防毒及網路安全

資工研究所
講師：林凱舜
links@cs.ccu.edu.tw

大綱

- 網路資訊安全
- 如何預防中毒
  - 如何判斷問題信件
  - 認識有問題的檔案副檔名
- 如何知道電腦中毒
- 中毒自救步驟
  - 線上免費掃毒
  - 安裝防毒軟體
  - 執行殺毒軟體

壹、網路資訊安全

「資訊安全」概念迷思

- 學校有設定防火牆，很安全？
- 我的電腦有防毒系統和防火牆，很安全？
- 網路線拔掉，我的電腦很安全？
- 不用電腦和網路，我的資訊很安全？

檢視您的電腦和網路安全

- 作業系統和防毒軟體隨時更新？(10分)
- Windows XP 防火牆已開啟？(5分)
- 網路環境已建置防火牆？(10分)
- 不使用免費、破解的軟體、遊戲和MP3？(20分)
- 不逛 XXX 或破解軟體的網站？(15分)
- 不喜歡開啟 EMAIL 中的附件？(20分)
- 電腦不常借他人使用或不借他人電腦使用？(20分)

案例

1、電子郵件帳號遭駭客竊取
2、公事家辦洩密(轉載自法務部)
3、警所私灌FOXY導致偵查筆錄外洩
4、全台近千網站被植入惡意程式
5、網路銀行資料遭竊取(轉載自刑事局)

電子郵件帳號遭駭客竊取(一)

案由：

國內大學之郵件伺服器與駭客中繼站建立連線，且特定電子郵件帳號遭登入下載郵件查看，疑似洩漏重要資訊內容。

電子郵件帳號遭駭客竊取(二)

預防方式：

(一)應注意電子郵件使用安全，勿開啟來路不明之信件，以免被植入後門程式竊取資料。

(二)郵件帳號及瀏覽器應取消記憶密碼功能，以避免帳號密碼記錄被駭客利用木馬程式竊取。

(三)個人電腦應安裝防毒軟體，且作業系統及防毒軟體應隨時更新，以避免漏洞產生。(如何更新XP系統)

(四)電子郵件及相關系統登入之密碼應定期更換。(密碼設定原則)

全台近千網站植入惡意程式(一)

案由：

據媒體報導：平均每10個網頁，就有1個植入惡意程式碼，「拒絕壞程式基金會」(http://stopbadware.org)發布「全台近千網站植入惡意程式」訊息，顯示目前網站內含惡意程式碼問題嚴重。

全台近千網站植入惡意程式(二)

預防方式：

(一)勿瀏覽非公務用途網站。

(二)個人電腦應安裝防毒軟體，作業系統及防毒軟體隨時更新。

(三)瀏覽器安全等級應設定為中級或更高等級。

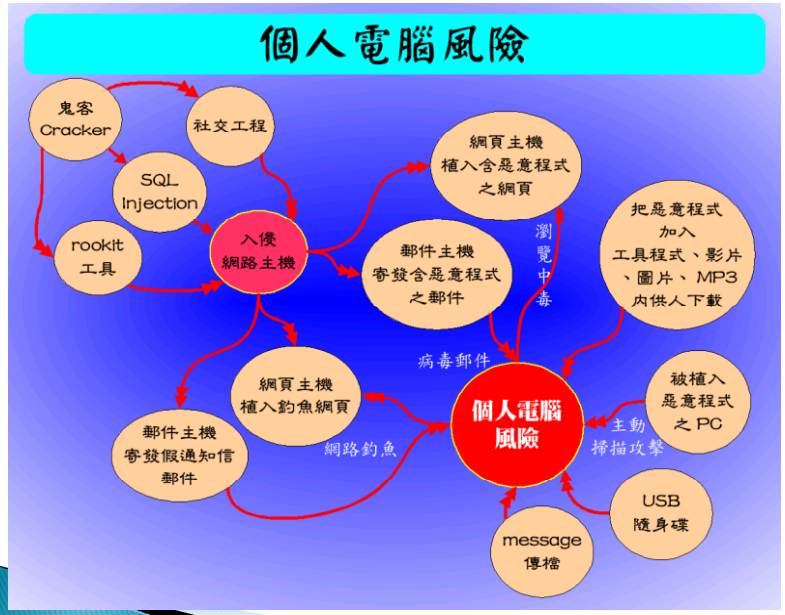
(四)勿任意下載或安裝來路不明、有違反法令疑慮（如版權、智慧財產權等）的電腦軟體。

