105年公務機密維護講習

－如何正確使用公務電腦及資訊

報告人：漢昕科技王顧問吉祥(105.4.12)

課程大綱

- 資安管理新挑戰
- 社交工程攻擊手法
- 網路釣魚防護須知
- 問題與討論

2016年十大安全威脅

- 進階持續性威脅攻擊(APT, Advance Persistent Threat)。
- 行動裝置的資料保護。
- 來自內部的威脅。
- 透過瀏覽器的攻擊持續增加。
- 社群網站引起的安全及隱私問題(個資法議題)。
- 檔案安全日趨重要(勒索軟體)。
- 資料安全走入雲端(雲端安全)。
- 駭客越來越猖獗(工具包使用簡易)。
- 資安變成商業營運必備要素(全球性議題)。
- 資料安全與隱私條例在全球有逐漸被聚合的趨勢。

資料參考來源：資安新聞網站

Evernote遭駭，要求近五千萬用戶改密碼

* 如果你是雲端筆記服務Evernote的愛用者，可能要注意一下這則新聞了。Evernote近五千萬名用戶發出修改密碼的通知函，理由是遭到駭客攻擊，導致大量用戶的帳號、電子郵件地址和密碼疑似外露。這也是繼Twitter和Facebook等社交網站遭遇駭客攻擊後，再一次有知名網站遇駭。
* Evernote透過官方部落格表示，用戶在Evernote中所記錄的各項內容並未被擷取，但為了小心起見，還是建議用戶儘快設定新密碼，以保障資訊安全。
* Evernote指出，該公司最初發現了非比尋常的可能性惡意活動。有些人用了不正當手法獲取了Evernote的帳號名稱、電子郵件和密碼。隨後，Evernote立即對該公司各平台的應用軟體進行升級，並協助所有用戶重新設定一組新密碼。
* Evernote執行長菲爾.李賓（Phil Libin）相當重視這起事件，他表示：「我們沒有儲存任何有關用戶的支付訊息，因此不會有與支付相關的資訊外露狀況。」

資料來源：isecurity

小心！史上最狠毒勒索軟體肆虐臺灣

* 勒索軟體CryptoLocker大舉入侵臺灣，公司與個人陸續傳出災情，該軟體會將受害者電腦加密，導致檔案無法使用，更限期3天支付9,000元贖金，否則將毀損解密金鑰。近日，有一支名為CryptoLocker的勒索軟體（Ransomware）現蹤臺灣，企業陸續傳出受害災情，該軟體透過釣魚郵件入侵，會將受害者電腦的檔案全數加密，導致檔案無法存取，而且駭客採用高超的加密技術，讓受害者無法自行復原，並限期3天支付9,000元贖金，否則將毀損解密金鑰，受害者苦不堪言。

資料來源：ITHOME

課程大綱

社交工程攻擊手法

引毒上身？五成網友主動下載有毒影音檔、電子郵件


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）

* 記者蘇湘雲 / 台北報導
* 總是抱怨網路毒駭事件層出不窮的使用者聽到以下消息，可能要先檢討自己為何如此「手癢」囉！入口網站最新調查顯示，網路中毒原因的前三名分別為「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為男性的三倍，而「火辣性感圖」的內容吸引者則大多數為男性網友。

何謂社交工程

- 社交工程(Social Engineering)為利用人性的弱點進行詐騙，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。駭客通常由電話、Email 或是假扮身份，問些看似無關緊要的問題等各種方法來進行社交工程。
  * 以人為本騙術為主
  * 技術門檻較低
  * 貪心：撿便宜的個性
  * 好奇：探索感興趣的事務
  * 缺乏警覺：有那麼嚴重嗎？

朋友？詐騙集團？

以假檢警手法詐騙，半年來得手超過4千萬元

* 南打偵八隊及屏東警方破獲以19歲古書維為首的詐騙集團，只有高職肄業的他吸收11名青少年當車手，以假檢警手法詐騙，半年來得手超過4千萬元，有退休老師被騙9次，領走畢生積蓄1200餘萬元，甚至差點連房子都抵押。

