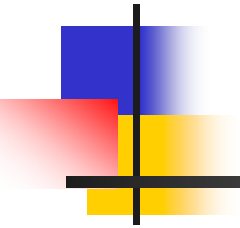
Hi克任務

南台企管阿基師

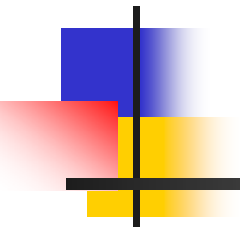
12

13

14



A 13 C



12

A 13 C

14

課程大綱

針對您常會中毒的發生的原因予以探討：

1.如何知道電腦中毒

2.了解中毒原因

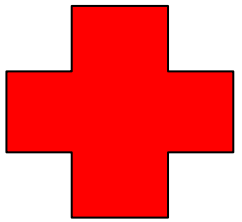
3.認識有問題的檔案副檔名

4.如何判斷問題信件

5.如何保護電腦資料

6.如何預防中毒

1. 如何知道電腦中毒
2. 了解中毒原因
3. 認識有問題的檔案副檔名
4. 如何判斷問題信件
5. 如何保護電腦資料
6. 如何預防中毒



認出徵兆，及早處理…

研判中毒狀況

- 認知：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。
- 狀態：
  1.電腦變慢、當機或每隔幾分鐘重新啟動。
  2.病毒有時會攻擊啟動電腦時需要的檔案
  3.按下電源按鈕之後整個螢幕都是空白
- 其他：可能是與病毒完全無關的軟硬體問題所造成
- 含有病毒之電子郵件訊息，病毒有偽造郵件地址能力
- 除非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。

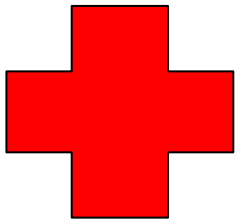
找出有問題的處理程序

- 「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。

防毒軟體介紹

ESET NOD32	http://www.nod32tw.com/
卡巴斯基	http://www.kaspersky.com.tw
F-Secure	http://support.f-secure.com/
趨勢PC-cillin	http://www.trendmicro.com.tw
賽門鐵克 諾頓	http://www.symantec.com/
PANDA	http://www.pandasoftware.com.tw/
McAfee 邁克菲	http://www.mcafee.com/tw/
其他：Virus Chaser、天網安全、江民、瑞星、金山毒霸.	

1. 如何知道電腦中毒
2. 了解中毒原因
3. 認識有問題的檔案副檔名
4. 如何判斷問題信件
5. 如何保護電腦資料
6. 如何預防中毒



威脅攻擊的類別與攻擊的途徑

攻擊類別及主要目的

- 電腦病毒-破壞電腦系統(**Windows...**)
  -感染更多電腦(**webmail...**)

