國立嘉義高工
資訊安全教育宣導研習

教務處 & 網管中心

行政院國家資通安全會報
資通安全責任分級

作業名稱 等級	防護縱深	ISMS推動	稽核方式	資安教育訓練 (一般主管、資訊人員、資安人員、一般使用者)	專業證照	檢測機關網站安全弱點
A級	NSOC直接防護/SOC自建或委外、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少2次內稽	1. 每年至少(3、6、18、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定	維持至少2張資安專業證照	每年2次
B級	SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少1次內稽	1. 每年至少(3、6、16、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定	維持至少1張資安專業證照	每年1次
C級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少(2、6、12、3小時)	資安專業訓練	每年1次
D級	防火牆、防毒、郵件過濾裝置	推動ISMS觀念宣導	自我檢視	每年至少 (1、4、8、2小時)	資安專業訓練	每年1次

校園或個人常見的資訊安全事件

- 網路詐騙
- 個資外洩
- 電腦中毒
- 誤上釣魚或惡意網站
- 違反智慧財產權或著作權法

網路詐騙

- 101年度資安動畫金像獎
  第二名：賈資安偵探事務所

Line 網路詐騙


沈小小成
2013/11/07 THU
這是那晚你沒來的照片，我被整慘了
https://photovip.is-found.org/img....
PM 3:10
林O民這是上次聚會的照片，你好好笑哦
https://appvip.istmein.de/img....
PM 3:10
周O恩這是我哥的新女友，是你同學嗎?
https://www.giaynham.com.vn/ad/photo....
PM 3:10
免費通話
視訊通話

Line
網路詐騙(二)

- **LINE詐騙新招 下載頭像改同名**

網路詐騙


LINE 防詐騙6撇步…
已讀1… 可開啟「隱私設定」中「阻擋訊息」的功能
已讀2… 取消「我的帳號」中「允許自其他裝置登入」，避免駭客取得的帳密後從電腦登入
已讀3… 非LINE好友傳訊息時，注意是否有不明連結，該訊息上方有「您尚未將本用戶加入好友名單內」警告，判斷是否為名單內好友
已讀4… 不要點開訊息中的短網址連結，如（goo.gl、bit.ly等）或IP連結，可先向發訊息朋友查證
已讀5… 未使用電信公司提供小額付款功能，可向電信公司取消服務。
已讀6… 詐騙集團常透過民眾好奇心詐騙，如遇詐騙情形，可撥打165求證
LINE
中央社製圖

更多參考網站

網路詐騙

- 參考資料

- 臉書
- 以目前主要的詐騙手法都是要竊取個資帳號密碼
  更絕的是拿著你的帳號密碼四處招搖撞騙，這些手法不可不防！

網路詐騙

參考資料

臉書八大可疑帳號

特性	可疑指數
一、你不認識對方	★★★
二、對方的帳號通常都是新申請的	★★★★★
三、對方的帳號中完全沒有貼文(全新的新帳號)	★★★★★
四、利用一些美女圖片當頭像	★★★★
五、來自其他國家	★★★
六、看不到對方塗鴉牆上的任何資料	★★★
七、對方的帳號中看不到任何其他照片或生活照	★★★
八、大部分沒有共通好友(因為剛開始騙)，但騙久了之後應該會有你的朋友罹難，屆時就會有共通好友了(這同時表示你的朋友已加入詐騙人物為好友)	★★★★

網路詐騙

- 警政署 防制網路詐騙影片

個資外洩

- 學校擁有大量的學生資料，各處室都有機會接觸到不同的程度的個資，在做資料交換或傳送時，應特別注意下列幾點:
  - 與委外廠商簽保密協定
  - 查證並詢問索取資料者之目的
  - 不相關的資訊不要給
  - 大量檔案壓縮加密再傳送
    (Word也有加密的功能:儲存→工具→一般選項)

個資外洩

- 案例:
  - **個資法首宗判例**
  - **基測個資 博暐涉賣給補習班**
  - 師生個資外洩 百度查得到
  - 委託廠商製作學生證，上傳資料至公共空間