* 嫌犯將所得金額都拿來開趴，到案時僅起出5萬元贓款，被害人到場指認氣得大罵這些「死囝仔」不得好死。

資料來源：中時即時

網路釣魚

- 網路釣魚(Phishing)是網路上在常見的社交工程，特別是利用Email來欺騙，對於此類攻擊的最佳對應方法就是在預覽前就刪除所有類似的郵件，如此亦可同時避免會在背景觸發不良程式的惡意郵件攻擊。
- 只要使用者警覺性不足，點選網頁連結或是開啟來路不明郵件的附加檔案，都可能被植入惡意程式。
- 當收到不尋常或太好康的訊息時，應思考訊息內容的可行性，千萬不要下載附件或是連結網頁，並依循資安通報管道進行通報。

網路釣魚方法

- 砍站程式
- 首頁植入惡意程式
- 將DNS名稱更改其中一個英文字母
- 用數字1取代英文I
- 或用數字0來取代英文O
- xxx.com.tw 或 xxx.com
- 發E-mail、廣告或簡訊
- Google搜尋排名
- 向Google買關鍵字廣告
- 偽站已存在很久

網路釣魚之媒介

- 搜尋引擎與入口網站
  - Google
  - Yahoo
- IM軟體
  - MSN
  - Skype
  - ICQ
  - Facebook
- E-Mail
- 手機簡訊
- 廣告

網路釣魚目的

- 廣告目的(不斷開啟惡意廣告)
- 攻擊目的(植入後門程式)
- 金錢目的(詐騙行為)
  - 花旗銀行(mail)
  - 旅遊網站
  - 拍賣網站
- 竊取帳號密碼與個人資料

課程大綱

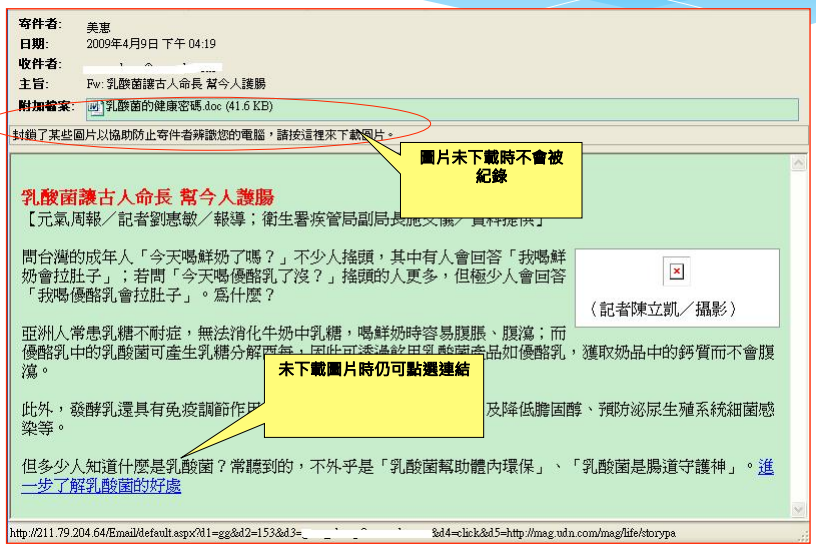
網路釣魚防護須知

惡意郵件攻擊

資料來源：法務部全球資訊網

- 好康報、養生保健、休閒娛樂、公務相關、美食、八卦新聞...

