A01-001

資訊安全管理-個人篇

課程大綱

- 資訊安全基本概念
- 十大資訊安全好習慣
- 結論

第一章 資訊安全基本概念

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

- 以範例說明資訊安全的重要性
  - 大考中心
  - 信用卡資訊外洩
  - 假銀行網站
  - 國小教師辦駭客
  - 無線網路溢波

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，所有的政府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

CIA

- 機密性：確保只有經授權的人，方能允許存取資訊。

  例如：公文的傳送只有公文的接收人才能看到公文的內容，一般來說電子公文系統會使用加密的傳輸管道來傳送電子公文，讓公文就算被攔截也無法被讀取。
- 完整性：確保資訊內容及資訊處理方法為正確而且完整。
- 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。

其它安全性服務

- Non-repudiation 不可否認性
  - 防止存心不良的使用者否認其所做過的事，包括送出信件，接收文件，存取資料等。即交易的收發雙方參與安全管制並無法否認執行過的交易，例如數位簽署就具備不可否認性。
- Authenticity 鑑別性
  - 辨別資訊使用者的身份，即可以記錄資訊是被誰使用過，例如帳號、身份字號、員工編號。
- Accountability可歸責性
  - 所有主要的資訊資產應有人負責，並指定資產的所有人負責保護，管理的記錄必須是可以追溯。
- Reliability 可靠性
  - 資訊的正確度與可靠的消息來源和系統執行穩定度有關

威脅來源的來源與動機

無意
Unintentional

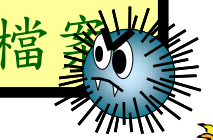
- 操作缺失
- 自然現象
- 認知不足
- 設計缺失

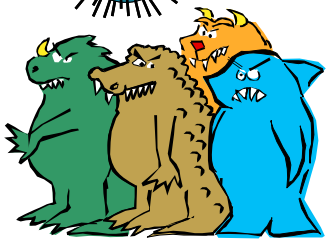
故意
Intentional

駭客

Internet

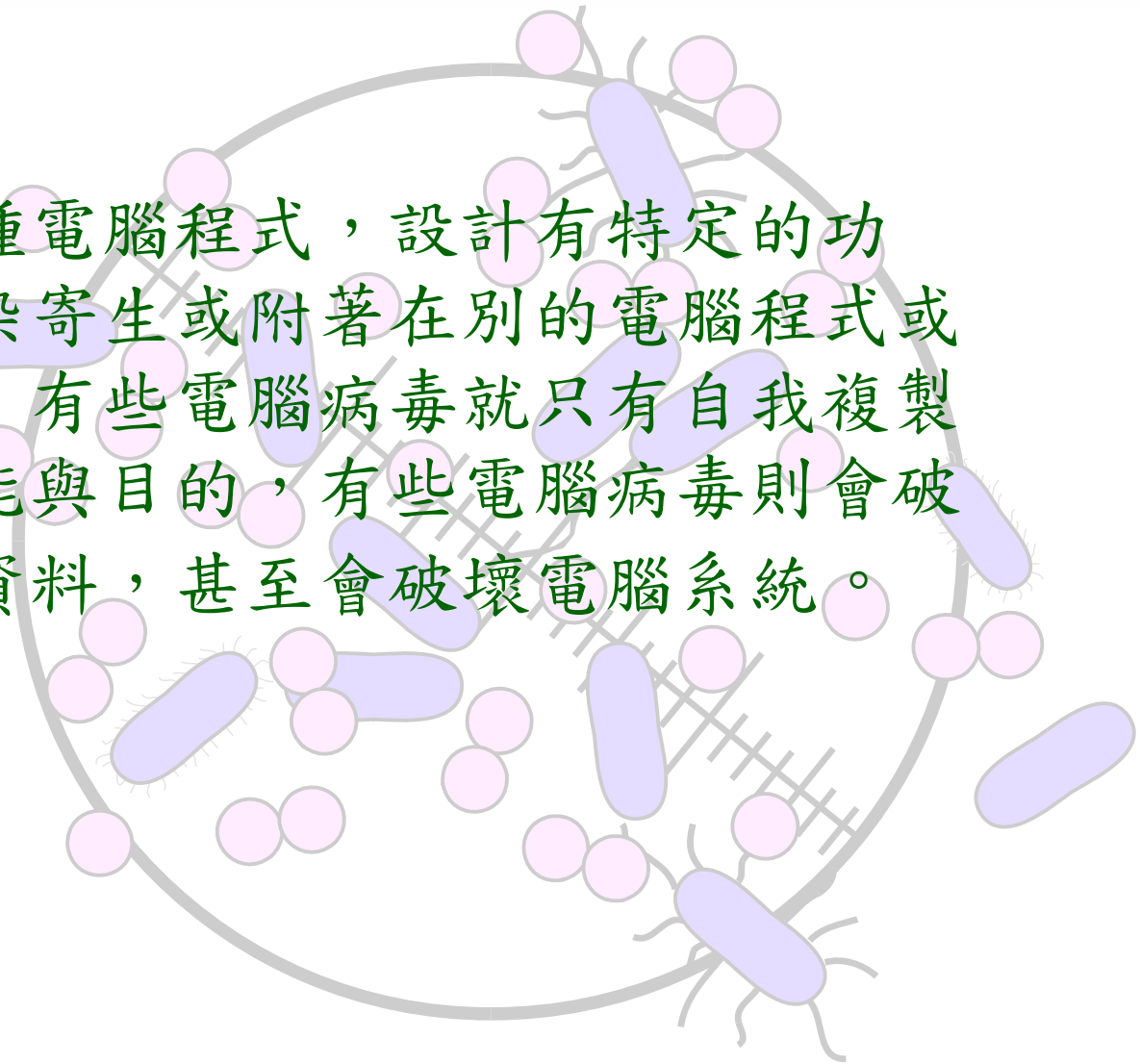
它也可以暗地打開某些通訊埠(port)，作為駭客自由進出你的電腦系統的後門，進而隨意存取你系統裡面各種重要的檔案