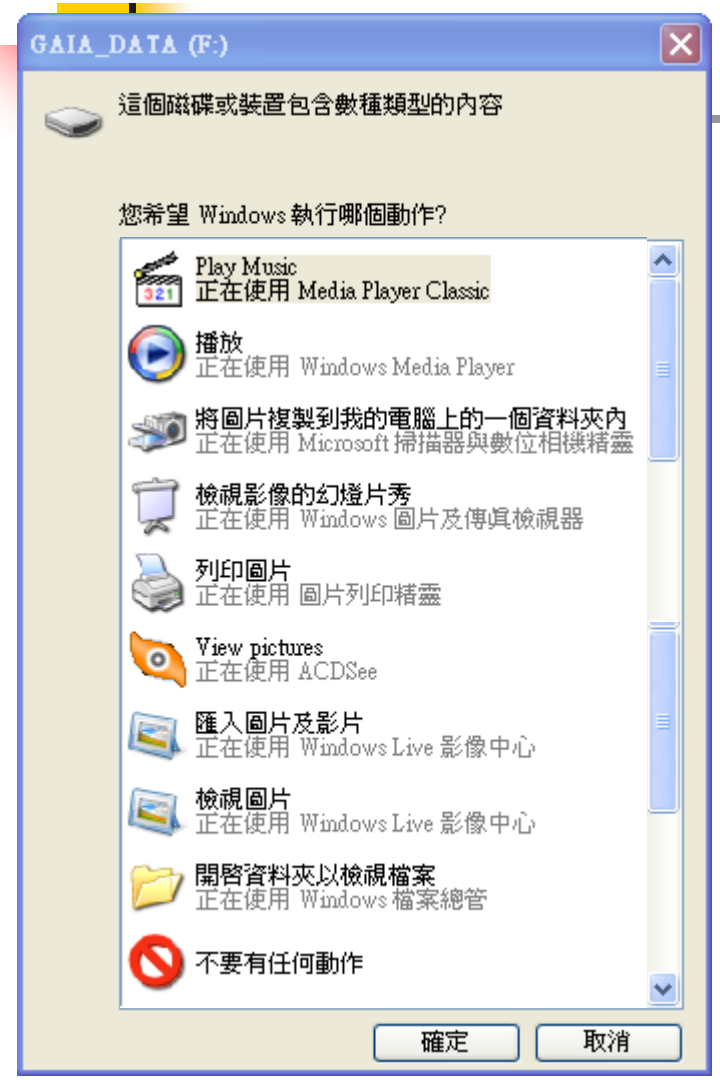
- 駭客攻擊-取得電腦控制權(**user**)
  -取得有用資料(**data**)
  -攻擊其他電腦(**hacker**)

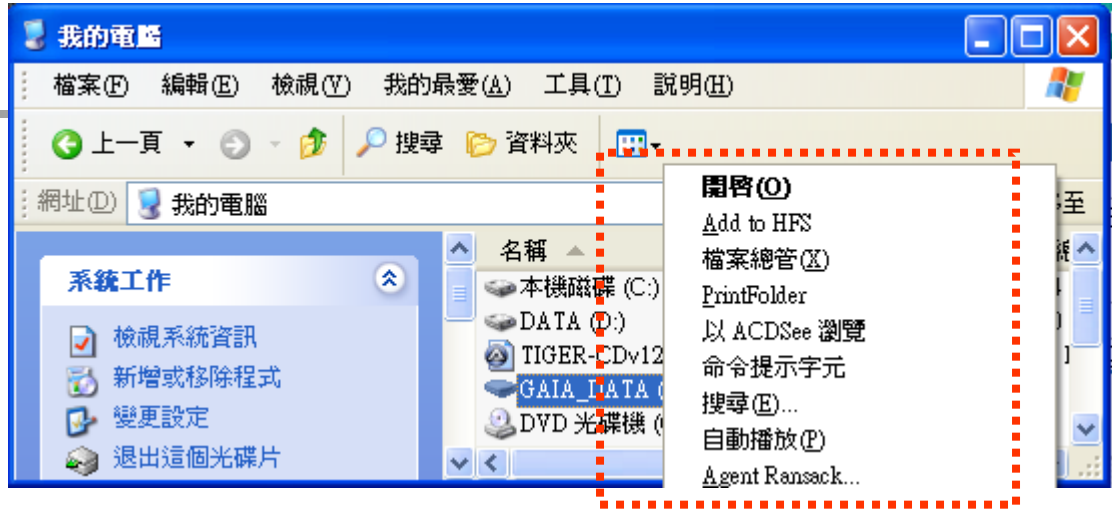
- 木馬與後門-取得特定資料(**Top Secret**)
  -取得電腦控制權(**control**)
  -攻擊其他電腦(**attack**)

中毒途徑

- 網路連線
- Mail內容/附件
- 問題網頁(情色、賭博、破解、駭客)
  - 置入有害程式/惡意連結
  - 跳出視窗的廣告
- P2P分享軟體
- 人為因素
  - USB隨身碟/其他儲存媒體

