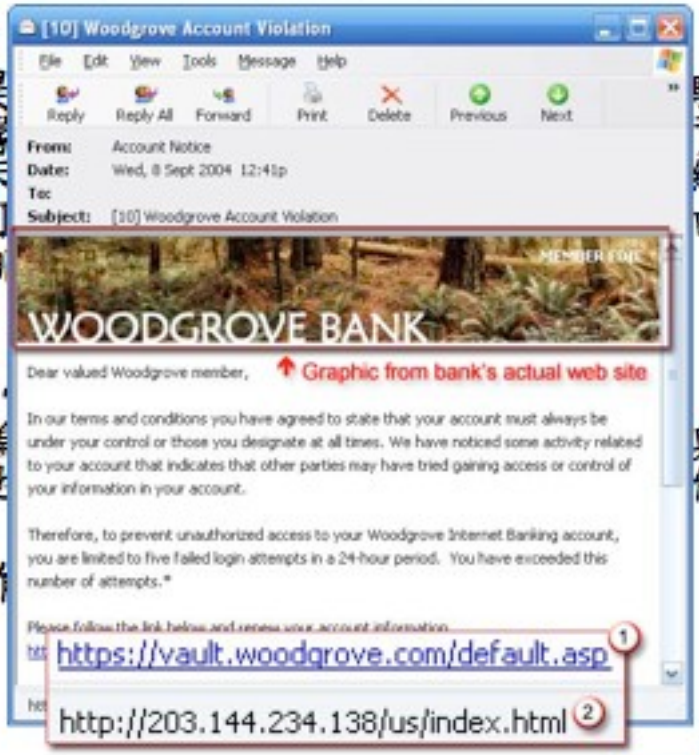
- 天堂遊戲／虛擬「寶物」種類多 可換真鈔
- 天堂遊戲／KEYLOG木馬 按鍵紀錄程式
- 高中生現金轉讓「虛擬貨幣」 未「文創」險被告
- 寶物遭小偷？ 網路虛擬竊案 警方頭痛
- 網路犯罪／虛擬遊戲儲值卡 首度淪為洗錢管道
- 數位觀察者／虛擬貨幣的前世今生
- 犯罪行為進入虛擬世界 天堂成地獄

網路釣魚

Solutions Services
系統整合・資訊服務的第一選擇

網路釣魚攻擊

- 何謂網路釣
  - 網路釣魚是
    利用各種瞞
    例如信用卡
    魚的途徑可
    信件或彈跳



騙人士
資料；
網路釣
由垃圾

- 網路釣魚詐
  - 騙子的詐騙
    也一樣。他
    特徵
  - 網路釣魚詐

與網頁
他重要

網路釣魚攻擊

冒充奇摩盜帳號密碼 網友拇穿「駭」人招數

〔記者林嘉東／台北報導〕網友上網一看見有彈跳式視窗出現（見圖，記者林嘉東翻攝），常習慣性移動游標點選，小心！這可能是你被騙的第一步。

最近網路盛傳一封電子郵件，揭露駭客利用拍賣網站上的彈跳式廣告，引誘買家點入後，再冒充奇摩登入頁面，騙網友輸入自己的帳號、密碼。

彈跳視窗請君入甕

這封主旨為「看看人家如何盜取你的帳號密碼」的電子郵件指出，歹徒先在各大知名拍賣網站上佯裝拍賣物品，接著在自己網頁下方設置一個彈跳式的廣告視窗，吸引買家及民眾點選，如果買家不察，真的點選、進入，螢幕還會出現警告畫面，要買家小心被設計，鄭衛民眾的心防。

網友一旦點閱並確認後，螢幕就會顯出冒牌的奇摩登入頁面，眼尖的網友若仔細比對，可察覺畫面上方的網址列，與正牌的雅虎奇摩網址列完全不同，但稍不注意，很可能就「引君入甕」。買家若依其提示，輸入自己的帳號、密碼，自然無法登入，畫面還故意顯示「你帳號密碼輸入錯誤」，而在此刻，被害人的帳號、密碼已經悄悄被對方蒐集到手。

網路釣魚攻擊

假銀行網站 竊個資盜存款

〔記者黃敦硯／台北報導〕喜歡透過網路交易的網友可得當心了！在敲下鍵盤進行交易的同時，對岸的中國廈門正有犯罪集團以遠端遙控功能及鍵盤側錄程式（keyloger），側錄你上網時所輸入的帳號密碼，他們還會在你電腦植入木馬程式，搜尋你電腦所有磁碟的憑證檔案，接著便可任意轉帳或盜取你的個人資料，讓你被看光光、盜光光。

掌握多名中國可疑共犯

刑事警察局說，近來有一個由兩岸駭客組成的詐騙集團，專門購買網路關鍵字廣告服務，再架設冒充銀行、航空公司的假官方網站，一旦網友連結，便會遭到詐騙集團以「網路釣魚」方式植入木馬程式，經連日追查，刑事局已掌握多名可疑中國共犯身分，正透過管道請中國公安代為追查，而因損害情形仍持續擴大，刑事局昨緊急提出警告，請網友提高警覺。

