資訊安全宣導課程

林彥丞 111/07/27

大綱

一. 資訊安全新威脅

二. 安全防護實務

A. USB病毒

B. 社交工程演練及防範對策

C. 資訊安全停看聽

D. 必須知道的資訊安全防範技巧

三. 物聯網之資訊安全隱憂

資訊安全新威脅

據說當年鐵達尼號沉沒現場，搜救隊伍曾打撈起海面上載浮載沉的LV硬殼行李箱，箱內居然滴水未進。

「每個行李箱都有一個唯一的開箱密碼，每位來LOUIS VUITTON專賣店購買行李箱的客人，都會得到一組自己的鑰匙和獨立密碼，客人可以用這一把鑰匙開啟自己所購買的所 有LOUIS VUITTON行李箱，旅途中不必再帶 著一大把鑰匙，也不必為找不到哪一把鑰匙 而煩惱。」

每一把鎖都進行編號，每一個號碼都記錄在 一張卡片上，由VUITTON公司保管，當買家 遺失的行李箱被人發現後，可以根據鎖上的號碼在VUITTON的卡片櫃中找到行李箱的主 人，並通知前來VUITTON公司認領。

資訊安全新威脅

- 你上網駭客竊密! 公共WiFi藏資安風險
- 露天拍賣4千帳號 遭停權

安全防護實務

USB病毒

- 隨身間諜
- 網路購買來路不明USB硬碟藏毒

萬能的Shift鍵？

AutoRun
當電腦讀到「AutoRun.inf」會自動執行「AutoRun.exe」

AutoPlay
電腦自動提出建議，讓你選擇最合適軟體來開啟檔案

如何防範？

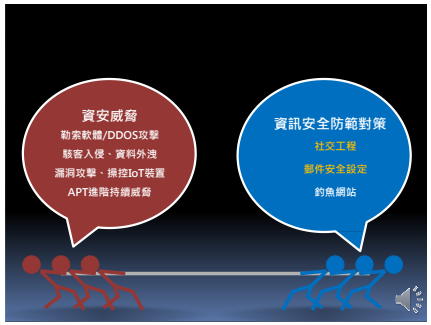
- 重要電腦，不隨意插上外來的USB隨身碟。
- 可由資訊人員以VM虛擬主機的方式來安裝USB掃毒軟體，進行USB插上之前的安全檢核。
- 公文資料勿放在USB內，以免資料遭竊與外流。

公文不重要？

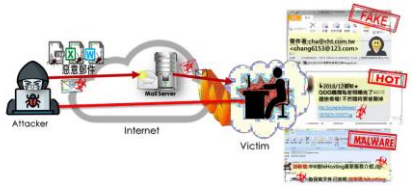
如果駭客拿到你認為毫無重要性的公文檔案，可能會：

- 把病毒與公文綑綁一起，你只要在電腦上執行公文檔案，病毒會自動入侵電腦，蒐集所有資料，或是破壞電腦。(例如病毒的指令是刪除電腦上的所有檔案)
- 喜歡惡作劇的駭客，有可能會把公文外洩的訊息當成新聞題材，賣給電視台，然後...外洩單位就會有一堆資安稽核做不完...。

社交工程演練及防範對策



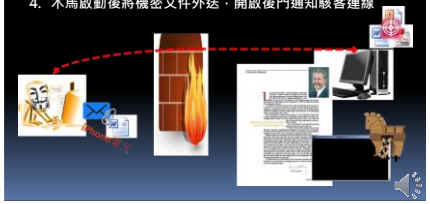
社交工程威脅與攻擊



- 利用人性弱點、人際交往或互動特性所發展出來的一種的詐騙技術
- 透過電話、電子郵件等方式偽裝身份誘騙您上勾受騙...
- 以郵件的攻擊最為常見，目的是為了避開嚴密的資通安全防護技術

社交工程攻擊手法

1. 蒐集訊息
2. 駭客利用Word/PDF等漏洞，將木馬夾在附件檔案中
3. 到處發信嘗試進行滲透
4. 木馬啟動後將機密文件外送，開啟後門通知駭客連線



透過Word漏洞攻擊-社交工程攻擊手法

案例分享:台灣健保局發現有人冒用健保局網址，連結木馬程式。

- 蒐集訊息
- 駭客利用Word/PDF等漏洞，將木馬夾在附件檔案中
- 到處發信嘗試進行滲透
- 木馬啟動後將機密文件外送，開啟後門通知駭客連線

利用郵件特性-社交工程攻擊手法

比對顯示名稱與電子郵件帳號?