USB隨身碟、外接HD

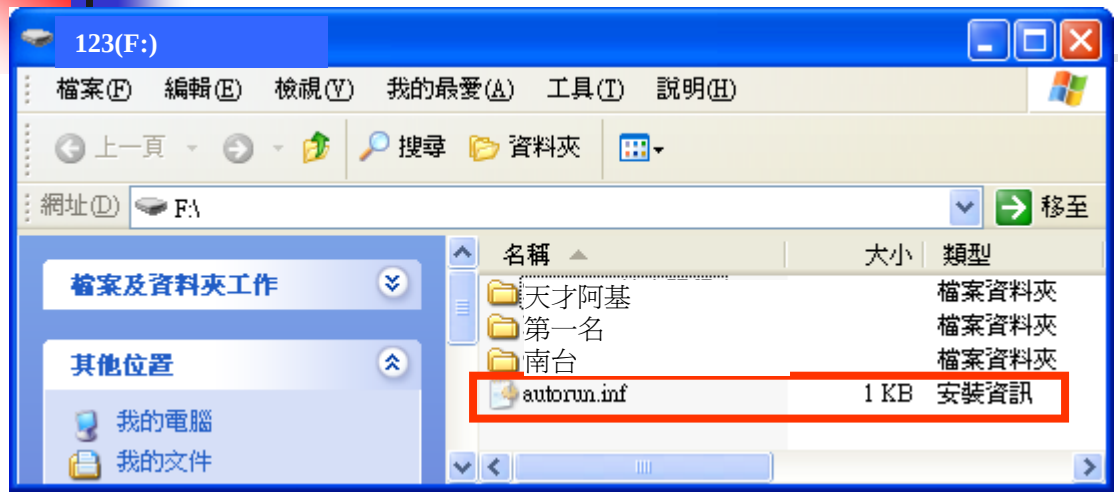




USB隨身碟正常開啟的畫面，

- 上圖：按滑鼠右鍵之快捷選單。若出現不該出現的選項時，例如英文/簡體中文的選項。
- 右圖：自動執行時出現不該出現的選項時，或不能略過時。

USB隨身碟、外接HD



xwatmaf_exe(rckywlq_exe)的autorun.inf的內容

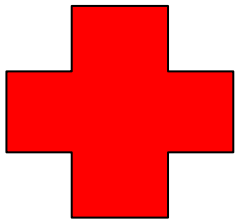
```
[AutoRun]
open=xwatmaf.exe
shell\open=湖羲(&O)
shell\open\Command=xwatmaf.exe
shell\open\Default=1
shell\explore=訛埭奪燴ㄖ(&X)
shell\explore\Command=xwatmaf.exe
```

```
[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
```