駭客詐騙集團利用關鍵字搜尋，架設假網站，搜尋「土地銀行landbank」網站的網址，英文「land」應是小寫的「l」（圖左下），仔細看可發現變成阿拉伯數字的「1」，一旦網友連結，便會遭到詐騙集團以「網路釣魚」方式植入木馬程式，即可任意轉帳或盜取你的個人資料。（記者黃敦硯翻攝）

網路釣魚攻擊

- www.google.com ←→ www.googl1e.com
- tw.yahoo.com ←→ tw.yuhoo.com ←→ tw.yahco.com
- 遊戲橘子公司tw.gannania.com ←→ tw.gamania.com
- 7-11：www.7-11.com ←→ www.7-ll.com
- 宏碁電腦www.accer.com.tw
- 合作金庫www.tcbc-bank.com.tw
- 土地銀行www.landbank.com.tw ←→ www.1andbank.com.tw
- 中國商銀www.1cbc.com.tw ←→ www.icbc.com.tw

網路釣魚攻擊

- 網路釣魚 (phishing)詐騙的電子郵件特徵
  - 確認您的帳號
  - 親愛的重要客戶
  - 如果您不在 48 小時內回覆，您的帳號將被關閉
  - 按一下以下連結來存取您的帳號
    - Masked URL 住址範例

- 對於可疑信件的應變方式
  - 檢舉可疑信件
  - 點選電子郵件中的超連結時請小心
  - 使用您個人書籤或直接在網址列上輸入網址
  - 當您在網站輸入個人或金融資料前確認安全簽章(SSL)
  - 不要在跳出視窗中輸入個人或金融資料
  - 經常檢查您的信用卡與銀行明細