- 法律責任:
  - 民事賠償:每人500元至20,000 元，單一事實最高2億

個資外洩

- **手機5大徵兆 資安恐陷危機**
  - 電池壽命變短
  - 通話經常不尋常中斷
  - 電信費用異常
  - 行動裝置效能變差
  - 自動下載軟體

電腦中毒

- 徵狀:
  - **電腦、網路變慢了**
  - 經常無故發生當機
  - **硬碟指示燈經常閃爍不停**
  - **磁碟、程式打不開**
  - **你的朋友常收到你的怪E-mail內容**
  - **IE、網頁不聽話**
  - **連上網路的時候，突然跳出各種視窗，或是瀏覽器突然出現從沒看過的網頁。**

參考網站

電腦中毒

- 傳播途徑:
  - **隨身碟**
  - 惡意網頁
  - **電子郵件夾帶檔案**
  - **安裝不明、免費的軟體**

電腦中毒

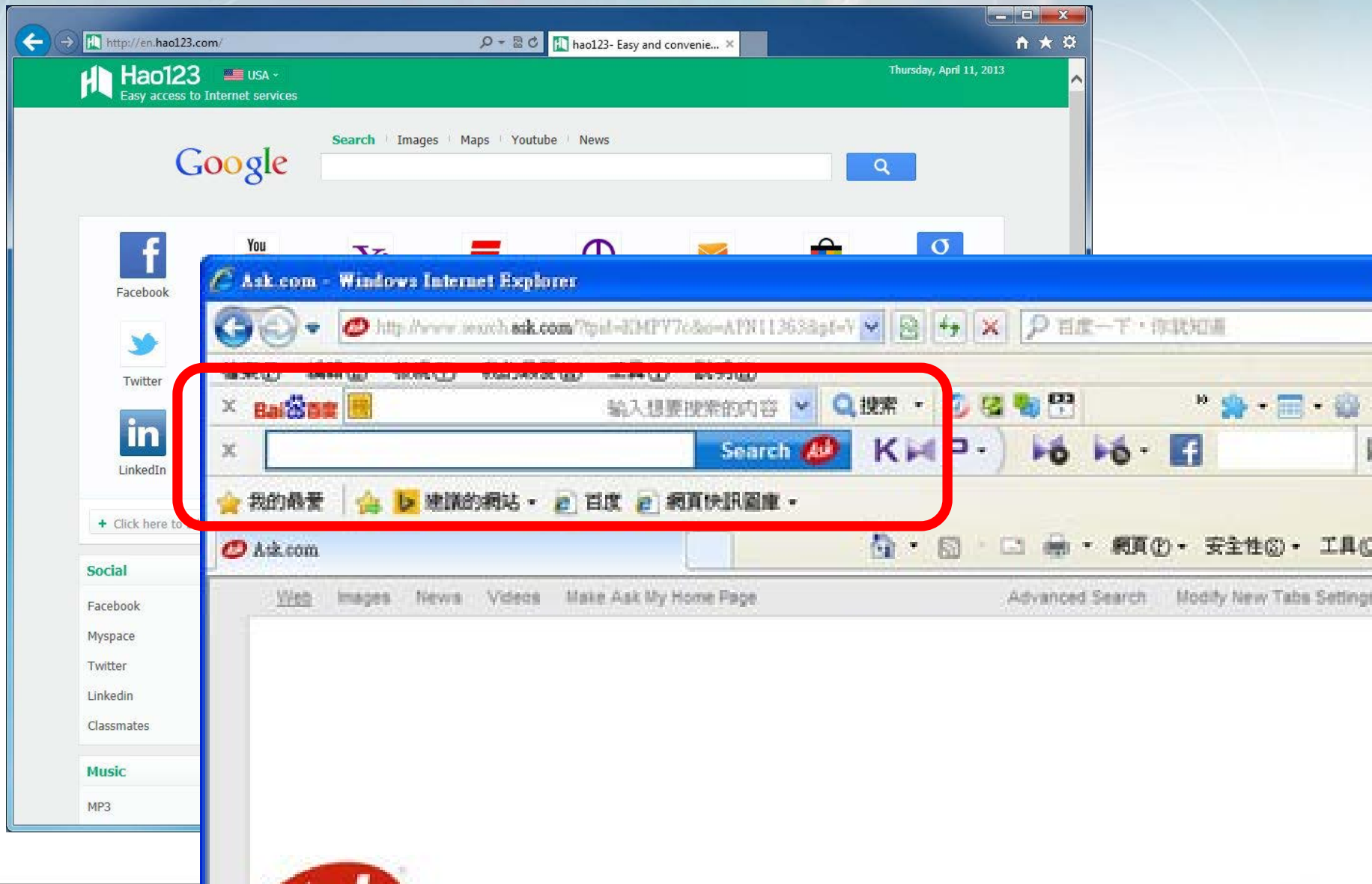
網路詐騙

- 案例分析
  - 劉小姐 2014/10/5 臉書
  - 新聞報導

電腦中毒

- 防範之道:
  - **盡量不用隨身碟，互傳資料時可透過電子郵件的附加檔案或學校的[網路硬碟]**
  - **安裝防毒軟體**
  - 時常更新防毒軟體與作業系統
  - **不要安裝不明軟體，下載軟體請到官方網站**