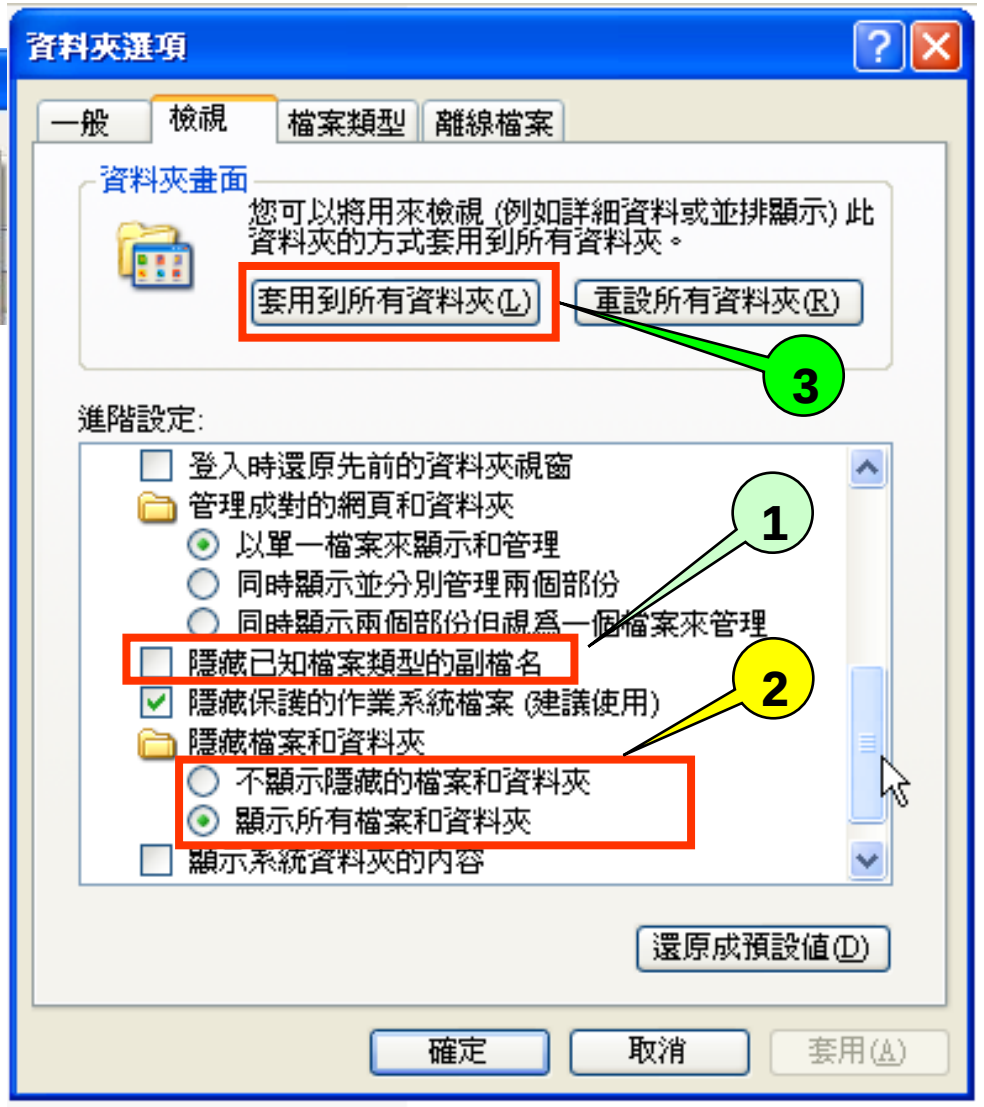
USB隨身碟-病毒偵測

以NOD32偵測病毒警告畫面

1. 如何知道電腦中毒
2. 了解中毒原因
3. **認識有問題的檔案副檔名**
4. 如何判斷問題信件
5. 如何保護電腦資料
6. 如何預防中毒



改變設定，顯示副檔名

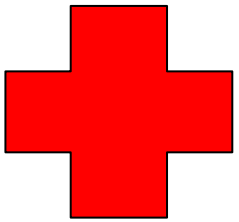


在任何一個windows工作視窗，由功能表->工具->資料夾選項->進入設定對話框。

需要注意的檔案副檔名

- .com：假檔
- .exe：可執行的程式檔
- .lnk：本機的捷徑
- .url：網址捷徑，常存在於“我的最愛”
- .pif：program information file (PIF) 程式資訊檔案
- .scr：檔案具有可執行的程式碼，病毒或蠕蟲
- .scf：可被SHELL32.DLL執行的檔案。
- 其他：.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。