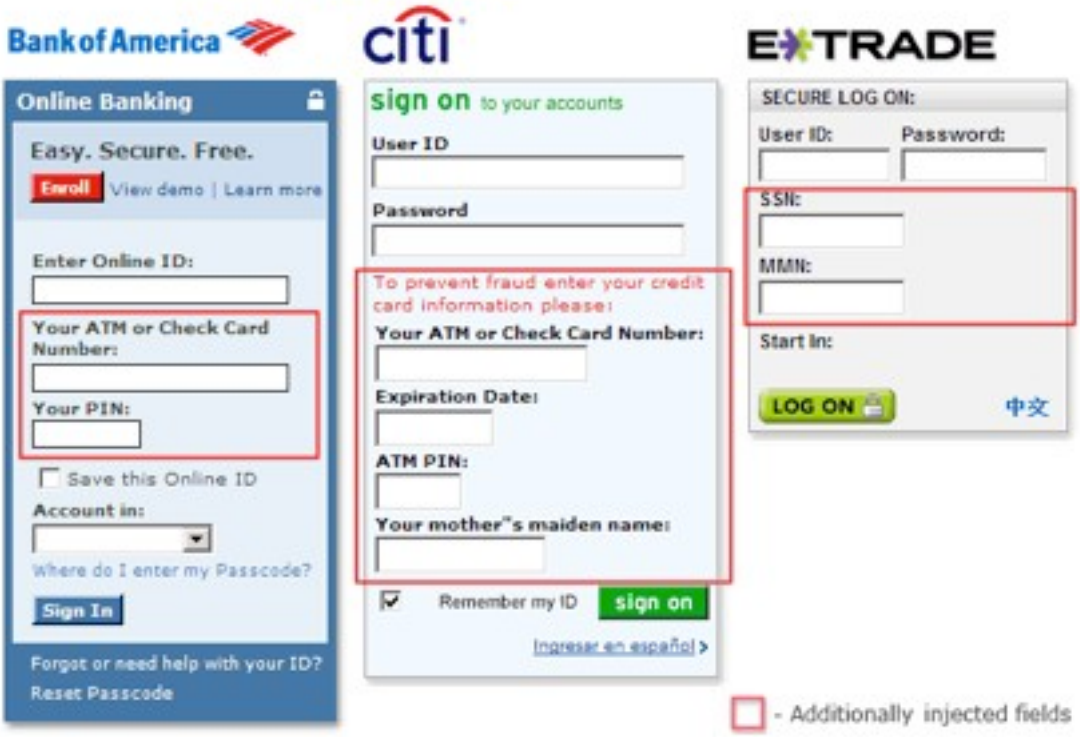
網路釣魚氾濫

- 詐騙網路銀行、線上遊戲帳號為主要目標
- 利用社交工程法獲取不法利益

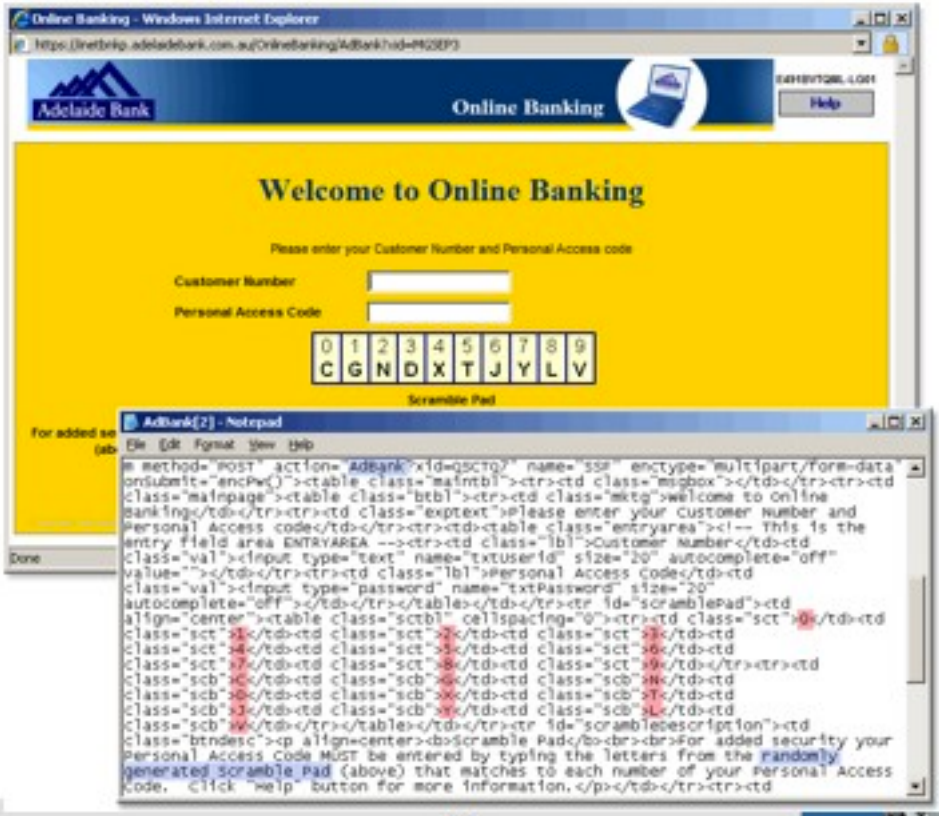
HTML Injection

Solutions
Services
系統整合，資訊服務的第一選擇

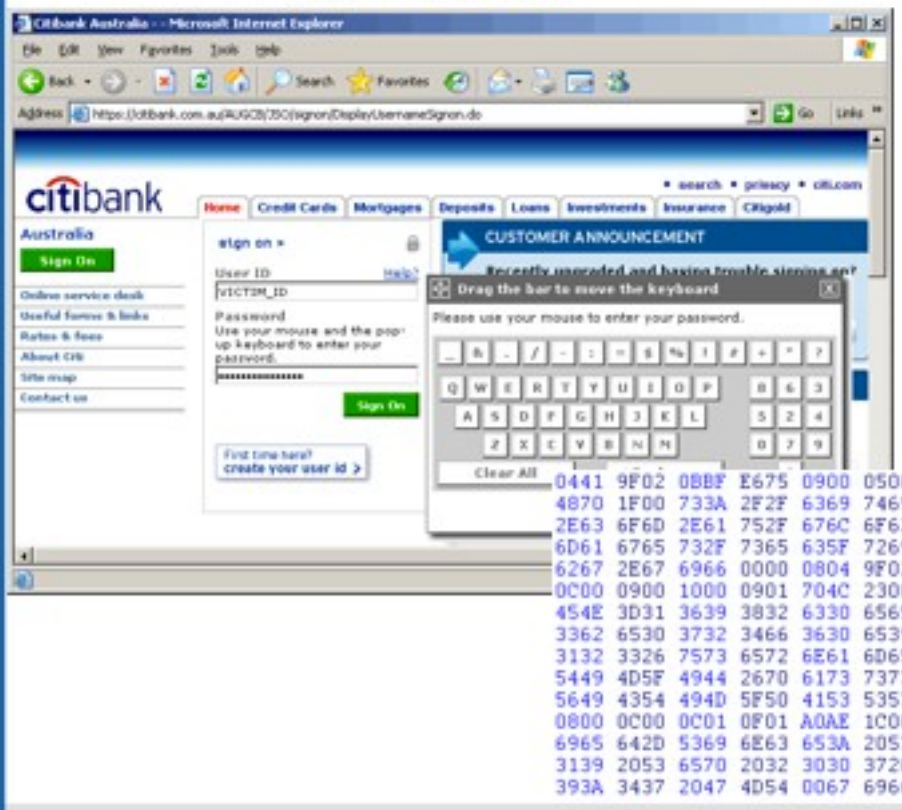
HTML Injection



Form Grabber



Form Grabber




```
0441 9F02 0BBF E675 0900 0500 1B01 1101 .A.....u........
4870 1F00 733A 2F2F 6369 7469 6261 6E6B Hp..s://citibank
2E63 6F6D 2E61 752F 676C 6F62 616C 5F69 .com.au/global_i
6D61 6765 732F 7365 635F 7269 6768 745F mages/sec_right_
6267 2E67 6966 0000 0804 9F02 0000 0000 bg.gif..........
0C00 0900 1000 0901 704C 2300 802B 9B02 ........pL#..+..
454E 3D31 3639 3832 6330 6565 3034 3932 EN=16982c0ee0492
3362 6530 3732 3466 3630 6539 6461 6261 3be0724f60e9daba
3132 3326 7573 6572 6E61 6D65 3D56 4943 123&username=VIC
5449 4D5F 4944 2670 6173 7377 6F72 643D TIM_ID&password=
5649 4354 494D 5F50 4153 5357 4F52 4400 VICTIM_PASSWORD.
0800 0C00 0C01 0F01 A0AE 1C00 6F64 6966 ............odif
6965 642D 5369 6E63 653A 2057 6564 2C20 ied-Since: Wed,
3139 2053 6570 2032 3030 3720 3032 3A35 19 Sep 2007 02:5
393A 3437 2047 4D54 0067 6966 0000 0000 9:47 GMT.gif....
```