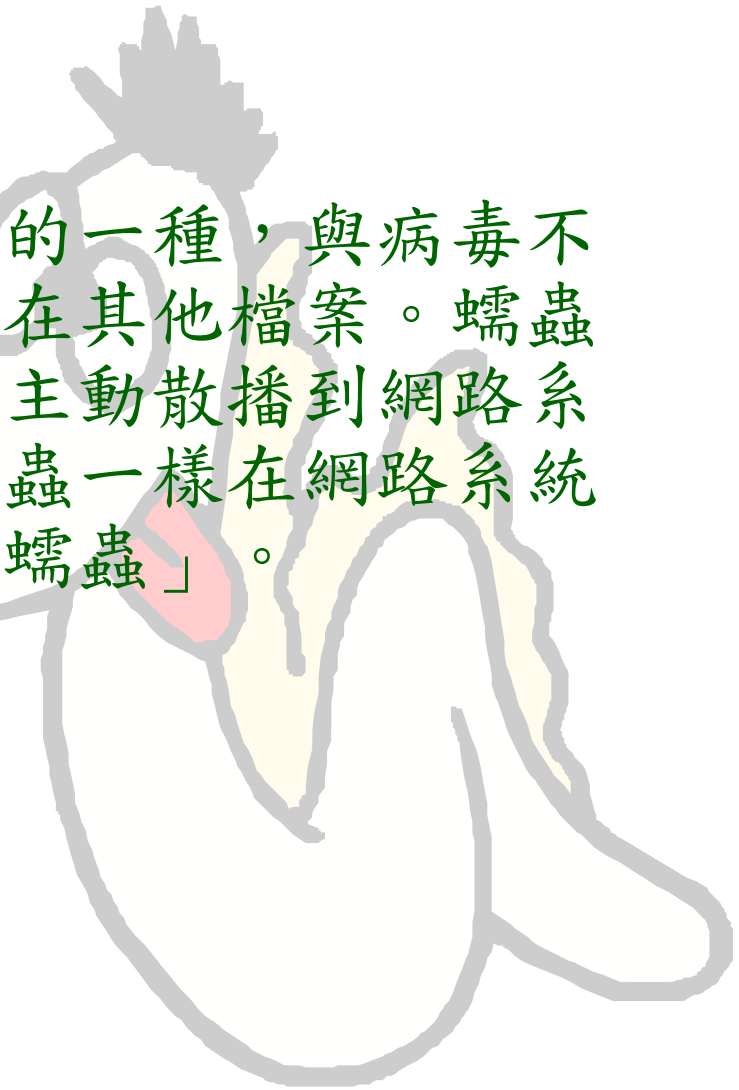
駭客工具通常會偽裝成一些有趣的小程式，然後由駭客送出或使用者自行從Internet下載這些經過偽裝的程式可以取得使用者電腦系統中的重要資料，並偷偷的回傳給駭客