1. 如何知道電腦中毒
2. 了解中毒原因
3. 認識有問題的檔案副檔名
4. **如何判斷問題信件**
5. 如何保護電腦資料
6. 如何預防中毒



顯示：所有信件 | 連絡人 | 好友 | 未讀取 | 已標示　　　　第 1-25 封郵件（共 120 封）　第一頁 | 上一頁 | 下一

刪除　標示 ▾　移至... ▾

寄件者	主旨	日期
▄▄給我低利其餘免談▄▄Leopoldo	★★專辦 現金卡,信用卡,房貸,信貸,代償,整合負債.....★★dolphin	38/1/19 (二)
▄▄給我低利其餘免談▄▄Leopoldo	★★專辦 現金卡,信用卡,房貸,信貸,代償,整合負債.....★★dolphin	38/1/19 (二)
■貸了還可再貸 ■■	不用事先繳交任何費用，額度利率讓您滿意	38/1/19 (二)
▲▲數位行銷▲▲Denny	★★每個人都有他開發的方式★★from	38/1/19 (二)
桂綸鎂`被拖去夜店廁所狂 幹	帶傳播小姐開房間.邊看A片邊做愛	38/1/19 (二)
★全球PMP薪資待遇調查▄▄Winest-w...	擁有PMP專案管理師-創造每人年薪11萬8元美金高薪	38/1/19 (二)
▄▄給我低利其餘免談▄▄Kendrick	██專辦土地房屋二胎及汽車貸款等,可貸額度保證全省最高██defined by	38/1/19 (二)
Stanley Keene	《最佳人氣王》噴水娃兒 VS 黑色會美眉 趕快來支持她們	38/1/19 (二)
▲銀行聯合貸款中心▲Billy	••債務救星.房貸.車貸.整合負債.通通幫你貸••from	38/1/19 (二)
成人網客服中心	2009年末最新成人光碟上架通知	38/1/19 (二)
★汽車貸款★Lyle	◆◆聯合貸款中心\專業銀行貸款\線上申貸\手續簡便\信貸,代償,整合負債,房貸,學...	38/1/19 (二)
發很大	大圖輸出最新指標（1200dpi)優惠實施中–	38/1/19 (二)
★考友社98公務人員招考▄▄Dick3636391	年滿十八歲，性別不拘 ‧不限學歷皆可報考	38/1/19 (二)
線上影片播放中心	線上隨點隨看不用等片子	38/1/19 (二)
██知名瘦身中心██Frankie	☆★☆你是認真想減重又擔心復胖的人嗎?☆★☆%WORD_2	38/1/19 (二)
★世界MBA名校評比中心__Paultsungju	全美前五大公立大學MBA，取得黃金權威碩士學位	38/1/19 (二)
中醫師-國際認證研習__shoulan0720	中醫特考將廢止！有心取得中醫師的您，該何去何從？	38/1/19 (二)

有問題的信件

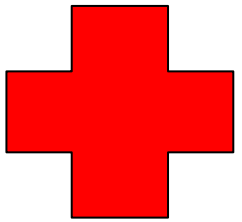
常見假冒的E-mail

- (✗)收件者：DEAR Chang厂01
- (○)收件者：DEAR 張 先生
- (○)寄件者：chang 001@yahoo.com.tw
- (✗)寄件者：chang 001@Yah00.com.tw
- (✗)寄件者：chang 001@hibank.com
- (○)寄件者：service@pchome.com.tw
- (○)寄件者：service@hellobank.com.tw

奇怪的附件


[virus Win32/Pacex.Gen virus] 看看吧~~我國中時寫ㄉ作文
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄
寄件者:
日期: 2008年7月9日 上午 03:49
收件者: zoeho84@yahoop.com.tw
主旨: [virus Win32/Pacex.Gen virus] 看看吧~~我國中時寫ㄉ作文
附加檔案: 小時候ㄉ作文國中時.zip (231 KB)
看看吧~~我國中時寫ㄉ作文 天啊~~看我小ㄉ時候多糗`^ - ^
總會在某些時刻，突然想起舊情人？他 現在過得還好嗎？- 馬上搜尋！

1. 如何知道電腦中毒
2. 了解中毒原因
3. 認識有問題的檔案副檔名
4. 如何判斷問題信件
5. **如何保護電腦資料**
6. 如何預防中毒



利用密碼保護，時時備份資料

資訊安全風險管理

- 不明人士要盤查=防止非法破壞
- 社交工程要小心=駭客就你身邊
- 電腦不用要登出=防止非法存取
- 機密資料要保護=離開就要登出
- 密碼設定要穩固=定期要更換
- 重要資料要備份=異地備份
- 應用系統要更新=補強系統的漏洞
- 電腦防毒要更新=木馬/駭客/後門程式
- 瀏覽網路要提防=預防網路釣魚cookie
- 電子郵件要過濾=處理電子郵件附件