Spyware

Spyware Threat

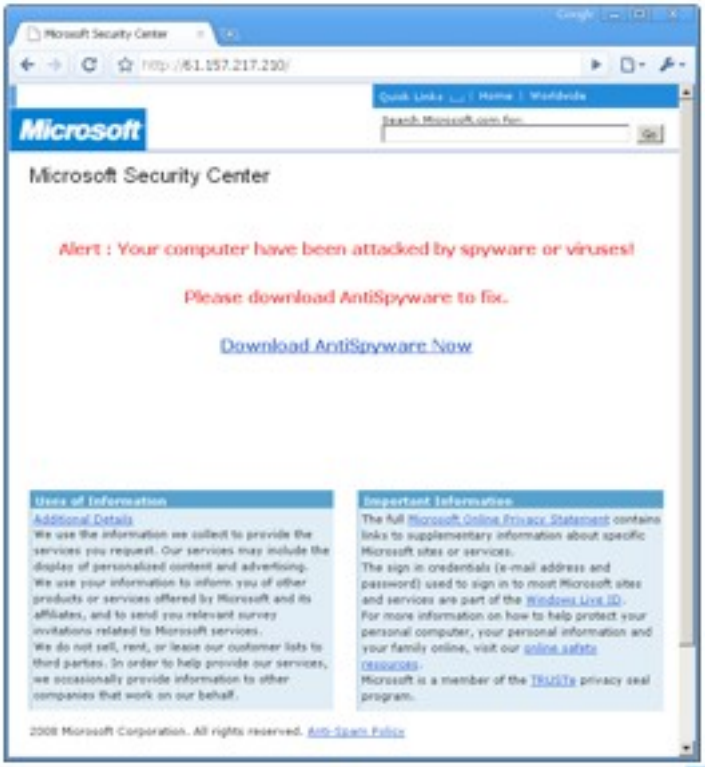
- 什麼是間諜軟體
  - 所謂的「間諜軟體」是一個統稱，泛指會在未經使用者同意的情況下進行廣告、收集私人資訊，或修改電腦設定等行為的軟體

- 間諜軟體的特徵
  - 我不斷看到廣告視窗
  - 我的設定遭到更改，而且無法恢復原本的設定
  - 我的網頁瀏覽器出現額外的元件，但我並不記得下載過這些元件
  - 我的電腦變得反應遲緩甚至當機

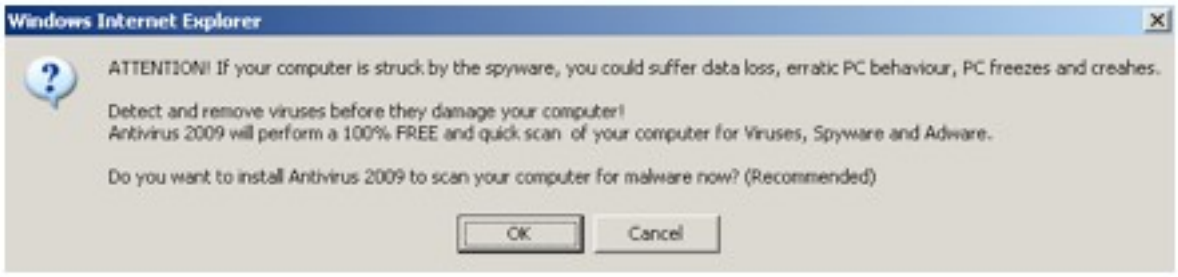
Are You Using Crack Version Software?

- Intervalhehehe: included in cracked version of WinRAR
  - Self-extractor runs WinRAR installer and a "explore.exe"
  - Redirect google.com, yahoo.com, etc. to websites that distribute rogue antivirus and antispyware solutions