電腦病毒



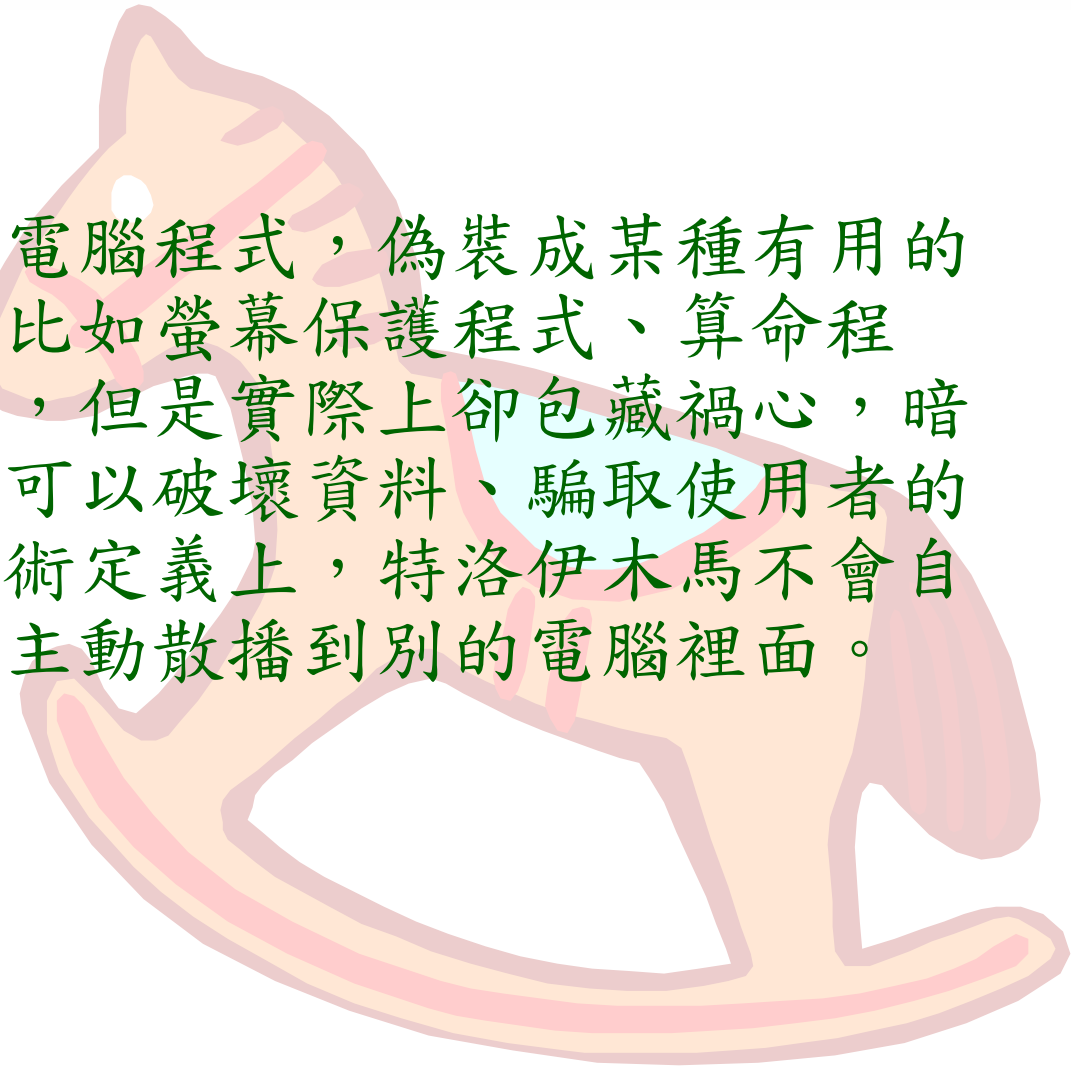
電腦病毒是一種電腦程式，設計有特定的功能，並且會感染寄生或附著在別的電腦程式或文件檔案裡面。有些電腦病毒就只有自我複製這個單一的功能與目的，有些電腦病毒則會破壞電腦裡面的資料，甚至會破壞電腦系統。

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，所以稱為「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

第二章 十大資訊安全習慣

1.不明人士要盤查

防止非法破壞

- 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

社交工程要小心

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？

好的，您的帳號是abc密碼是123

- 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

3.電腦不用要登出

防止非法存取

- 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
  - 杜絕來自網路破壞
  - 防止帳號或密碼被盜用
  - 防止重要資料遭竊