  - **新購的電腦在安裝完必要的軟體後，請電腦公司幫忙安裝還原系統，遇到太難纏的病毒，用還原的方法是最有效率的方法，平常資料盡量不要放在C槽、桌面、我的文件夾，因為還原後擺在這些地方的資料都會消失。**

誤上釣魚或惡意網站


http://en.hao123.com/
hao123- Easy and convenie...
Hao123
USA
Easy access to Internet services
Thursday, April 11, 2013
Google
Search
Images
Maps
Youtube
News
Facebook
Twitter
LinkedIn
Social
Facebook
Myspace
Twitter
Linkedin
Classmates
Music
MP3
Ask.com - Windows Internet Explorer
Search
Ask.com
Web
Images
News
Videos
Make Ask My Home Page
Advanced Search

誤上釣魚或惡意網站

- 徵狀:
  - 瀏覽器首頁被置換
  - 時常會跳出廣告視窗
  - 個資被盜

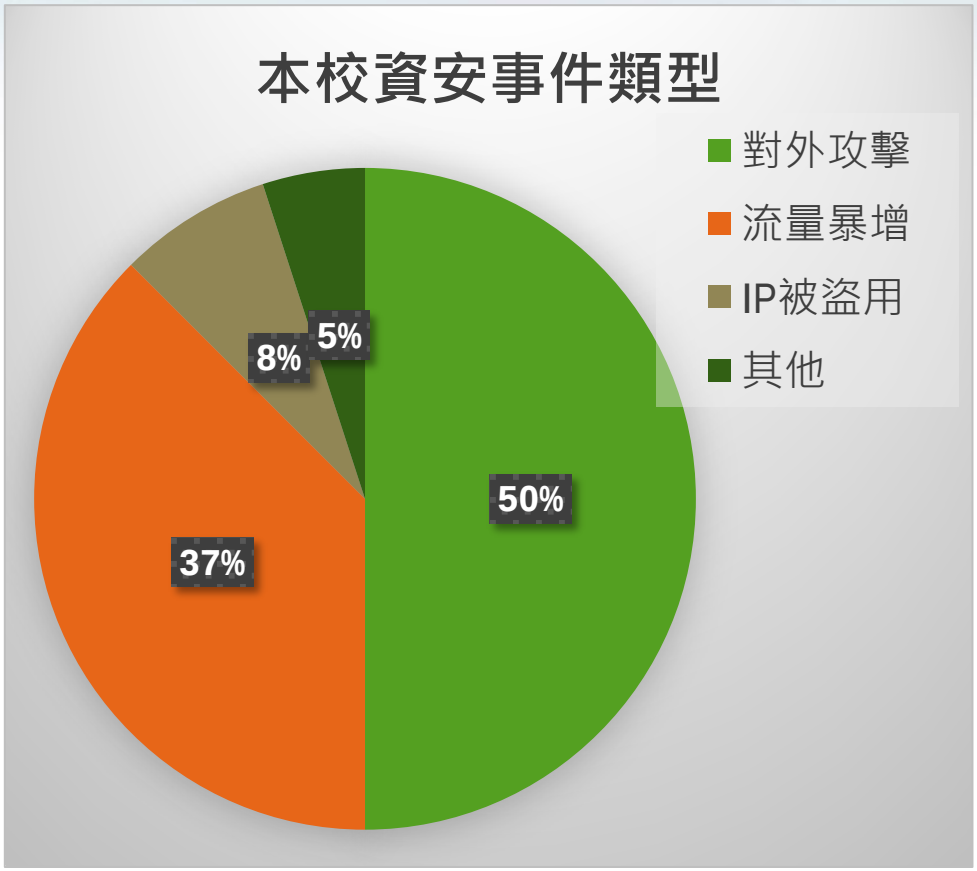
- 常見手法
  - 使用與官網相似的網址與頁面(例:yahoo拍賣)
  - 網路抽獎廣告連結(iPhone6 抽獎)
  - 裝熟套交情的訊息
  - 免費軟體暗度陳倉(例:KMplayer)、暗藏木馬