全民資安網

- https://www.i-security.tw/index.asp
- 實作(資安健檢)

了解中毒原因

了解威脅攻擊的類別
及攻擊的途徑



攻擊類別及主要目的

- 電腦病毒
  - 破壞電腦系統
  - 感染更多電腦
- 駭客攻擊
  - 取得電腦控制權
  - 取得有用資料
  - 攻擊其他電腦
- 木馬與後門

中毒途徑

- 網路連線
  - 廣域 / 區域
- 問題網頁
  - 置入有害程式/惡意連結
  - 跳出視窗的廣告
- 電子郵件內容/附件
- P2P分享軟體
- 人為因素
  - USB隨身碟/其他儲存媒體

區域/廣域網路的入侵

- 長時間的連線讓蠕蟲或駭客有足夠時間找出個人電腦的弱點而進行攻擊。
- 作業系統的弱點被利用來進行入侵。
- 常以防火牆加以阻擋。

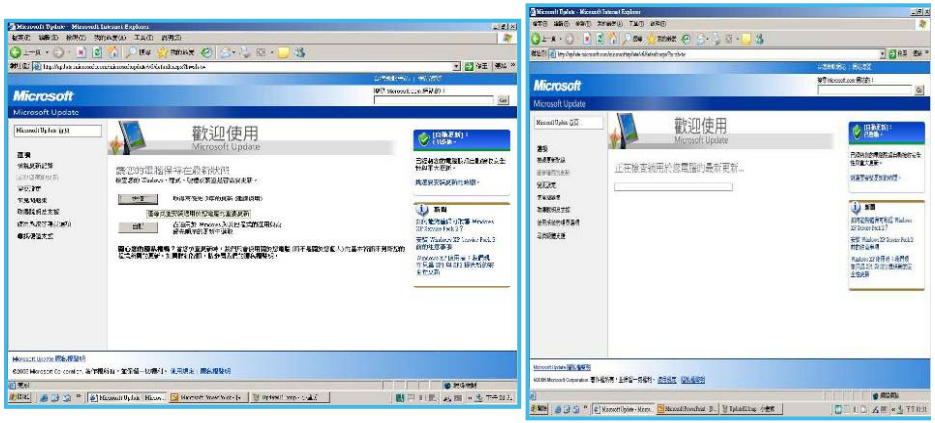
防毒

- 確保電腦受到安全防護的三個步驟
  - 開啟Windows Update 。
  - 在IE6/IE7阻擋跳出視窗。
  - 使用網際網路防火牆
- 防毒軟體安裝
- Live Update 線上更新病毒碼

