資訊安全與素養



課程大綱

- 資訊安全基本概念
- 資訊安全好習慣
- 重要資料要備份
- 應用系統要更新
- 電腦防毒要更新
- 螢幕保護設定及系統登入密碼設定
- 案例
- 結論

資訊安全基本概念

- 資安影片
- 資訊安全的意義
- 資訊安全可保護資訊免受多種威脅的攻擊，保障個人重要資料
  - –檔案
  - –網路資料庫
  - –電子郵件
  - –個人資料

資訊安全的本質

- 無孔不入
  – 整體資訊安全是建構於一系列環環相扣的保護機制下
  – 攻擊或破壞者只要找出其中最弱的一環，就可以完全瓦解整個保護機制。
- 覆巢之下無完卵
  – 只要最弱的一環被瓦解，所有的重要資料都可能被竊取或破壞。
- 沒有百分之百的安全
  – 必須對可能造成問題的弱點加以防護

資訊安全的目標

- 機密性：確保只有經授權的人，方能允許存取資訊。
- 完整性：確保資訊內容及資訊處理方法爲正確而且完整。
- 可用性：確保經授權的使用者當需要時，能存取資訊及使用相關的資產。

威脅來源的來源與動機

- 無意
  自然現象
  設計缺失
  操作缺失
  認知不足
- 故意

駭客

- 駭客工具通常會偽裝成一些有趣的小程式，然後由駭客送出或使用者自行從Internet下載這些經過偽裝的程式可以取得使用者電腦系統中的重要資料，並偷偷的回傳給駭客

電腦病毒

- 電腦病毒是一種電腦程式，設計有特定的功能，並且會感染寄生或附著在別的電腦程式或文件檔案裡面。有些電腦病毒就只有自我複製這個單一的功能與目的，有些電腦病毒則會破壞電腦裡面的資料，甚至會破壞電腦系統。

電腦蠕蟲

- 電腦蠕蟲也可說是電腦病毒的一種，與病毒不同的是，蠕蟲不會感染寄生在其他檔案。蠕蟲的主要特性是會自我複製並主動散播到網路系統上的其他電腦裡面。就像蟲一樣在網路系統裡面到處爬竄，所以稱爲「蠕蟲」。

木馬程式

- 木馬程式是一種電腦程式，偽裝成某種有用的或有趣的程式，比如螢幕保護程式、算命程式、電腦遊戲等，但是實際上卻包藏禍心，暗地裡做壞事；它可以破壞資料、騙取使用者的密碼等等。在學術定義上，特洛伊木馬不會自我複製，也不會主動散播到別的電腦裡面。

社交工程

- 是一種利用人際關係間的互動特性• 通常攻擊者會利用E-mail、電話或者是假的網站，騙取重要資料

資訊好安全習慣(一)

- 1.不明人士要盤查
  不明人士，在辦公區域內走動，應該主動詢問其來意。發現可疑狀況應加以制止或通知相關人員處理，即使是認識之同仁，進出其沒有權限出入之區域，也要加以勸阻或通知相關人員處理。
- 2.社交工程要小心
  如果你接到這種電話沒有確認對方的身分，就會輕易的把資料給別人，造成資料外洩，被有心人士利用好的，您的帳號是abc密碼是123您好，我是稽核處的組長，我現在在外面開會，臨時需要查一筆資料，但是我忘了帳號跟密碼你可以幫我查嗎？

資訊安全好習慣(二)

- 3.電腦不用要登出
  - •離開座位，電腦應該設定螢幕保護程式。
  - •長時間離開辦公室，記得將電腦關機
- 4.機密資料要保護
  - •敏感及機密文件不可遺留於桌面上
  - •必須存放於安全之場所並加以上鎖
  - •螢幕淨空
    - – 關機
    - – 登出
    - – 啓動螢幕保護程式
- 5.密碼設定要穩固
  - •密碼如果不夠複雜，很容易被破解並造成安全上的衝擊。

密碼設定小技巧

- 以中文輸入法按鍵來當成密碼
- 以英文字或數字穿插
- 將英文字母位移數個字
- 以英文的一句諺語或一段歌詞，取每個英文字字首當成密碼。

重要資料要備份

- – 預防重要資料或設備損壞遺失
- – 確保可用性
- • 可藉由不同的工具軟體達到備份的目的
- – Windows本身所提供的程式
  開始→附屬應用程式→系統工具→製作備份
- – 存放於儲存媒體並放置於安全場所

應用系統要更新

補強系統的漏洞

- 駭客經常透過漏洞來入侵電腦
- 作業系統或應用程式設計上的問題
- 更新軟體的修補程式
  - Windows update
  - Office update

電腦防毒要更新

- 防止電腦病毒及木馬的危害
- 不要隨意複製或下載不明檔案
- 不要隨意開啓檔案
- 不要安裝未經驗證安全的軟體
- 隨時注意病毒最新資訊，可以在相關資訊安全連結網站找到：
  –技服中心網站
  –防毒軟體廠商
  –報章雜誌
- 安裝防毒軟體或反間諜軟體
- 定期更新病毒碼及間諜軟體之定義