4.機密資料要保護

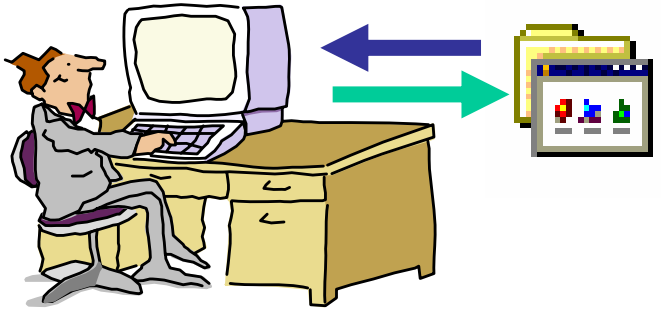
清桌作業

- 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
  - 啟動螢幕保護程式

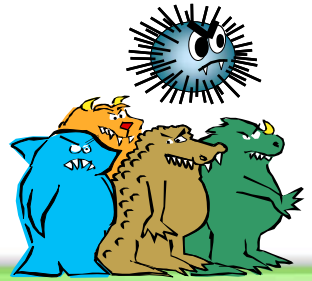
電子檔案文件保護

- 重要或敏感的檔案要分開存放
- 沒權限就不允許開啟或更改
- 設定密碼、或以加密軟體保護

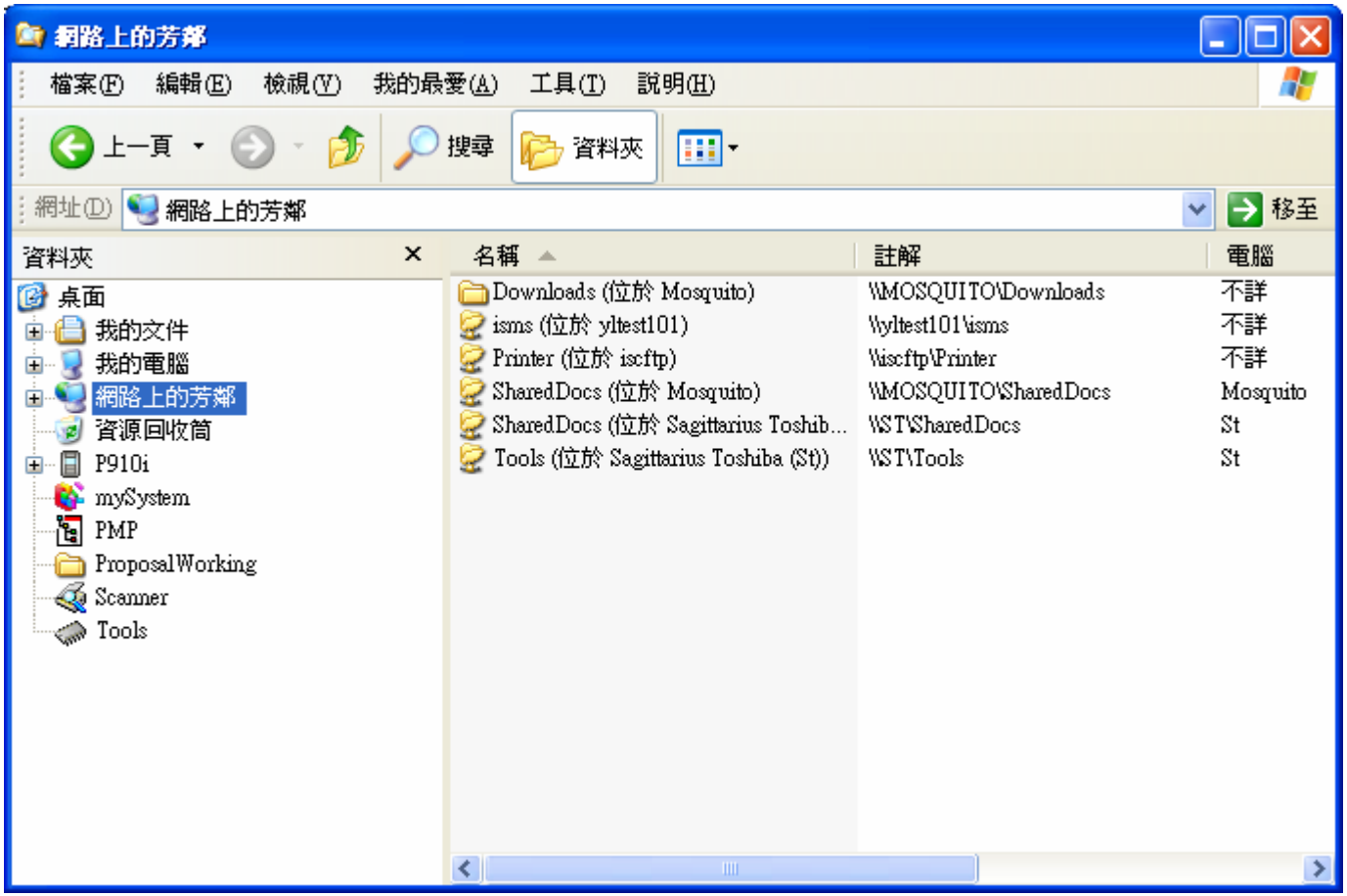
防止共用電腦時檔案被破壞



設定資料夾與檔案權限

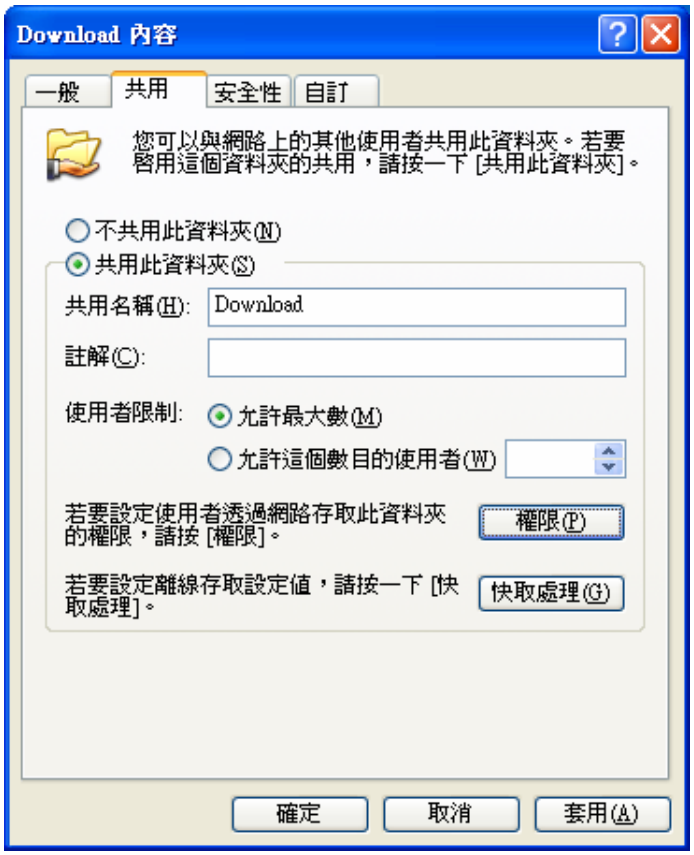


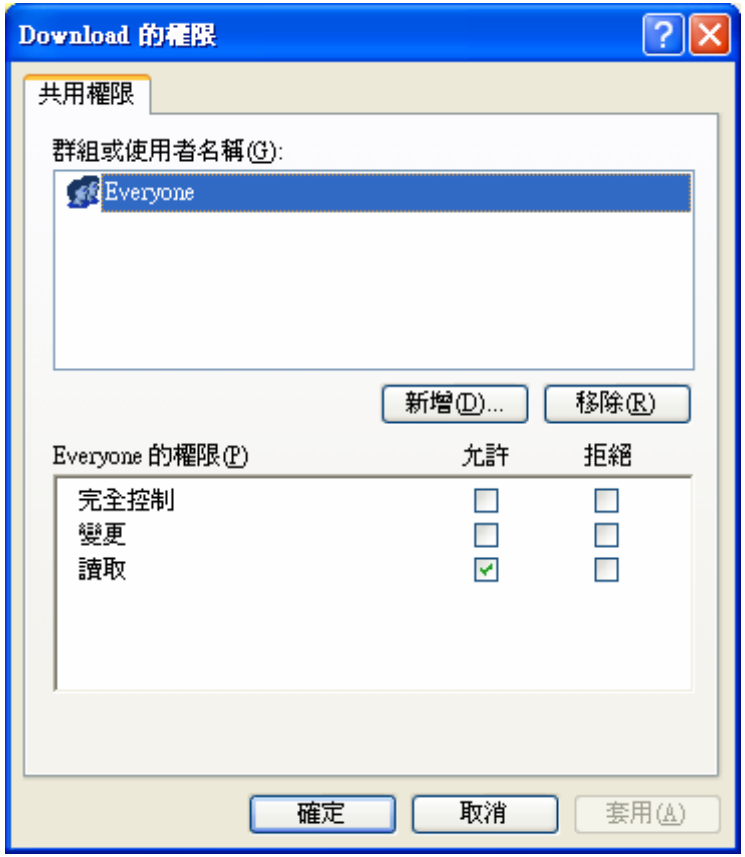
網路芳鄰與共用資料夾


網路上的芳鄰
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
資料夾
網址(D) 網路上的芳鄰
移至
資料夾
桌面
我的文件
我的電腦
網路上的芳鄰
資源回收筒
P910i
mySystem
PMP
ProposalWorking
Scanner
Tools
名稱
註解
電腦
Downloads (位於 Mosquito) \\MOSQUITO\Downloads 不詳
isms (位於 yltest101) \\yltest101\isms 不詳
Printer (位於 iscftp) \\iscftp\Printer 不詳
SharedDocs (位於 Mosquito) \\MOSQUITO\SharedDocs Mosquito
SharedDocs (位於 Sagittarius Toshib... \\ST\SharedDocs St
Tools (位於 Sagittarius Toshiba (St)) \\ST\Tools St