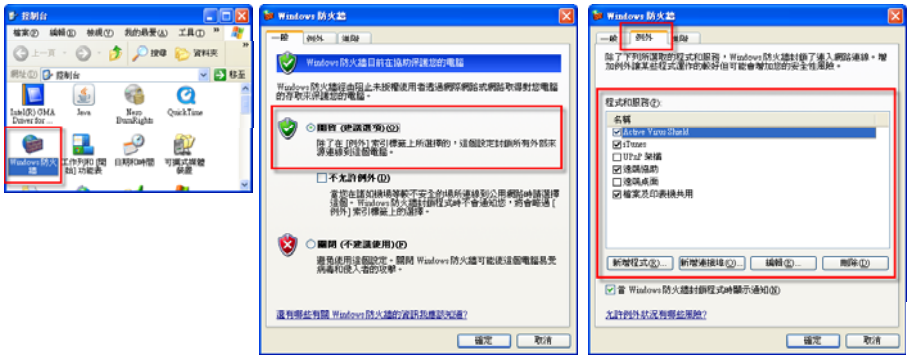
Windows Update

- 為了作業系統的最新狀態，必定要進行更新。
- 持續利用Windows Update，務必從 Microsoft Windows Update 或 Microsoft Office Update 下載 Microsoft 更新和補充程式。
- 保持您的 Microsoft 軟體在最新狀態，修補已知安全漏洞。

Update：Microsoft Update



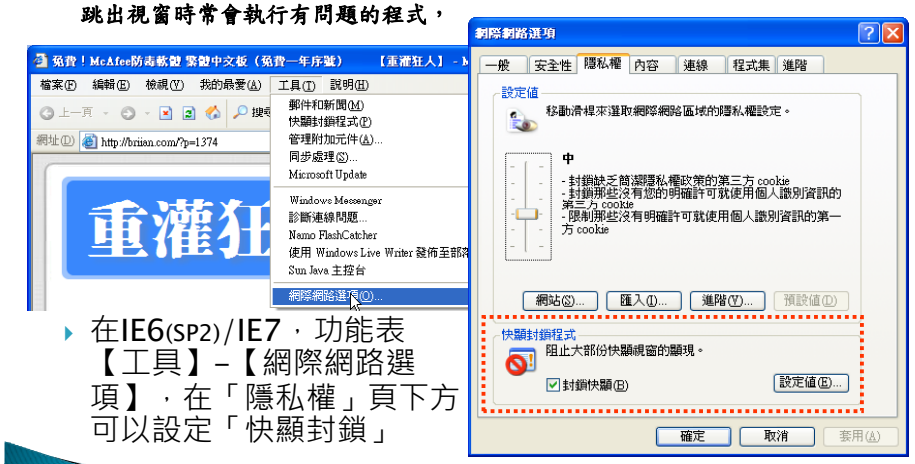
開啟網路連線防火牆



IE 設定

在IE阻擋跳出視窗

跳出視窗時常會執行有問題的程式，



- 在IE6(SP2)/IE7，功能表【工具】-【網際網路選項】，在「隱私權」頁下方可以設定「快顯封鎖」

網站的下載/惡意連結

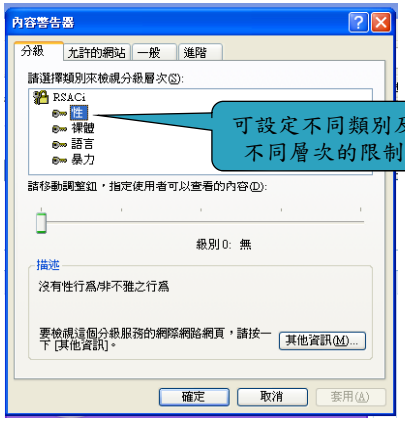
- 假冒的網頁誘使使用者開啟程式，或輸入機密資料。
- 下載的軟體 / 音樂 / 影片都可能包含病毒或木馬。絕不要從不信任的來源下載軟體。
- 在網路上使用帳號的密碼需要足夠的強度，混合數字及大小寫英文，最好再加入一些符號。免得網站及WebMAIL盜用，而傷害他人。
- 部分網頁被植入有害程式碼，可在背景安裝間諜 / 木馬程式。(常出現在跳出視窗)

釣魚網站防護

- O0 l1
- 土地銀行
- www.landbank.com.tw
- www.1ankbank.com.tw
- 台灣銀行
- http://my.bot.com.tw/
- http://www.my-bot.com/