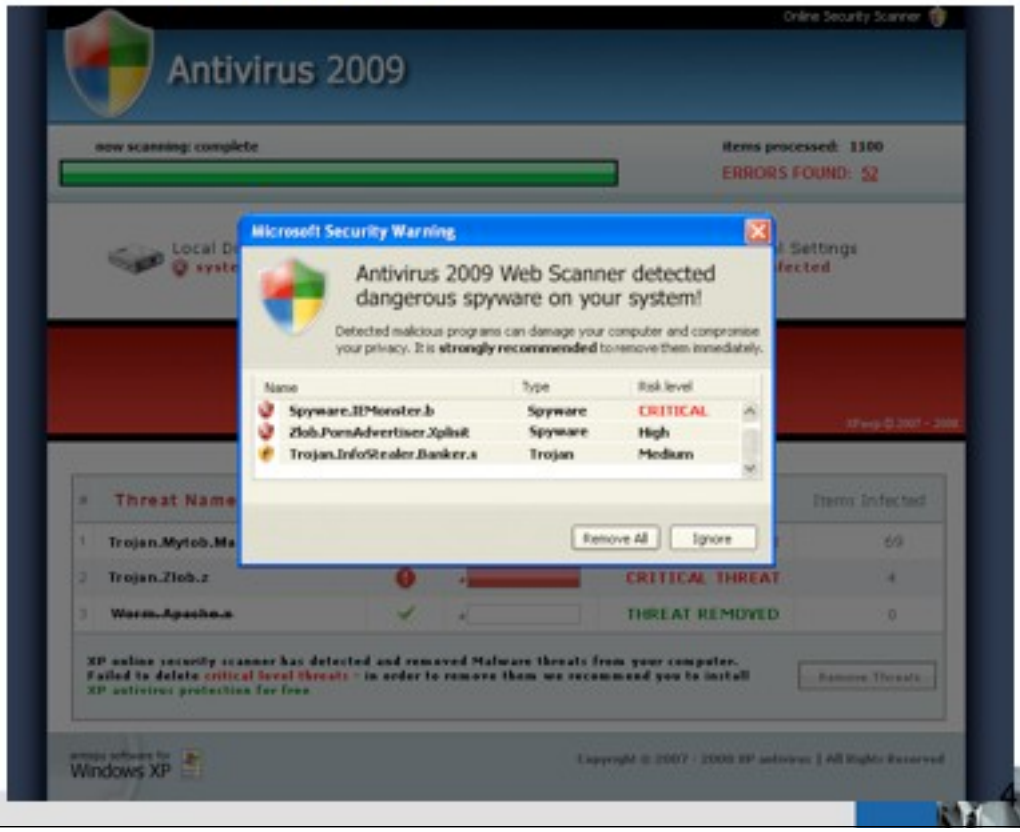
Are You Using Crack Version Software?



Antivirus 2009



Antivirus 2009



Botnet

Solutions
Services
系統整合，資訊服務的第一選擇

熱門新聞

正常網站卻隱藏惡意程式　企業應爲員工上網行爲把關

（記者[illegible]君／台北）

2006/10/20

過去資安專家[illegible]統漏洞潛入你的電腦。但根[illegible]急機四伏。

IDC1項名爲「[illegible]意程式最常使[illegible]

上月在台灣[illegible]過電子地圖或[illegible]近期發現當使[illegible]因爲該網站早[illegible]網站，轉往另[illegible]

而IDC的調查[illegible]感染病毒僵[illegible]路做爲私人用途的企業，比[illegible]止利用公司電腦進行私人用[illegible]規則並達成協議，也可透過[illegible]

僵屍電腦BotNet病毒肆虐　台灣網路受害高居全球第六

ETtoday 更新日期：[illegible]

國內這半年多來出現一種[illegible]供的資料顯[illegible]防制中心今[illegible]速全面清查[illegible]刑事局科技[illegible]國內已有20[illegible]政府機關、[illegible]對不特定對[illegible]

殭屍病毒入侵台灣　電腦遭殃

中國時報 更新日期：2006/10/04 07:00

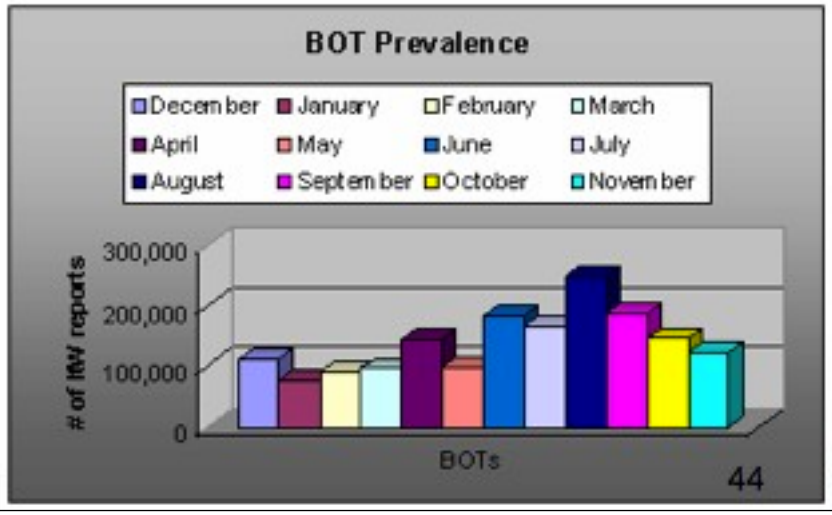
病毒快報／冒充安全更新程式蠕蟲　上百家企業受害

ETtoday 更新日期：2006/10/26 10:14　記者：記者陳曉雯／台北報導

趨勢科技於日前發現一隻冒充安全更新程式並自動至網站下載更新的蠕蟲：WORM_STRAT.DX，該蠕蟲是一隻會散發大量郵件的蠕蟲家族，憑著重複透過電子郵件四處散播，已經造成台灣、日本、中國大陸等地超過百家的企業傳出感染報告。趨勢科技表示繼今年九月WORM_STRATION.WO病毒在Microsoft 預定推出當月安全性公告的前一天，冒充安全更新程式而大量散播，並不到一個月就累積了155隻變種之後，此隻WORM_STRAT.DX蠕蟲之變種亦持續累積中，用戶應謹慎面對。