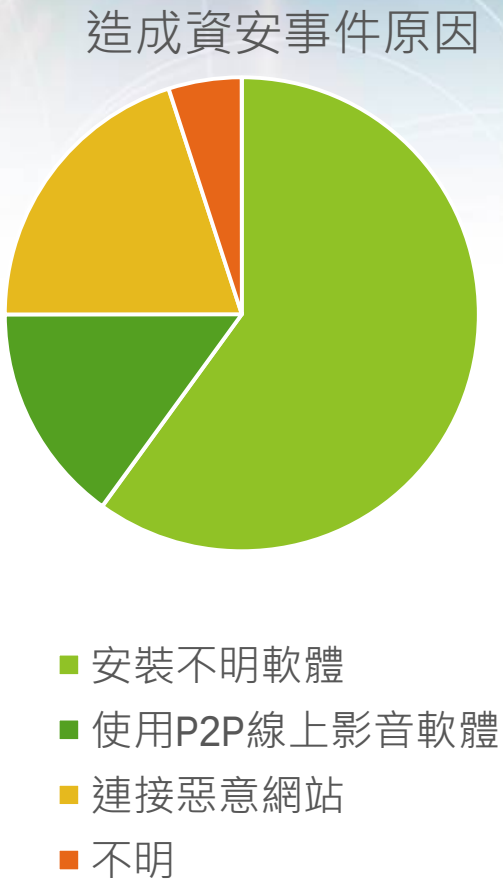
誤上釣魚或惡意網站

- 網路釣魚的防範撇步
  - 對於詢問您個人資料的信件提高警覺
  - 不要隨意點選信件中的網址連結及開啟附件
  - 勿貪小便宜點選好康連結
  - 定期檢查交易紀錄與網站帳號
  - 透過加密的網頁功能傳送個人資料 (網址列的開頭為 https://www.xxx.xxx)

- 參考資料

本校的資安事件分析


本校資安事件類型
對外攻擊
流量暴增
IP被盜用
其他
50%
37%
8%
5%


造成資安事件原因
安裝不明軟體
使用P2P線上影音軟體
連接惡意網站
不明

違反智慧財產權或著作權法

- Q:學校舉辦的各種表演、比賽或紀念活動，常常會利用其他人的著作，像是歌唱比賽，會公開演出他人的詞曲創作，這樣有違反智慧財產權嗎?

違反智慧財產權或著作權法

- 如果沒有賣門票、變相收取像入場費、清潔費等費用，也沒有針對該活動支付給表演的學生或老師任何報酬（對於競賽優勝所頒發的獎金，解釋上並不是屬於表演的報酬），可以在舉辦特定活動的時候，公開演出或公開上映他人的著作。

違反智慧財產權或著作權法

- 參考資料

- Q:有部影片叫「明天過後」，雖然是好萊塢的商業片，但對地球暖化造成的後果有不錯的教育意義，我可以從出租店租來給學生看嗎?