這些欄位都是可以改的

電子郵件社交工程防範

社交工程的基本防護

- 執行各種作業系統、應用軟體的更新及設定。
- 必須安裝防毒軟體，並確實更新病毒碼。
- 密碼設定要符合複雜度的要求。
- 不要輕易相信電話中任何非經正式授權的請求。
- 不要任意安裝未經授權的軟體。
- 小心釣魚網站、詐騙廣告的陷阱。
- 不使用公務信箱作為登入的帳號。
- 不於社群網路中談論有關公務之相關內容。
- 修改個人資料的隱私設定(提供最少個資為宜)。
- 不要輕易點選陌生的加好友請求。
- 不任意點選社群網路聊天室或電子郵件的連結。

社交工程宣導短片 - 防駭三部曲

辨識惡意郵件要領

主旨欄位有標示[外部郵件]，表示此信是從公司外部寄來的信，需要提高警覺:如與公務無關則勿開啟；即使與公務有關，如有疑慮，仍需以電話向寄件者確認是否寄發此信件，以避免被惡意郵件攻擊(如勒索軟體)。

資訊安全停看聽

防護三部曲-停看聽

- 停–使用任何新系統前，必須先
  - 執行各種作業系統更新、應用軟體設定
    - Windows / Office Update
    - 設定瀏覽器安全性
  - 啟用個人防火牆
    - 控制台→Windows 防火牆→開啟防火牆
  - 安裝防毒軟體，並確實更新病毒碼 ftp://ftp.tust.edu.tw:3321
  - 不要安裝來源不明的軟體

- 停–
  - 不瀏覽可疑或非法網站
  - 不使用電腦時，採取登出、設定螢幕保護、關機或等防護

- 停–

使用任何電子郵件軟體前，必須先

- 設定收信軟體安全性
  - 關閉郵件預覽功能
  - 關閉自動下載圖片
  - 不要自動回覆讀信回條
  - 以純文字模式開啟郵件
- 防止垃圾郵件
  - 設定過濾垃圾郵件機制

- 停–

使用任何電子郵件軟體前

- 不開郵件附件和不點擊連結
- HTML可以撰寫ActiveX，只要電子郵件是HTML格式，□瀏覽含有執行碼的電子郵件，就觸發ActiveX執行

防護三部曲-停看聽

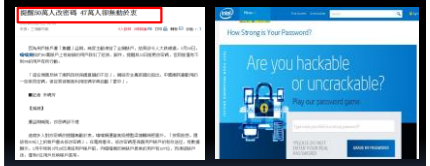
- 看–開啟電子郵件前應先檢視
  - 寄件人
    - 不認識的寄件人，開信要再三確認
  - 郵件主旨
    - 非關公務的郵件儘量不看
  - 附加檔案
    - 這些類型的附加檔案都要小心 exe、com 、 scr、pif、bat、cmd、doc、xls、pps/ppt、reg、lnk、hta、zip、rar、swf、html、mdb
    - 名稱顯示與業務無關或檔名怪異、錯誤，請勿開啟

❖看–已經在使用的作業環境
- 定期更改密碼
- 不同系統使用不同密碼
- 定期更新系統及軟體版本
- 不要在業務系統執行與系統無關的活動


防護三部曲-停看聽

❖聽–若懷疑郵件來源，必須進行確認
- 透過電話或其他方式向寄件人確認郵件真偽
- 不要在開啟郵件狀況下，直接按刪除鈕，應回到郵件清單(index)下刪除郵件，以免無意間直接開啟下□封郵件

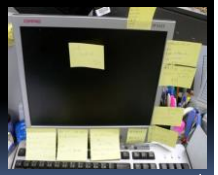

我的密碼夠安全嗎？



- 密碼設置建議
  - ✓ 古詩，例如：五言絕句
  - ✓ 某個自己記得起來的語彙，例如：保密防諜（1l3au4z;62u,6）

養成良好的資安觀念

- 不將公文資料以及公用設備攜帶出去。
- 不將外來隨身碟與公用電腦連結，避免病毒透過隨身碟進行感染。
- 電腦上的防毒軟體要定時更新。
- 電腦系統要定期更新漏洞修補程式。
- 不隨意開啟廣告郵件(有可能會中毒)
- 不隨意點選超連結網址(有可能會中毒)
- 不將開機及網站登入密碼貼在螢幕邊上。



必須知道的資訊安全防範技巧

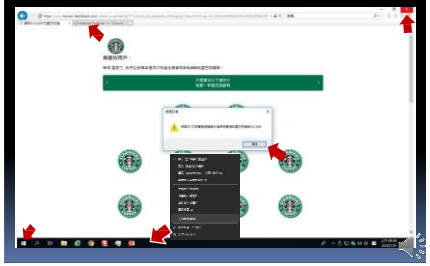
Line訊息要學會看盾牌顏色！

看到問題點了嗎？

辦別facebook真假粉絲團~

看到問題點了嗎？

瀏覽網頁出現釣魚訊息時，該怎麼辦?