僵屍網路大行其道

- 估計有7百萬台的僵屍電腦
- 超過8成垃圾郵件的元兇
- 一年至少引起超過10億次的click fraud
- 平均每月成長15%



何謂 Bot & Botnet

- Bot
  - 又稱為魁儡程式或魁儡蟲，遭受感染後常見的行為如同魁儡或殭屍般可受遠端有心人士操控此電腦
- Botnet
  - 又稱殭屍網路 Zombie Network，或機器人網路 Robot Network，即一群 Bot 所組成的電腦網路
  - 駭客藉由 IRC 等管道遠端控制受感染的主機，可發動網路攻擊，包括竊取私密資料、網路釣魚(Phishing)、散布垃圾郵件(Spam)、發動阻斷式服務(DDoS)—恐嚇被駭網站等犯罪行為

藉由知名網站散播

連線至僵屍網路下載更多的惡意程式

Google Hacking

Solutions
Services
系統整合・資訊服務的第一選擇

Google Hacking Database (GHDB)

Google "admin account info" filetype:log 搜尋 進階搜尋 | 使用偏好

搜尋所有網站 ○ 搜尋所有中文網頁 ○ 搜尋繁體中文網頁

所有網頁

log started at 31-12-04 16:12 ... - [翻譯此頁]
... Default VirtualServer created 31-12-04 16:12:47,WARNING,Info,SERVER, admin account
info: username: admin password: xj8dbm 31-12-04 16:12:47,WARNING,Info ...
mem[redacted]erver.log - 4k - 頁庫存檔 - 類似網頁

```
------------------------------------------------------------
------------- log started at 31-12-04 16:12 ------------
------------------------------------------------------------
31-12-04 16:12:46,ALL,Info,server,      Server init initialized
31-12-04 16:12:46,ALL,Info,server,      Server version: 2.0.20.1 Win32
31-12-04 16:12:47,WARNING,Info,SQL,     created table ts2_servers
31-12-04 16:12:47,WARNING,Info,SQL,     created table ts2_server_privileges
31-12-04 16:12:47,WARNING,Info,SQL,     created table ts2_channels
31-12-04 16:12:47,WARNING,Info,SQL,     created table ts2_channel_privileges
31-12-04 16:12:47,WARNING,Info,SQL,     created table ts2_clients
31-12-04 16:12:47,WARNING,Info,SQL,     created table ts2_bans
31-12-04 16:12:47,ALL,Info,server,      Starting VirtualServer id:1 with port:8767
31-12-04 16:12:47,WARNING,Info,SERVER,  Default VirtualServer created
31-12-04 16:12:47,WARNING,Info,SERVER,  admin account info: username: admin password: xj8dbm
31-12-04 16:12:47,WARNING,Info,SERVER,  superadmin account info: username: superadmin password: oihpaf
31-12-04 16:12:48,ALL,Info,server,      Server init finished
31-12-04 16:14:40,ERROR,All,fnaMain,    unable to detect external ip
31-12-04 16:16:40,ALL,Info,server,      Server shutdown initialized
31-12-04 16:16:43,ALL,Info,server,      Server shutdown finished
```


Google Hacking Database (GHDB)

Google filetype:xls 身分證字號 搜尋 進階搜尋 | 使用偏好

所有網頁 ○ 中文網頁 ○ 繁體中文網頁 ○ 台灣的網頁

[xls] 人力需求表 - 上午10:44
檢索摘取: Microsoft Excel - HTML 版
13, 身分證字號S1[redacted]135, 鄭 碧比雅久, 14, 出 生 日 期52 年 02 月 02 日, 年 月 ... 21, 身分證字號P12[redacted]819, 鄭 碧三陳 ...
www[redacted]出入證申請書-1 (新) .xls -
類似網頁

姓 名林[redacted]雍				牌照號碼J86 —[redacted]
身分證字號S 1 2 0[redacted] 1 3 5				鄭 碧比雅久
出 生 日 期[redacted] 02 月 02 日			年 月	出廠年月2000 年 10 月 年
交 通 工 具	□汽車□機車 □其他 可複選			顏 色銀
刷 卡 編 號7 6 3 4 8 3				C、C124
勞保加保日期93 年 07 月 12 日			年 月	有效日期 98 年 03 月 年
戶 籍 地 址 高雄[redacted] 鳳南里 11 鄰鳳明[redacted] 1 號		機車排氣檢查合格日期：96 年 03 月		
個人連絡電話	0 9 3 5[redacted]	工 作 類 別	□自工□冷作□配管□電焊□電工□鉛架□行政管理□其他 依職務選.	

Google Hacking Database (GHDB)

Google filetype:xls 身分證字號 生日 住址 -範本 搜尋 進階搜尋 | 使用偏好

所有網頁 中文網頁 繁體中文網頁 台灣的網頁

[XLS] Sheet1

檔案類型: Microsoft Excel - HTML 版

2, 職稱, 姓名, 身分證字號, 性別, 生日, 住址, 電話, 3, 校長, 張[redacted], J12[redacted]3, 男, E+4年10月16日, 新竹縣[redacted]58號, 03-55[redacted]06 ...