設定共用資料夾的使用權限

- 原則禁止，例外開放 ？
- 原則開放，例外禁止 ？





5.密碼設定要穩固

密碼遭破解之統計數據

密碼長度	26 英文字母	26 英文字母+10 數字	52大小寫英文字母	96可印出字元
4	0	0	1 分鐘	13分鐘
5	0	10分鐘	1 小時	22 小時
6	50分鐘	6 小時	2.2 天	3 個月
7	22 小時	9 天	4 個月	23 年
8	24 天	10.5個月	17 年	2287 年
9	21 個月	32.6 年	881 年	21萬9000年
10	45 年	1159 年	45838 年	2100萬年

帳號與密碼

- 密碼如果不夠複雜，很容易被破解並造成安全上的衝擊。
- 管理重要系統或機密資料的帳號，更需加強密碼的強度。
- 必須定期更換
- 停用 Guest 或 Anonymous 帳號，就是所謂來賓或匿名帳號。

密碼設定小技巧

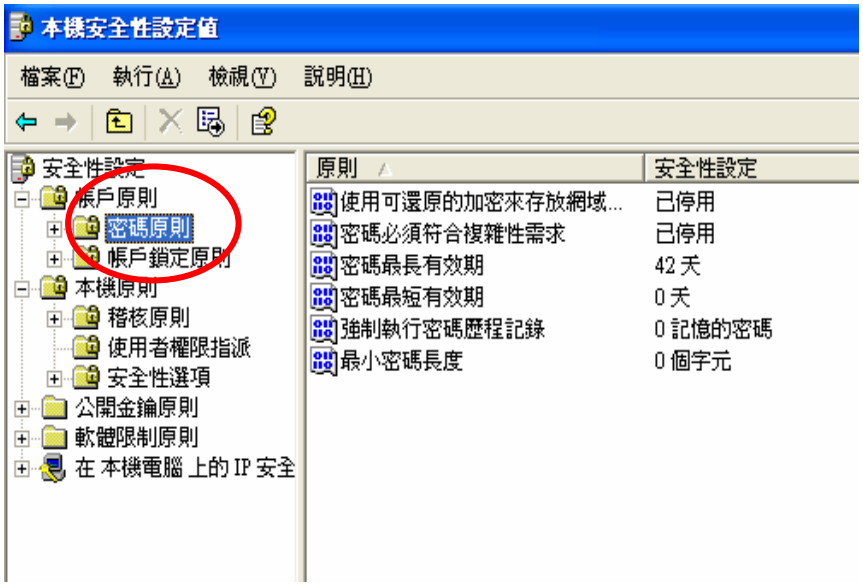
- 以中文輸入法按鍵來當成密碼
- 以英文字或數字穿插
- 以英文字或數字穿插
- 將英文字母位移數個字
- 以英文的一句諺語或一段歌詞，取每個英文字字首當成密碼。