設定密碼之概念

數字(0~9)

4位＝10^4

5位＝10^5

6位＝10^6

英文字母(大、小寫)

4位 =>$(26X2)^4=7.83X10^6$

5位 =>$(26X2)^5=3.80x10^8$

6位 =>$(26X2)^6=1.98x10^{10}$

符號(鍵盤上符號) 至少15種以上

使用3個符號，組合有$15^3=3.38X10^3$

使用4個符號，組合有$15^4=5.06X10^4$

使用5個符號，組合有$15^5=7.59X10^5$

三種以上組合的變化、足夠位數及經常更改

可使密碼較難被猜出，因為沒有足夠的時間來嘗試

設定密碼之計算方法

- 位置記憶法=利用鍵盤上的位置來記憶
  - ex:1q2w3e4r5t9i8u7y6t
  - ex:rtyuijnbg1002

設定密碼之計算方法

- 以SHIFT鍵任意改變英文大小寫及數字/符號，把常用文字/數字造成很大變化。
- 例：0938152375
  - 每隔1位數字加按SHIFT鍵
    變成 0(3*1%2#7%
  - 每隔2位數字加按SHIFT鍵
    變成 09#81%23&5
  - 不規則的加按SHIFT鍵，很難猜吧！

自然人憑證=網路上的身分證

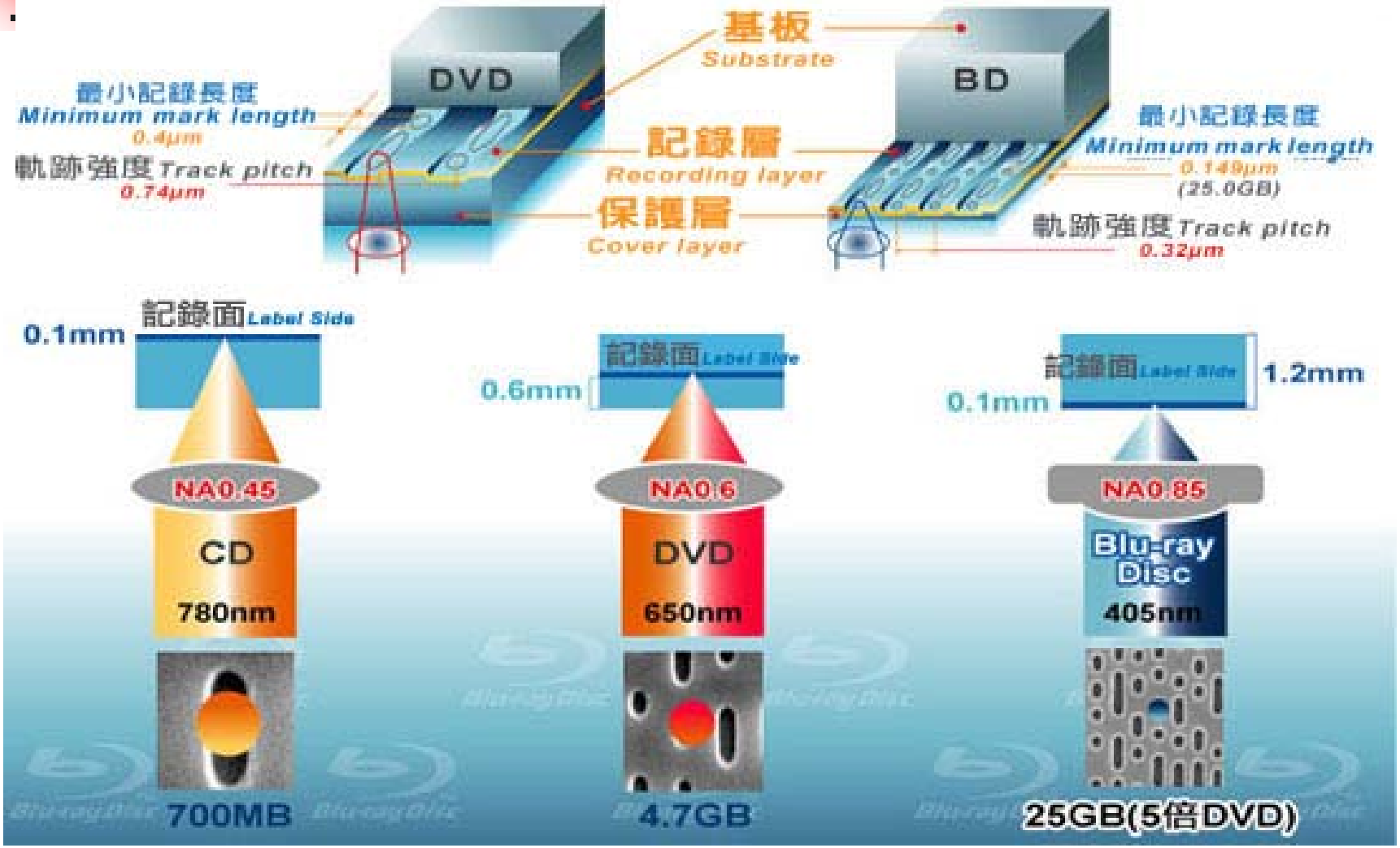
- 就是一種「電子簽章」。這種電子簽章會經由IC晶片卡自己演算並加密一組密碼，並儲存在IC晶片卡中。
- 以後就用這張IC卡來確認身分，在網路上無法假冒，就算遭駭客攔截了也沒用，資料都被密碼鎖住了，根本就解不開。(除非有這張卡)
- 目前金融卡也是IC晶片卡，更加安全。網路ATM操作，加上抽取IC晶片卡的動作要求，沒有此卡就不能操作。