163.[redacted]c/92_4.xls - 類似網頁

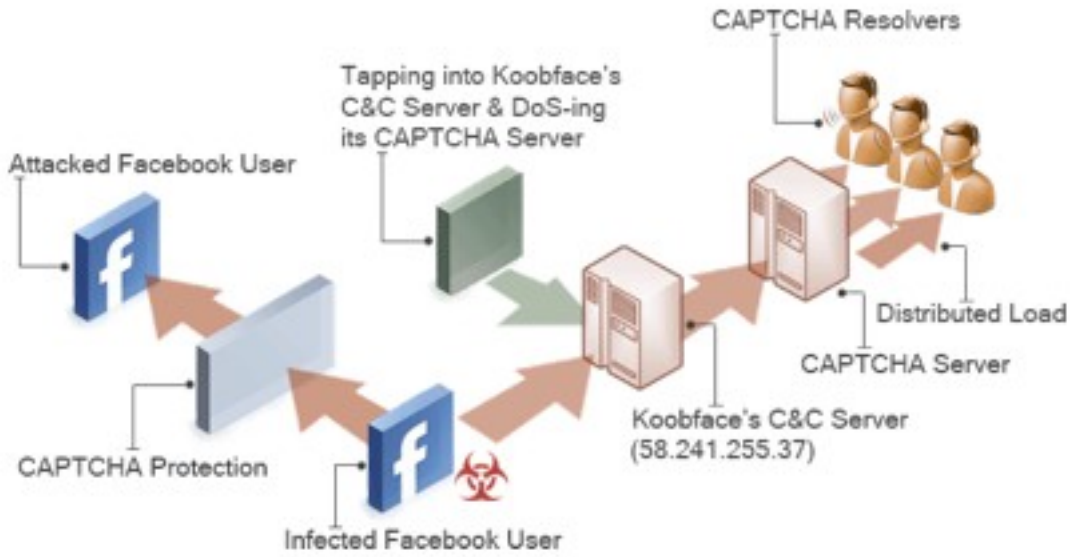
Google Hacking Database (GHDB)

	A	B	C	D	E	F	G
1	[redacted]國民中學科學研習小組申請進入苗栗三義大克山自然保護區人員名冊						
2	職稱	姓名	身分證字號	性別	生日	住址	電話
3	校長	張[redacted]	J120[redacted]	男	E+4年10月16日	新竹縣[redacted]	[redacted]306
4	教務主任	洪[redacted]	E102[redacted]	男	E+4年8月21日	新竹縣[redacted]	[redacted]336
5	教學組長	張[redacted]	K120[redacted]	男	E+4年3月30日	苗栗縣[redacted]	[redacted]010
6	註冊組長	黃[redacted]	M220[redacted]	女	E+4年9月24日	新竹市[redacted]	[redacted]450
7	衛生組長	劉[redacted]	K120[redacted]	男	E+4年12月22日	新竹縣[redacted]	[redacted]437
8	幹事	陳[redacted]	J220[redacted]	女	E+4年9月15日	新竹縣[redacted]	[redacted]850
9	學生	古[redacted]	J123[redacted]	男	E+4年12月6日	新竹縣[redacted]	[redacted]698
10	學生	徐[redacted]	J222[redacted]	女	E+4年1月15日	新竹縣[redacted]	[redacted]020
11	學生	吳[redacted]	J222[redacted]	女	E+4年8月29日	新竹縣[redacted]	[redacted]975
12	學生	邱[redacted]	S124[redacted]	男	E+4年9月24日	新竹縣[redacted]	[redacted]943
13	學生	羅[redacted]	J123[redacted]	男	E+4年11月4日	新竹縣[redacted]	[redacted]236
14	學生	魏[redacted]	J123[redacted]	男	E+4年6月10日	新竹縣[redacted]	
15	學生	廖[redacted]	J123[redacted]	男	E+4年5月15日	新竹縣[redacted]	[redacted]011
16	學生	蔡[redacted]	J123[redacted]	男	E+4年12月8日	新竹縣[redacted]	[redacted]870
17	學生	林[redacted]	J222[redacted]	女	E+4年6月22日	新竹縣[redacted]	[redacted]561
18	學生	林[redacted]	J222[redacted]	女	E+4年3月21日	新竹縣[redacted]	[redacted]283
19	學生	邱[redacted]	J223[redacted]	女	E+4年12月20日	新竹縣[redacted]	[redacted]383
20	學生	彭[redacted]	J123[redacted]	男	E+4年4月13日	新竹縣[redacted]	[redacted]027
21	學生	范[redacted]	J123[redacted]	男	E+4年9月17日	新竹縣[redacted]	[redacted]985