違反智慧財產權或著作權法

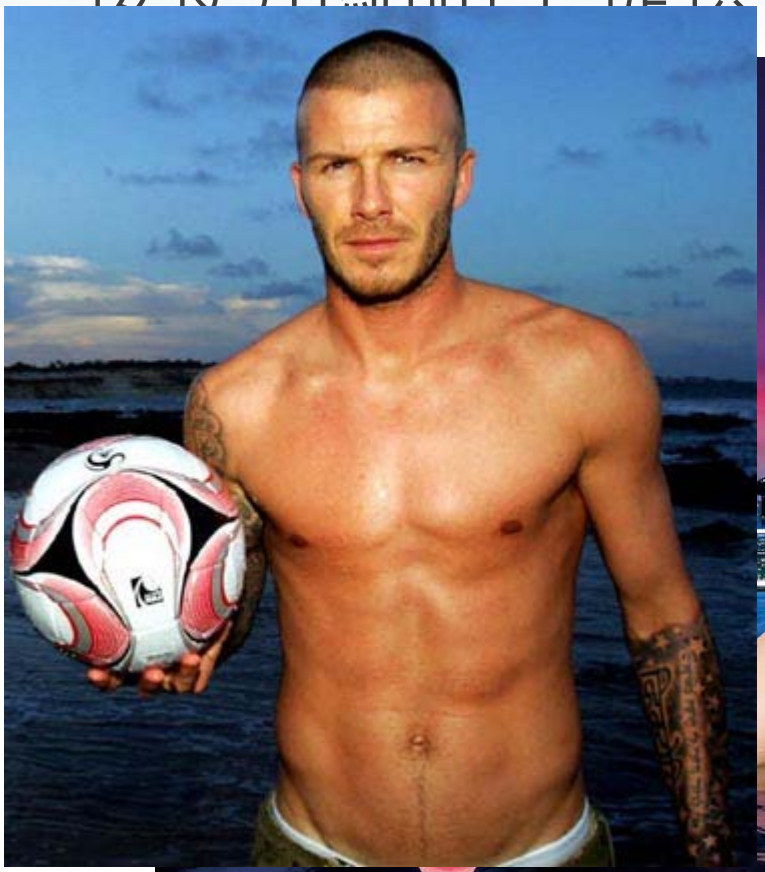
- 參考資料

- 即使從出租店租來的DVD合法影片，或自己購買的影片，也不能在公共場合播放(除非購買的是公播版)。

  學校的老師如果基於非營利的教育目的，播放的影片與課程內容相關，而且所利用的質與量占被利用原著作的比例低，其利用結果對於影片的市場不會造成「市場替代」的效應，可依著作權法第52條之規定引用部分影片，作為教材的內容而在課堂上播放，不必取得授權。

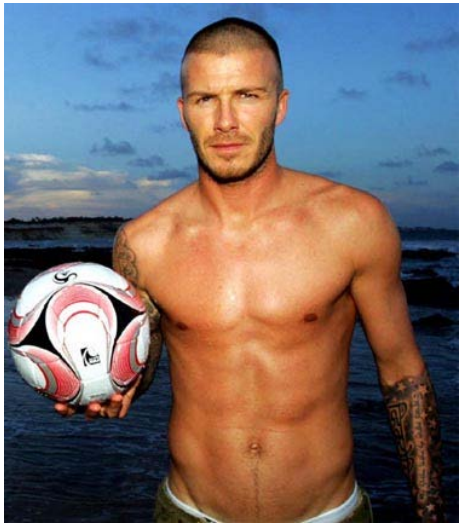
違反智慧財產權或著作權法

- 學校各單位製作海報時或投影片，可否直接使用網路上提供的免費圖片？



違反智慧財產權或著作權法

- 網路上的網頁、照片、圖片、視訊等，除非著作權人有明確的授權，否則均應假定這些他人所發表的著作，都受到著作權法保護，未經合法授權或屬於著作權法之合理使用的情形，不得任意利用他人著作。



違反智慧財產權或著作權法

- 參考資料

- 著作權法第52條規定，「為報導、評論、教學、研究或其他正當目的之必要，在合理範圍內，得引用已公開發表之著作。」

報告完畢
謝謝各位

資訊安全防身術

- 不論學校內部採用多強大的防火牆系統、防毒軟體、或其他資安技術軟硬體設施，仍無法確保校園網路使用與電腦使用是百分之百的安全。
- 國內外許多的研究調查機構均提到，資訊網路安全中最薄弱的一環，往往是電腦及網路系統的使用者。
- 確保使用者具備基礎的資訊安全概念，是低成本的資通安全實施重點，不但能夠有效地提升企業資訊安全落實成果，其效果更勝於高價採購最新技術與設備。