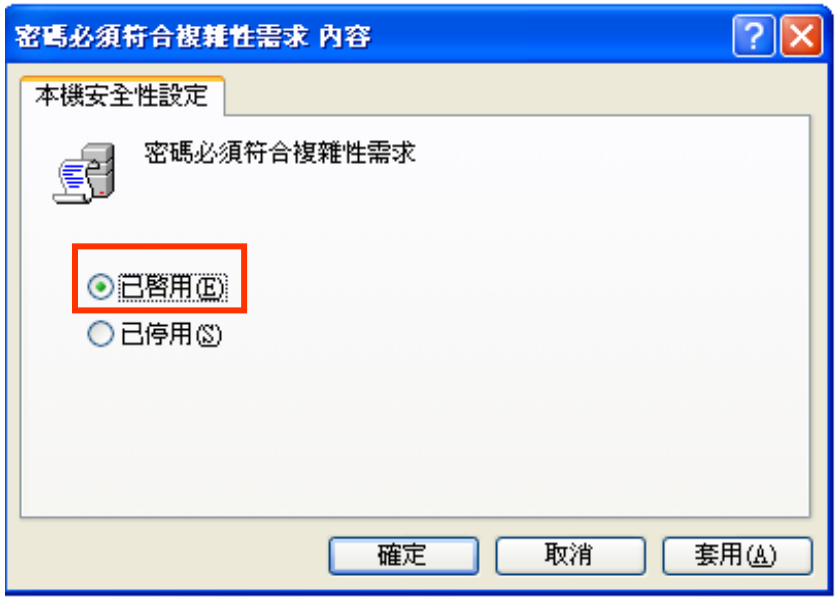
密碼設定範例

- 技巧1
  - 以中文輸入法按鍵來當成密碼，我的手機號碼(倚天輸入法)
    - Xo3 de4 /y3 ge hz4 ma3
- 技巧2
  - 以英文字或數字穿插
    - good + 5829等於 g5o8o2d9
- 技巧3
  - 將英文字母位移數個字Birthday往前位移1個字母
    - Ahqsgczx
- 技巧4
  - 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Raindrop keeps following on my head.
    - Rkfomh

密碼原則設定

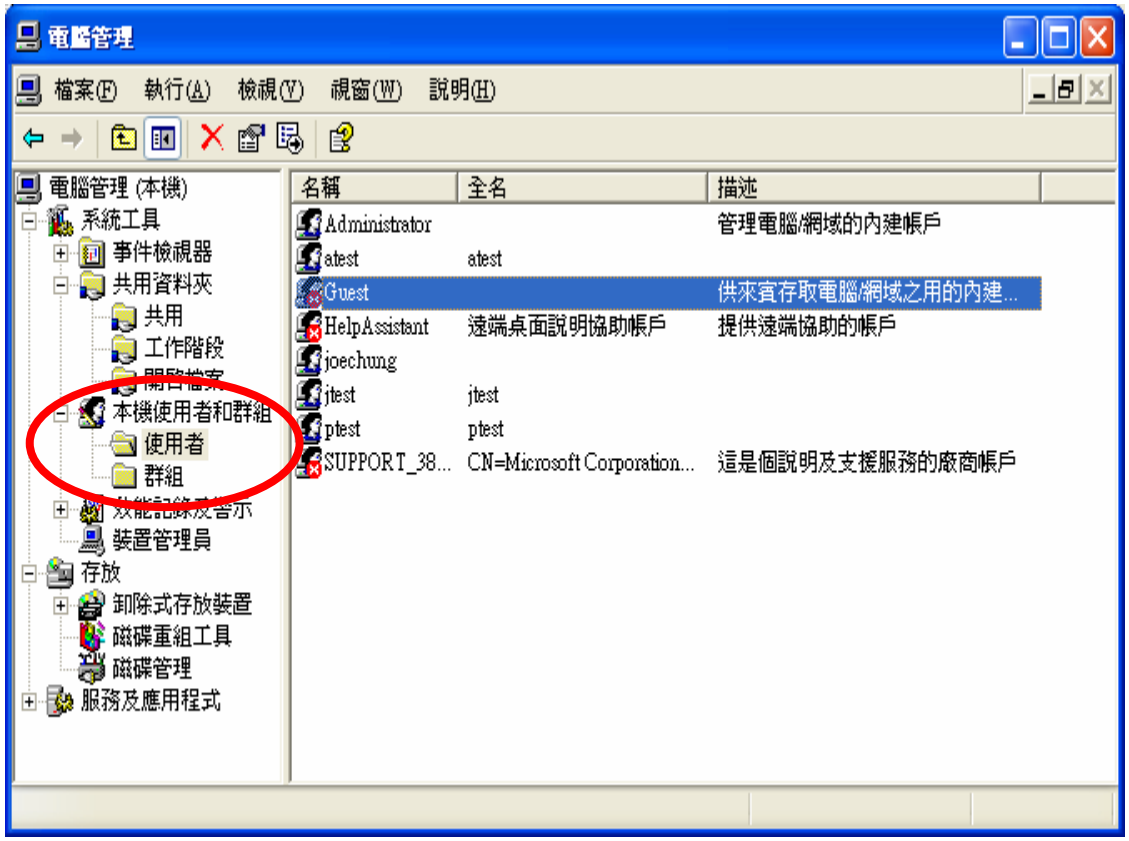
- 透過控制台進入系統管理工具
- 點選「本機安全性原則」，進入「帳戶原則」下的「密碼原則」，設定密碼最長有效期、密碼最短有效期、最小密碼長度。
- 啟用「密碼必須符合複雜性需求」