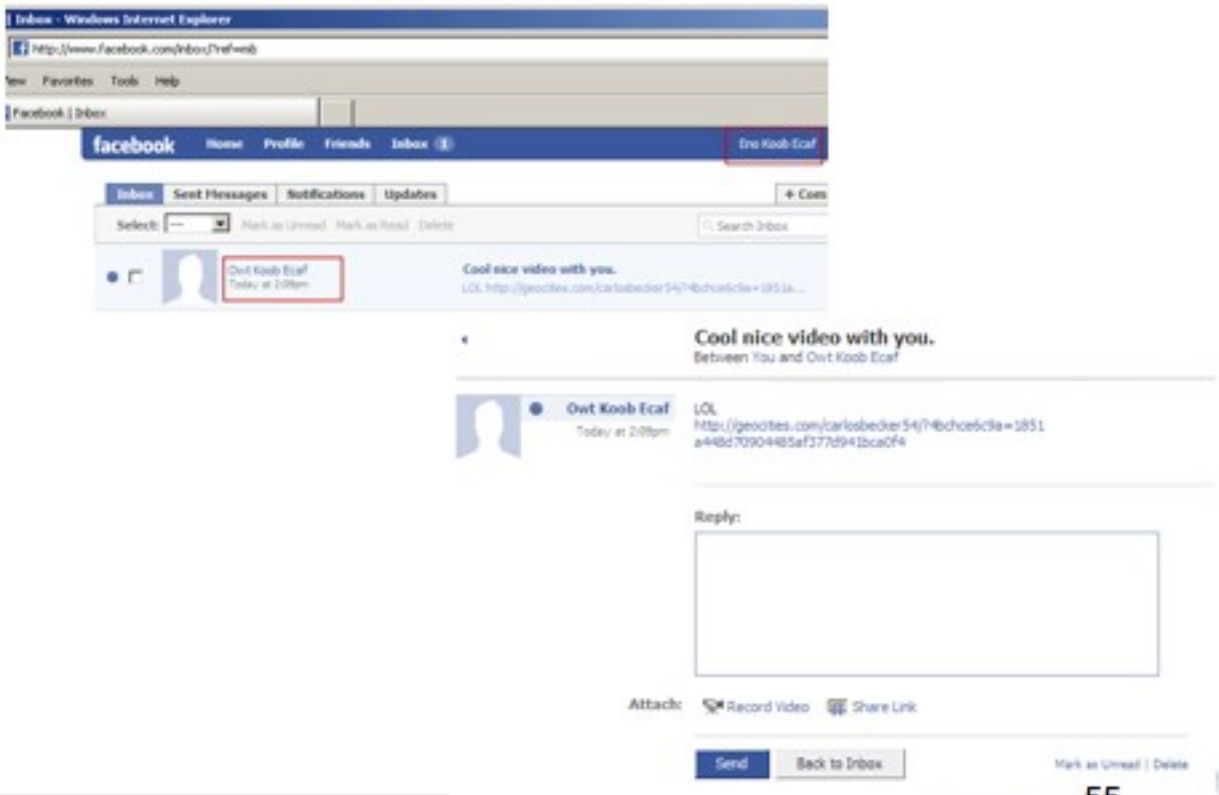
Koobface

Solutions
Services
系統整合，資訊服務的第一選擇

Koobface



Koobface



Koobface

正確有效的防護觀念

Solutions

系統整合，資訊服務的第一選擇

Services

如何避免個人資料外洩

對任何主動接觸的電話、來訪、簡訊與電子郵件都要小心，對任何宣稱是合法機構員工的人都要直接向該機構加以確認。

- 不要任意提供公司或學校單位的任何資訊，包含個人資料與組織架構。
- 不要在信件中提到任何個人資料或財務資訊，也不要回應請求此類資訊的電子郵件

如何避免個人資料外洩

未確認網站安全設定之前，不要傳輸個人或財務資訊

- 留意 URL 的正確性
- 若有任何疑問，直接聯繫該網站或公司，不要點選網站上的連絡連結
- 安裝合法、正確的防毒軟體、防火牆、垃圾郵件過濾器

面對網際網路潛在威脅的方法

- 定期更改帳號與密碼，最好是英文加上數字，並不洩漏予他人
- 安裝最少的系統元件：降低被入侵的風險
- 安裝最新的Server Pack及Hot Fix，確保Bugs都已經修復
- 關閉不需要的服務和埠(Ports)
- 遠離來路不明的軟體，檔案，磁片及光碟 ；並隨時注意電腦異常狀況
- 掌握病毒情報：隨時注意最新的病毒新聞
- 定期更新病毒碼、掃毒引擎及程式
- 定期備份

別當好奇寶寶，但要適度雞婆

- 不要瀏覽非工作相關或不信任的網站
- 不要下載安裝未經認可的軟體或程式
- 不要開啟可疑或非工作相關的信件附檔
- 對任何提到"緊急"或"個人金融"保持懷疑態度
- 對信件有任何一點疑慮千萬不要點選e-Mail裡的超連結
- 不要填寫e-Mail裡有關個人金融資料的表格
- 在網站上輸入信用卡號或個人資料時先確認該網站安全性
- 不將e-Mail留在任何公開的網頁上
- 不開啟來歷不明之信件、 不轉寄非必要之信件、 不回應任何未知的信件
- 經常或定期登入你的網路帳號
- 定期確認你的銀行帳戶、信用卡的交易狀態都正確無異常
- 自助互助，告知相關單位你發現的網路釣魚事件

Q&A