資料備份

- 除了病毒/木馬/駭宮的攻擊之外，硬體也可能會損壞，定期備份是電腦使用者的基本工作。
- 沒有任何儲存媒體是永遠不會損壞。
  - 外接HD – 容量變化大
  - 光碟片–CD-R/RW / DVD±R/±RW / 藍光DVD
  - 備份伺服器/磁帶

藍光技術原理

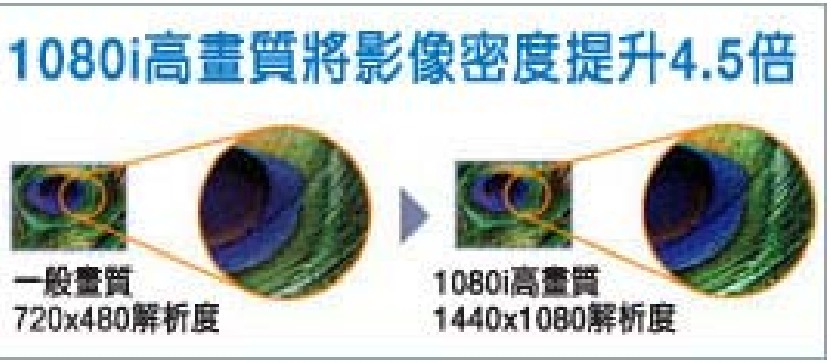
CD DVD BD記錄原理比較



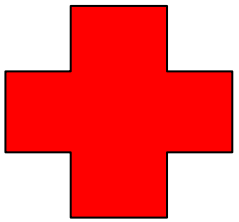
藍光技術規格比較

	可記錄容量	
CD	700MB	CD的7倍容量
DVD	4.7GB	DVD 的5倍容量
BD	25GB	

	DVD	BD
視訊編碼	MPEG-2	MPEG-2 MPEG-4 AVC / H.264 VC1
最高解析度	720*480(4:3)	1920*1080(16:9)
影像傳輸速度	9.8 Mbps(SD)	40 Mbps(HD) 15 Mbps(SD)
音訊編碼	LPCM Dolby Digital DTS	LPCM, Dolby Digital, DTS DTS0-HD, Dolby Digital Plus Dolby True HD