一、牢而不破的密碼設定

- 大部分使用者都知道密碼設定的重要性，但多數的電腦使用者經常忽略或沒有養成設定安全密碼的習慣。
- 密碼使用訣竅如下：

一、牢而不破的密碼設定

- 定期更新密碼
  - 為確保密碼的機密性，使用者應定期更新密碼，減少密碼外流的機率。

一、牢而不破的密碼設定

- 設定優質密碼
  - 設定優質的密碼（不容易被猜中的密碼）
    保護各個電腦系統是非常重要的。為減少密碼遭受駭客破解所造成損失，電腦管理者也需要一套程序來確保密碼的正常運作。
  - 設定優質密碼的秘訣如下：

一、牢而不破的密碼設定

- 設定至少 6 個字元的密碼
  - 密碼設定建議字元至少需為 6 個字元的字串。
  - 為提高密碼使用的安全性，設定 6 個以上字元的密碼字串，並且定期更新密碼，可提高密碼的安全性。

一、牢而不破的密碼設定

- 避免使用重複的字母或數字，如aaa1122, 555iii99。
- 使用數字、字母、符號混合穿插的密碼字串。
  - 為增加密碼被破解的難度，應避免使用簡單且他人容易取得的資料為個人密碼（姓名、電話、生日、電子信箱網址等）。
  - 建議以大小寫字母、數字、及符號（＃％＄@…）混合方式設定密碼。

一、牢而不破的密碼設定

- 不使用過於複雜而無法記憶的密碼
  - 過於複雜的密碼導致使用者必需寫下密碼便於記憶，卻提高了密碼外洩的風險。
- 利用特殊符號記憶密碼
  - 若要使得密碼簡單易記，使用者可以選擇喜愛的名字但務必穿插數字或符號以增加密碼破解的難度，並將特定的字母用類似的符號或數字取代。
  - 例如將happiness 修改為h@pp1n3ss ，可同時使得密碼簡單易記，又能增加密碼使用的安全性。

一、牢而不破的密碼設定

- 避免重複使用已使用過的密碼
- 避免使用簡單且字典查得到的單字或學校名稱縮寫
- 檢測密碼強度：
  - http://www.refly.net/passwordchecker
  - http://www.microsoft.com/taiwan/athome/security/privacy/password_checker.mspx

一、牢而不破的密碼設定

- 良好的使用習慣
  - 不告訴別人密碼，包括男女朋友、職務代理人、上司等。
  - 若懷疑有人可能知道你的密碼時，即刻更改。
  - 不設定過於複雜難記的密碼。
  - 不寫下密碼　。
  - 定期更換密碼。

二、遠離網路釣魚犯罪陷阱與騙局

- 網路犯罪集團常利用電子郵件或網頁進行網路釣魚行為，使用者須注意任何信函以及網址正確性，先從字面分辨與確認信函的正確性，以提高警覺度。

二、遠離網路釣魚犯罪陷阱與騙局

- 防範訣竅：
  - 不回應任何來自不明單位於電子信件中要求提供個人隱私安全相關資訊，這些資訊包括使用者名稱、密碼、帳號。
  - 不點選來路不明的電子郵件中所載之網頁連結。
  - 不利用校園網路轉寄垃圾信函。
  - 點選網頁連結前請一定要仔細辨認。