防止誤上色情網站

- 在功能表的【工具】-【網際網路選項】，在「內容」頁中可以設定「內容警告器」



台灣網站分級推廣基金會:
http://www.ticrf.org.tw/chinese/rating-installation.htm

如何判斷問題信件

電子郵件附件

- 當您開啟電子郵件附件 (通常是按兩下附件迴紋針圖示) 時就會啟動病毒。
- 秘訣：絕不要開啟電子郵件所附加的任何內容，除非這是您預期的附件，「而且」您知道該檔案的實際內容。
  如果您收到不認識的人所傳來的電子郵件和附件，建議立即刪除。
- 不能放心開啟認識的人傳來的附件。病毒和蠕蟲有能力竊取電子郵件程式的資訊，並可以假冒任一人，將自己傳送給通訊錄所列出的每個人。因此，如果您收到的電子郵件中包含您不瞭解的訊息或不預期的檔案，請務必與對方連絡，先確認附件的內容再開啟。

收件人不是你的信件

- 常只用你的帳號的部分來稱呼你。如以上的gaia_hwang是email帳號的前半部分，所以不是你的朋友/客戶寄來的。

常見假冒的E-mail

- (✘)收件者：DEAR wang001
- (○)收件者：DEAR 王建國 先生
- (○)寄件者：wang001@yahoo.com.tw
- (✘)寄件者：wang001@Yah00.com.tw

奇怪的附件

即時通訊軟體

- 中毒的使用者會傳送有問題的附件或連結，若按下則會感染，再傳送有問題的附件或連結給你的連絡人。也可能盜取帳號資料，發出病毒郵件。

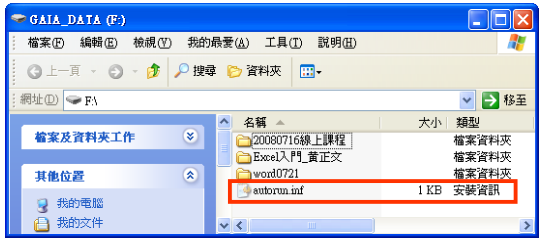
P2P軟體的下載

- 下載的軟體 / 音樂 / 影片都可能包含病毒或木馬。最好不要使用，至少要極小心檢查這些下載的檔案後，才可以使用它們。
- 假檔案

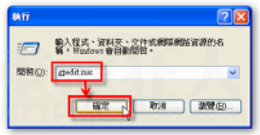
USB隨身碟–病毒偵測

- NOD32偵測到病毒的警告畫面

USB隨身碟



- 〔開始〕→【執行】，開啟「執行」對話盒後，請輸入「**gpedit.msc**」，再按一下〔確定〕按鈕，開啟群組原則設定頁面。



xwatmaf_exe(rckywlq_exe)的autorun.inf的內容

```
[AutoRun]
open=xwatmaf.exe
shell\open=湖義(&O)
shell\open\Command=xwatmaf.exe
shell\open\Default=1
shell\explore=詋埭奪燴　(&X)
shell\explore\Command=xwatmaf.exe
```

```
[AutoRun]
open=xwatmaf.exe
shell\open=打開(&O)
shell\open\Command=xwatmaf.exe
shell\open\Default=1
shell\explore=資源管理器(&X)
shell\explore\Command=xwatmaf.exe
```