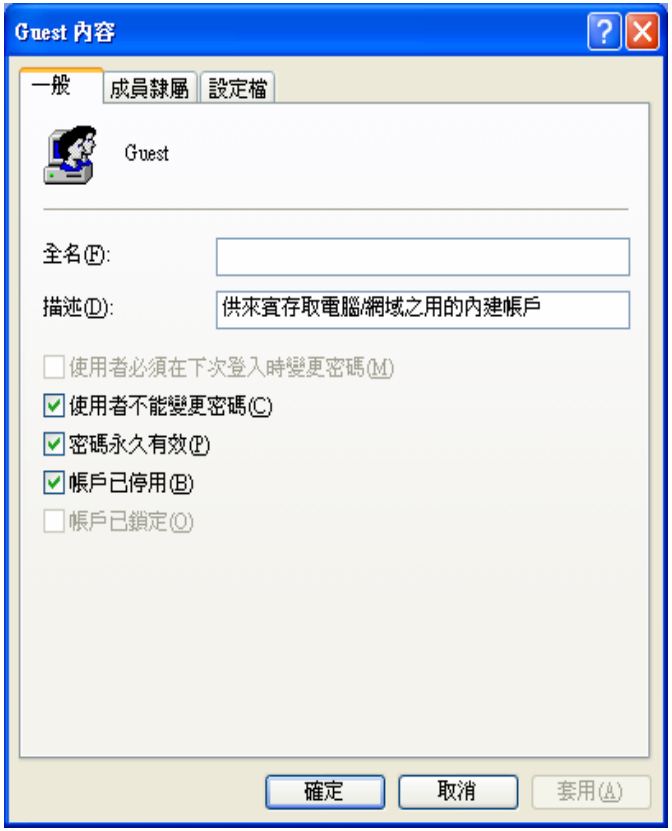




停用來賓(guest)帳號

- 控制台>系統管理工具>電腦管理





6.重要資料要備份

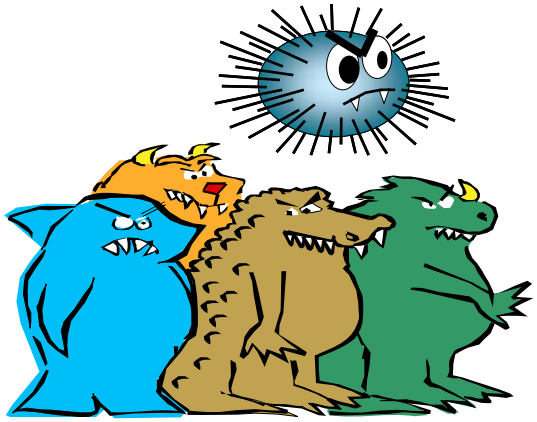
檔案備份

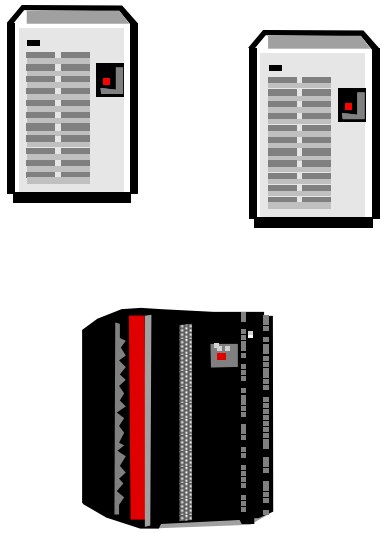
- 備份的重要性
  - 預防重要資料或設備損壞遺失
  - 確保可用性
- 可藉由不同的工具軟體達到備份的目的
  - Windows本身所提供的程式
    - 開始→附屬應用程式→系統工具→製作備份
  - 存放於儲存媒體並放置於安全場所

7.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





8.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
- 不要隨意開啟檔案
- 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
- 不斷的當機或重新啟動
- 印表機印不出來
- 畫面顯示不尋常的錯誤訊息

9.瀏覽網路要提防

預防網路釣魚

- 不法人士偽造知名網站或是利用標題聳動的電子郵件作為誘餌，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
- 可能為詐騙之郵件標題
  - 「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。」

使用網路服務需知

- 調查網站的聲譽
- 提供個人資訊時要檢查有無隱私權政策
- 進行線上交易要確定有加密措施(https)

小心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

小心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

10.電子郵件要過濾

處理電子郵件附件

- 處理電子郵件附件的五大祕訣
  - 除非您瞭解附件的來源且您知道會收到該附件，否則請勿開啟任何附件。
  - 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。
  - 使用防毒軟體並時時更新。
  - 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為病毒。
  - 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。

結論

政府機關的資訊安全除了健全的基礎設施之外，最重要的是先做好，個人的資訊安全，只要機關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，機關內部資訊安全就能得到保障，進而提升我國整體資訊安全環境。