釣魚郵件記錄方式



判斷網路釣魚郵件方式

- 發信人的名稱或郵件地址
  - 是否有異常？需確認發信者的身分
- 電子郵件的主旨與內容
  - 與本身的工作、業務是否有關連
- 網頁連結或夾帶附件檔案是否可疑
  - 郵件內異常網址連結判斷
    - www.microsoft-mis.com
    - www.hinet1.net , www-hinet.net
    - www.paper-pchome.com , www.pchorne.com
    - 使用不明IP 代替URL（如：http://220.33.444.12/）

判斷網路釣魚郵件方式(續)

- 附加檔案之檢查
  - 與接收者的日常工作是否有關
  - 往往帶有惡意攻擊碼的檔案不易察覺
  - 常見病毒附件檔案副檔名
    （.bat、.pif、.exe、.zip、.src、.cmd、.rar等）
- 對於切身相關的電子郵件，若內含威脅、利誘、警告、提示等訊息內容，先思考後再行動作，應考慮詐騙之可能性

防範惡意程式與詐騙

個人資訊勿隨意登錄於不明網站

- E-mail 管理
  - 區分公司及個人使用之信箱
  - 在外登錄註冊之信箱，容易收到許多垃圾郵件，使用時務必小心
  - 不回覆來源不明之郵件
- 定期安檢作業
  - 即時更新軟體修補程式
  - 即時更新防毒軟體及病毒碼
  - 經常對系統進行檢測
- 實體隔離
  - 機敏資料應於實體隔離主機上作業

同仁對於可疑電子郵件應有警覺性

為何我會收到這封郵件?
* 應確認寄件來源及寄件者

我是否應該收到這封郵件?
* 應確認郵件主旨及郵件內容

我是否應該開啟這封郵件?
* 是否與業務工作相關
* 不開啟(點選)連結是否有影響
* 審慎查證(寄件者或資訊科)

電子郵件安全防制措施

- 同仁之電子郵件應「關閉預覽郵件」設定。
- 同仁之電子郵件應設定為「以純文字模式」開啟郵件。
- 不隨意開啟及轉寄與業務無關之電子郵件及網站。
- 如發現為不明來源或疑似網路釣魚之郵件應直接刪除。
- 不隨意點選或下載郵件內之連結與附件檔案。
- 如發現可疑信件應先與寄件者確認其真偽或通報資訊單位查證。
- 不隨意開啟郵件（確認寄件人）
- 不隨意開啟或下載附件
- 善用密件收件人
- 非必要不設自動回覆
- 不隨意留下郵件地址予他人
- 注意陌生之寄件者
- 了解組織傳送郵件規定

防範惡意電子郵件使用者防護

* 停 - 使用任何電子郵件軟體前，須先確認以下設定
  * 是否已安裝防毒軟體並確實更新病毒碼
  * 取消郵件預覽功能(outlook express/檢視/版面配置/預覽窗格，不要勾選顯示預覽窗格的設定)
  * 儘量使用純文字模式開啟信件(outlook express/工具/選項/讀取/讀取郵件，☑在純文字中讀取所有郵件)
* 看 - 收到信件後必須注意
  * 信件主旨是否與本身業務相關
  * 開啟信件前須先確認信件來源，否則建議刪除
* 聽 - 若懷疑信件來源必須進行確認
  * 透過電話或電子郵件向寄件人確認信件真偽

改善個人習慣

- 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
- 隨時更新作業系統與應用程式
- 安裝必要的防護軟體
- 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Email裡的超連結
- 不要填寫Email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

改善個人習慣(續)

- 不將Email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
- 安裝防止網路釣魚詐騙的工具軟體
- 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
- 確認你的瀏覽器、收信軟體、文書軟體及其他程式是最新版本，而且都已更新修補程式
- 自助互助，告知相關單位你發現的網路釣魚事件

總結：組織單位落實資安應有之作為

- 僅收集業務所需之資料，不要過度收集
- 個資的獲取與傳遞，需取得當事人同意
- 檢視現有作業流程是否存在安全之漏洞
- 導入適當技術控管措施以防止資訊外洩
- 加強作業人員之資安訓練與政策宣導
- 導入資訊安全管理制度，例如.ISO 27001標準

問題與討論