電腦中毒的徵兆

- 執行速度比平常慢
- 常常鎖定或不回應
- 磁碟或磁碟機無法存取
- 畫面上的功能表及對話方塊扭曲
- 不斷打開新視窗
- 不斷的當機或重新啓動
- 印表機印不出來
- 畫面顯示不尋常的錯誤訊息

瀏覽網路要提防

- 預防網路釣魚
- 不法人士僞造知名網站或是利用標題聳動的電子郵件作爲誘餌，騙取個人或機密資料。
- 最好不要下載及安裝未經授權軟體
- 避免下載不想要的軟體
- 點選連結網站要確認網址以免受騙
- 可能爲詐騙之郵件標題
  「請確認您的帳戶資訊」、要求更新信用卡資訊、「如果您不在48 小時內回應，您的帳戶將會關閉。」「親愛的客戶。」「請按一下下方的連結，進入您的帳戶。」

cookie的潛在危機

- cookie會自動記錄在網際網路的瀏覽及輸入的資料
- 應定期刪除cookie
- 調整隱私權之設定值

msn也會駭人

- 不隨便接收來路不明的檔案
- 不隨便點選陌生的網址
- 不要傳送個人資料，例如身分證字號、信用卡號碼等

電子郵件要過濾

- 除非您瞭解附件的來源且您知道會收到該附件，否則請勿開啓任何附件。
- 如果電子郵件附件係由不知名人士寄出，請立即刪除該郵件。
- 如果您必須寄送電子郵件附件給別人，請告知收件人，以免您的信件被誤認爲病毒。
- 使用垃圾郵件篩選功能協助您阻擋有害的電子郵件，很多這類郵件都含有危險附件。

螢幕保護裝置設定

- 1 執行：開始 / 控制台 / 顯示 (選擇【螢幕保護裝置】頁籤，如右圖)
- 2 設定：等候5分鐘
- 3 勾選：V繼續後，以密碼保護
- 4 套用 / 確定



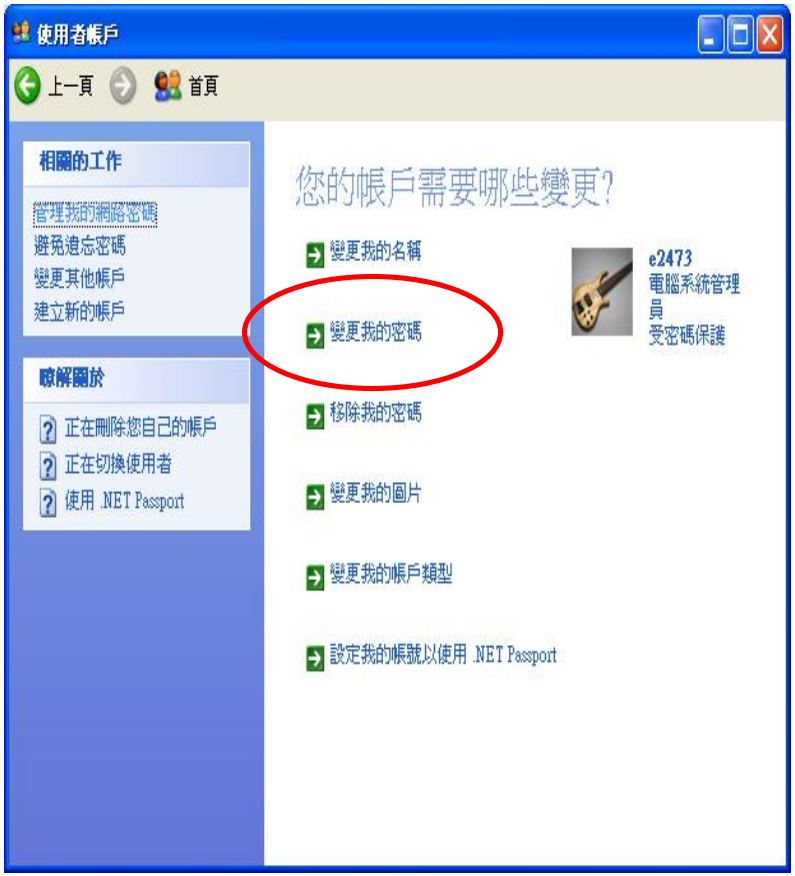
系統登入密碼設定(一)

- 1 執行：開始 / 控制台 / 使用者帳戶，如右圖
- 2 選擇使用者後，如下圖



系統登入密碼設定(二)

- 選擇變更我的密碼



結論

- 資訊安全最重要的是先做好，個人的資訊安全，只要同仁養成良好的使用習慣，人人隨時做好資訊安全第一線的防護，內部資訊安全就能得到保障，進而提升整體資訊安全環境。