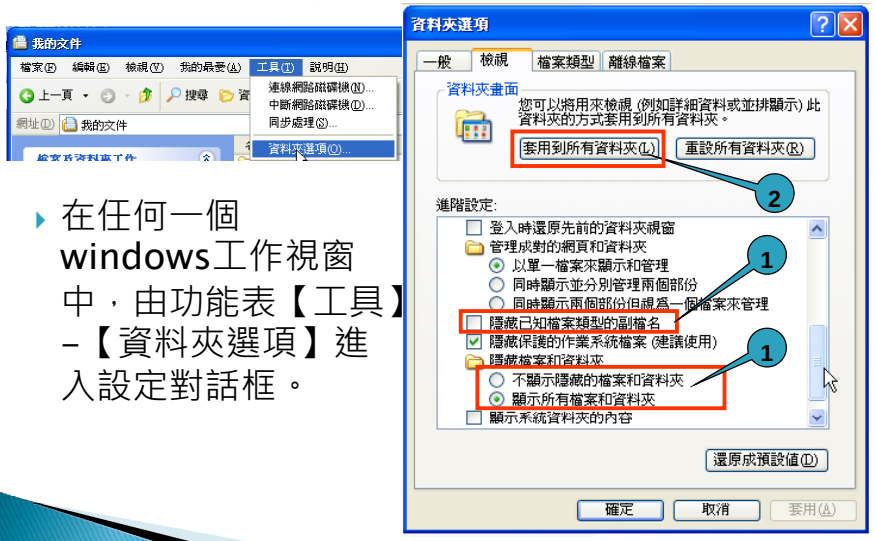
USB隨身碟

其他儲存媒體

- 從電腦磁片/外接硬碟/光碟片散佈
  - **向朋友借的，甚至在商店中購買**
  - **這些感染病毒的途徑較不常見。**

認識有問題的檔案副檔名

改變設定，顯示副檔名



- 在任何一個windows工作視窗中，由功能表【工具】-【資料夾選項】進入設定對話框。

需要注意的檔案副檔名 1

- .com
- .exe
  - 可執行的程式檔

需要注意的檔案副檔名 2

- .lnk
  - 本機的捷徑
- .url
  - 網址捷徑，常存在於“我的最愛”。
  - **Uniform Resource Locator (URL) 通用資源定址器 (URL)**：獨一無二地識別網際網路上某一個位置的位址。全球資訊網站台的 URL 開頭是 http://，例如這個虛構的 URL：http://www.example.microsoft.com/。URL 可包含許多詳細資料，例如，超文字網頁的名稱通常會以副檔名 .html 或 .htm 來識別。

需要注意的檔案副檔名 3

- .scr
  - Windows Screen Saver常用副檔名。其檔案具有可執行的程式碼。
  - 假如在電子郵件附件中收到此副檔名之檔案，可能是病毒或蠕蟲的製作，執行它會被感染而中毒。

需要注意的檔案副檔名

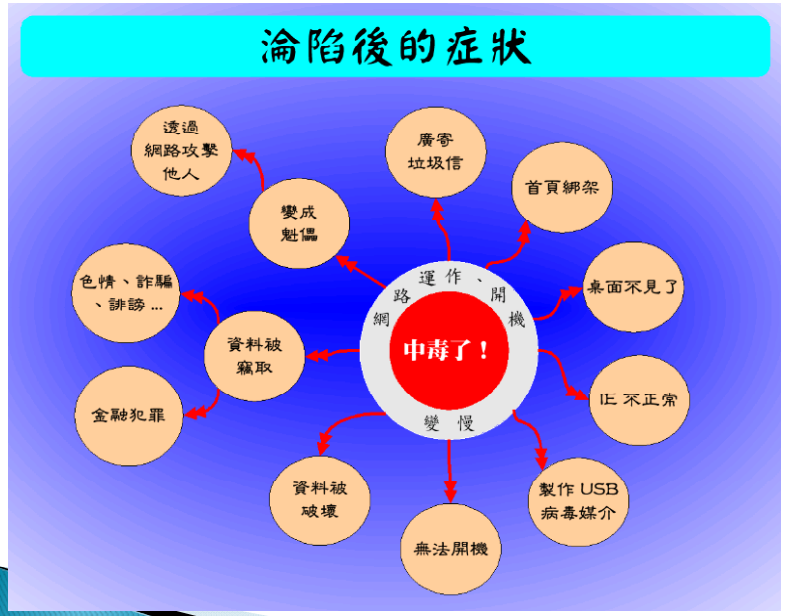
- .zip
- .RAR
- .7z
- .arj
- .lzh
  - 不同壓縮軟體製作出來的壓縮檔，必須利用解壓縮工具來解壓才可以使用。