1. 如何知道電腦中毒
2. 了解中毒原因
3. 認識有問題的檔案副檔名
4. 如何判斷問題信件
5. 如何保護電腦資料
6. 如何預防中毒



盡可能達成的防毒觀念

- 減少使用盜版軟體
- 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
- 提高瀏覽器安全性設定
- 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

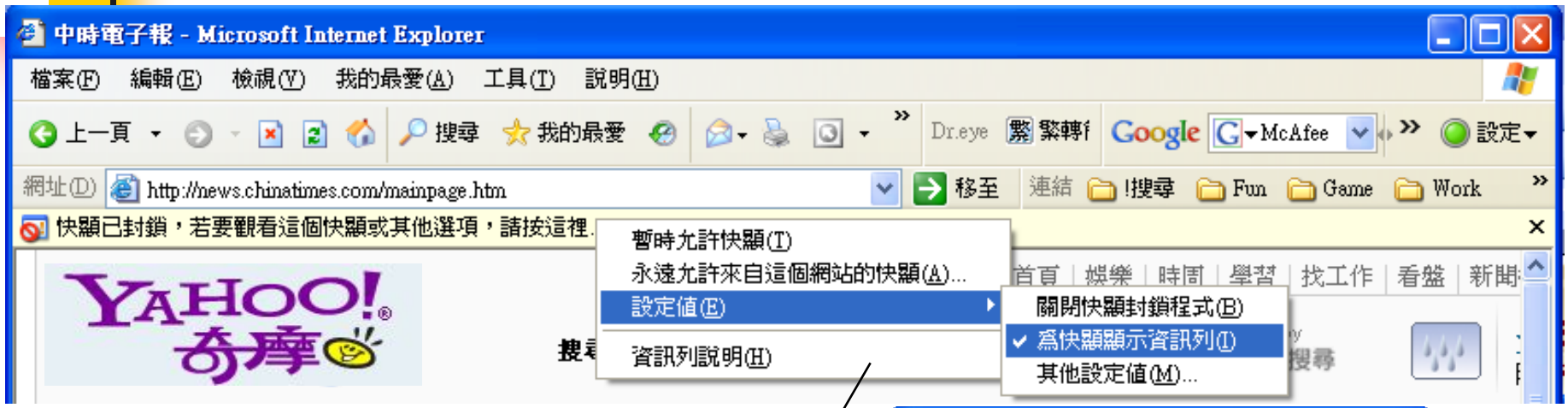
Windows Update

- 為了作業系統的最新狀態，必要時再更新
- 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。

在IE6/IE7阻擋跳出視窗

- 在IE功能表->工具
  ->網際網路選項
  ->「隱私權」下方設定
  ->「快顯封鎖」

注意快顯功能



在開啟「快顯封鎖」功能後，遇到有跳出視窗的網頁會出現-資訊列，在「資訊列」上按滑鼠鍵(左右皆可)會出現選單也可由此進行相關設定

- 另外，按「設定值」可以進行「例外網站」等設定

線上掃毒、掃木馬服務(免費)

- 卡巴斯基 http://www.kaspersky.com/virusscanner
- F-Secure http://support.f-secure.com/enu/home/ols.shtml
- 趨勢PC-cillin http://housecall.trendmicro.com/housecall/start_corp.asp
- PANDA http://www.pandasoftware.com.tw/freescan/activescan.htm

結論

- 資訊安全科技不斷演進
- 網路攻擊技術也隨之更新
- 網路使用者應隨時了解新技術
- 選擇企業適合的解決方案
- 持續的吸收新知並接受教育訓練

- 感謝大家的聆聽..

eachi1001@mail.stut.edu.tw