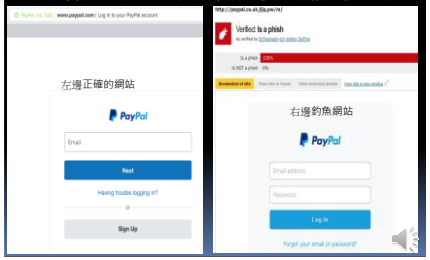
(惡意)手機惡意程式

手機詐騙簡訊攻擊

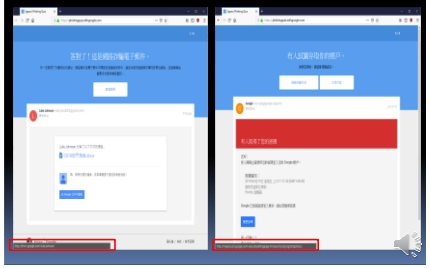
短網域成為釣魚網站最大的代罪羔羊

釣魚網站 – 與真實網站相似

★模仿官方網站的登入頁面，誘導使用者輸入帳號密碼



Google釣魚網站小測驗



資訊安全短片-
110年資安影片 第1名：三資小豬

三資小豬

針對資安 - 因應原則

只有在平時就做好準備，
才能快速因應突如其來的資安威脅

正確的資安觀念

- 提高警覺 加強危機意識
- 預防 詐騙手法攻擊

謹慎的防範動作

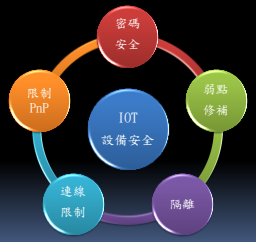
- 不隨意開啟下載郵件或軟體
- 定期系統更新 定期資料備份

物聯網之資訊安全隱憂

無所不在的物聯網設備

- 目前物聯網裝置的應用會越來越普遍，但與其有關的資安事件頻傳，因此無論是製作的廠商，還是企業乃至於個人，都應該提高警覺，重視這些設備的安全性

物聯網設備的安全



隱私問題

- 關心你的那些事?
- 誰正在偷窺你
- 隱私與物聯網

隱私問題

- 物聯網最大的問題，可能是隱私。
- 這麼多感應器與智慧設備，會收集關於你的大量訊息。
- 大量的監視攝影機及智慧手機裡頭的全球定位系統(GPS)晶片，追蹤你的行動。

科技來好處 同時你也要付出代價

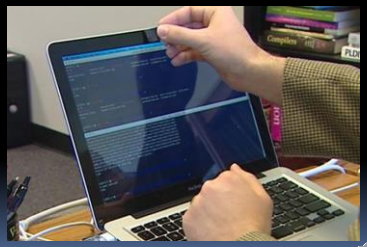
- 你希望線上零售商的網站記住你的喜好、上次買什麼，免得每次上網站都得重新輸入這些資訊;付出的代價就是網站曾在你的裝置上安裝餅乾(cookie)，追蹤你在網站上的行為，還會記錄你從哪裡上網、買東西後會去哪裡。
- 保全攝影機可以幫你避開小偷、強暴犯和恐怖份子;付出的代就是你和那些壞蛋一起被監視。

穿戴式裝置個人資料外洩

網路監視器被駭　女子入浴成實境秀

小心駭客控制你的生活用品

想避免被駭客監視？FBI 建議!!



隱私及資安問題

- 物聯網連接的設備經常監視和跟蹤消費者的行為，以此來調整和改善消費者體驗；然而用戶可能根本沒有被告知哪些數據將會被收集，又如何被使用。
- 裝置上所蒐集的資料誰可以擁有，不同組織或商業團體間互相交換這些資料是否合法等議題，目前皆未有明確法令的規範。

物聯網安全威脅

連網裝置複雜管理困難

- 物聯網裝置連上網路，通訊連接設備須具互通性，導致侵入裝置或滲透網路變得越來越容易，駭客攻擊將更加頻繁

傳輸未加密

- 80%進行資料傳輸時未加密
- 60%進行軟體更新時未加密

物聯網架構安全威脅

應用層
- 連結的物品多且複雜
- 隱私機密遭竊取、惡意中斷網路連線

網路層
- 無線通訊安全
- 訊號在空氣中傳輸易遭受外部截取

感知層
- 設備無人監控
- 機器容易被破壞盜取或冒名使用

物聯網架構安全威脅

感知層
- RFID標籤：硬體結構簡單、缺少加密性
- 容易被偽造，訊息容易被推算
- 傳輸及安全標準的不相同



物聯網安全威脅

網路層
- 存儲空間，計算能力及通信能力有限
- 資料加密、安全認證及管理，入侵檢測技術不足
- 無線傳感器網路(如IEEE 802.11、802.15等技術)，大功率無線設備可直接干擾其訊號

應用層
- 統一身份認證、統一金鑰管理及安全營運平台不足
- 整體系統和資料的故障修復

物聯網安全是全民都要面對的問題

製造商
- 開始設計時，必須將資安納入考量，並且開發者需要有安全開發經驗、訓練，最好產品在上市前滲透測試

企業用戶
- 需將物聯網設備盤點並列管，若是無法修補的設備，應考慮隔絕於主要網路之外
- 防護措施需將整個網路架構納入資安考量，並在採購時，要求廠商確保設備安全性

終端使用者
- 了解使用裝置的風險，如果不確定設備的功能，最好就不要使用
- 使用時，要將預設密碼更換成高度複雜的密碼

總結

- 資訊安全與個資防護應是一種習慣與文化，而不能只是一種技術與專業。