十全十美的防毒觀念

- 不使用盜版軟體
- 不隨意使用P2P軟體
- 長時間離開座位時，記得關閉電腦
- 好奇心勿過重
- 隨時將作業系統保持在最新狀態
- 將瀏覽器安全性設高
- 電腦必安裝安全軟體–防毒、防間諜及防火牆
- 防毒軟體要時常更新
- 定期進行全系統掃描
- 養成資料備份的習慣

如何知道電腦中毒

認出徵兆，及早處理



研判電腦中毒

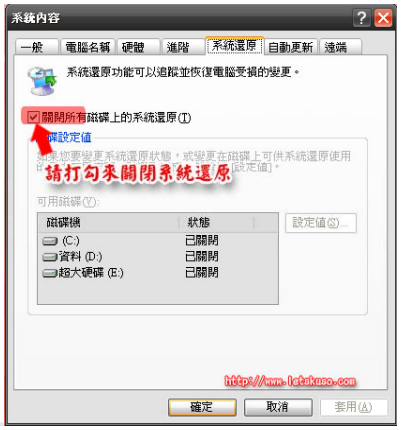
- 開啟和執行受到感染的程式時，您不一定會知道自己已感染病毒。您的電腦速度可能會變慢、當機，或者每隔幾分鐘重新啟動。
- 病毒有時會攻擊啟動電腦時需要的檔案。若是如此，您可能會發現按下電源按鈕之後整個螢幕都是空白的。
- 這些徵狀都是電腦中毒常出現的現象 — 不過也可能是與病毒完全無關的軟硬體問題所造成的。
- 除非您的電腦已安裝最新的防毒軟體，否則沒有任何方法能確定您是否感染病毒。

解毒的流程

- 【Step 1】關掉WindowsXP SP2的"系統還原"
- 【Step 2】儘可能的更新病毒碼及掃毒引擎
- 【Step 3】找出可疑的檔案並移除它
- 【Step 4】使用工具軟體完整掃描電腦
- 【Step 5】進入安全模式
- 【Step 6】重新開機

【Step 1】關掉WindowsXP SP2的"系統還原"

- 你可以從「開始功能表」中開啟「控制台」->「系統」，出現〔系統內容〕對話盒時，請切換到〔**系統還原**〕活頁標籤.
- 「**系統還原**」儲存的地方常常都是**病毒的避難所**，原因就是防毒軟體沒有辦法清系統還原資料夾(**System Volume Information**)裡的病毒，所以乾脆就把它關了吧！



【Step 2】儘可能的更新病毒碼及掃毒引擎

- 安裝防毒軟體(商用)
  - 商用防毒系統
    - 卡巴斯基、NOD 32
    - 諾頓(NORTON)、趨勢(Pc-cillin)
  - 防毒版 & 網路安全版(Internet Security)

【Step 2】儘可能的更新病毒碼及掃毒引擎

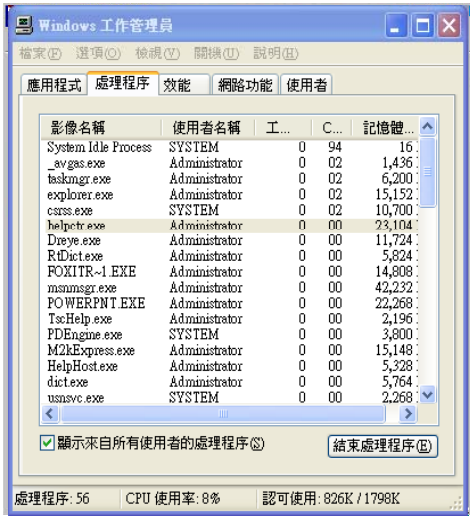
- 安裝防毒軟體(免費)
  - **Avira AntiVir PersonalEdition Classic(小紅傘)**
    http://www.free-av.com
  - **avast! 4 Home Edition(有中文版)**
    http://www.avast.com/cnt/download-avast-home.html
  - **BitDefender**
    http://www.bitdefender-asia.com

Avira AntiVir：Avira小紅傘個人免費正體中文體驗版

下載連結: http://g-ray.com.tw/download/avira_antivir_personal_tc.exe

【Step 3】找出可疑的檔案並移除它

- 一起按下「Ctrl + Alt + Delete」3個按鍵，叫出Windows工作管理員。
- 利用排序找出耗用 CPU或記憶體較多的原兇。
- 再把它的名稱去google搜尋一下，或許可以找出相關訊息。



【Step 3】找出可疑的檔案並移除它

- http://tw.trendmicro.com/tw/home/

【Step 3】找出可疑的檔案並移除它

- http://www.symantec.com/zh/tw/index.jsp

線上免費掃毒

- 卡巴斯基
http://www.kaspersky.com/virusscanner
- 賽門鐵克 諾頓
http://security.symantec.com/sscv6/default.asp?langid=ch
- 趨勢PC-cillin
http://housecall.trendmicro.com/housecall/start_corp.asp
- McAfee 邁克菲
http://us.mcafee.com/root/mfs/default.asp

【Step 4】使用工具軟體完整掃描電腦

共享軟體：

- Spyware Doctor(反間諜)
(http://www.pctools.com/spyware-doctor/)

【Step 4】使用工具軟體完整掃描電腦

- LAVASOFT Ad-Aware Free
- http://changyang319.pixnet.net/blog/post/5268105

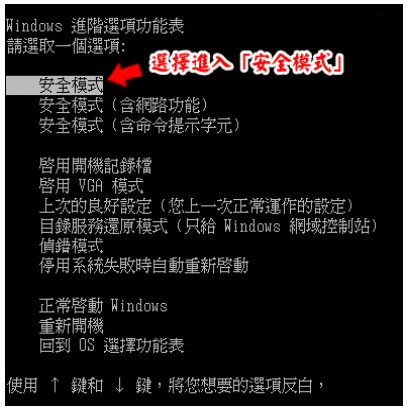
【Step 4】使用工具軟體完整掃描電腦

免費的有：

- Kavokiller (隨身碟掃毒)
http://www.webrush.net/game76420/
- USBcleaner (隨身碟掃毒)
http://big5.usbcleaner.net/download.htm

【Step 5】進入安全模式

- 進入「**安全模式**」的方法，請你在打開電腦之後，看到**WindowsXP開始的圖案之前**，一直的按「**F8**」按鍵，之後會出現一個黑底白字的畫面，這時請選擇第一個「安全模式」進入，如果你會命令提示字元，也可以選擇「安全模式(含命令提示字元)」



【Step 5】進入安全模式

- 進入安全模式後，因為系統只載入基本的開機的程序及驅動程式，所以”**有可能**”病毒就沒有被載入，所以在這個時候來進行清除病毒的動作會比較有效。接下來就請做：
- 1) 使用「檔案總管」或是「命令提示字元」找到【**Step 3.4**】因為拒絕存取或使用中而殺不掉的檔案，再試著殺殺看。
- 2) 接下來再次使用【**Step 4**】防毒軟體(Antivirus、adaware)再試著清看看。

【Step 7】重新開機

- 重新開機後，請再回到【Step 3】，再次檢查所移除的程式有沒有復發的現象。
- *(如果你發現已經殺掉的木馬會一再的復發，就要請找更專業的人士解決，或是重灌了。如果你還想再繼續解的話，你可以上網去搜尋這個木馬的相關資料，再想對策來解決)*

結論

- 資安科技不斷演進
- 攻擊技術也隨之更新
- 隨時了解新技術
- 選擇適合自己企業的解決方案
- 持續的吸收新知及接受教育訓練