二、遠離網路釣魚犯罪陷阱與騙局

www.vvest.com

www.west.com

www.paypa1.com

www.paypal.com

https://ebank.bot.com.tw

http://ebnk.bot.conn.tw

http://tw.bid.yahoo.com/

http://tw.bids-yahoo.com/

二、遠離網路釣魚犯罪陷阱與騙局

www.vvest.com

www.west.com

www.paypa1.com

www.paypal.com

二、遠離網路釣魚犯罪陷阱與騙局

https://ebank.bot.com.tw

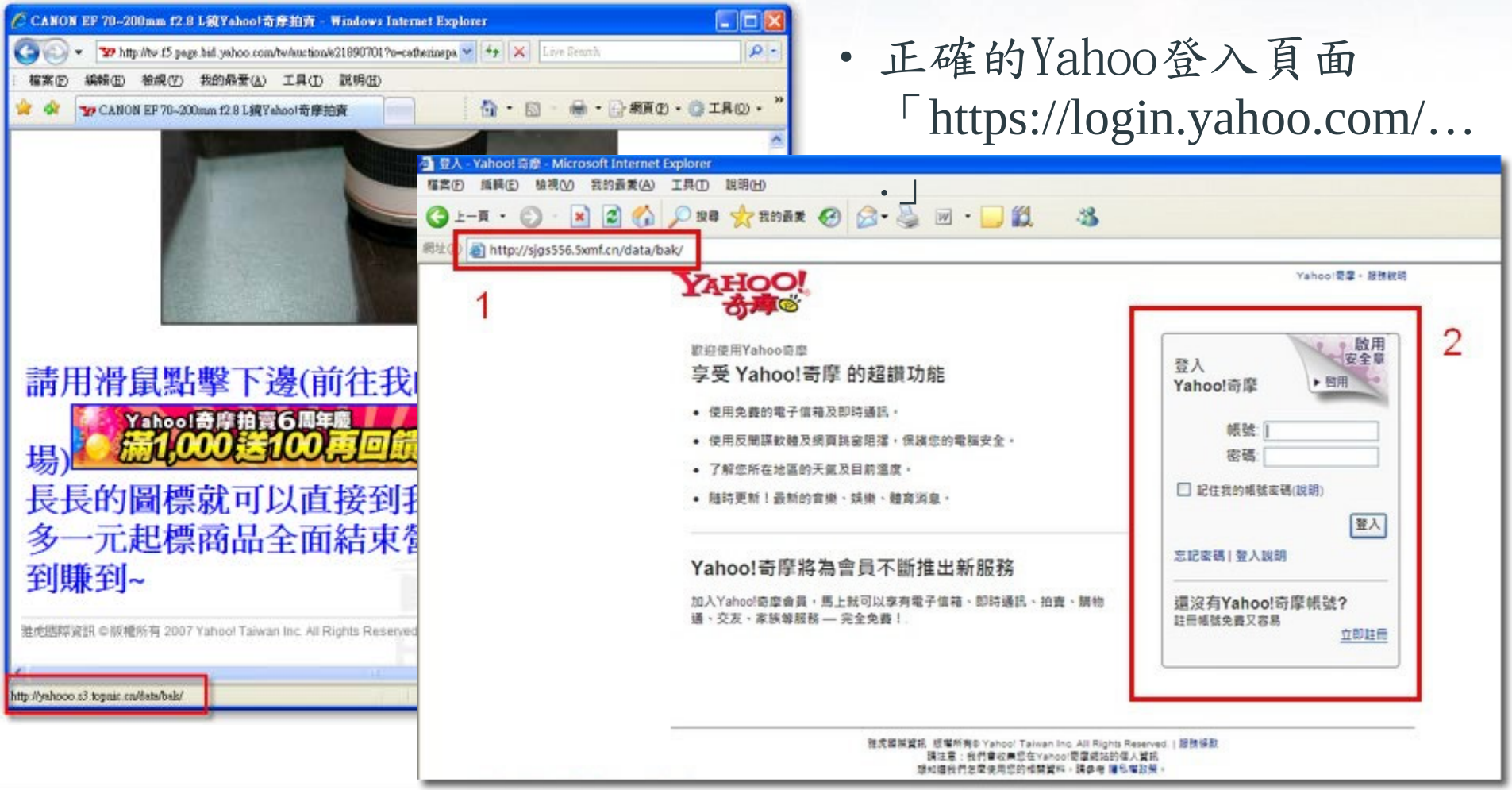
http://ebnk.bot.conn.tw

http://tw.bids-yahoo.com/

http://tw.bid.yahoo.com/

二、遠離網路釣魚犯罪陷阱與騙局

- 詐騙網址hxxp://yahooo.s3.topnic.cn/data/bak/



- 正確的Yahoo登入頁面「https://login.yahoo.com/…

三、確保工作領域的私密

- 員工經常會把機密性資料文件、備忘紙、以及記載個人相關資訊等文件，隨意放置於桌上。
- 或者將資料進行完善的分類，並且儲存在電腦桌面上，這些動作都很容易導致資料的外洩。

三、確保工作領域的私密

- 防範訣竅：
  - 當離開個人座位時，啟動鎖定功能(視窗鍵+L)或設定螢幕保護程式，並設定關閉螢幕保護程式的密碼。

三、確保工作領域的私密

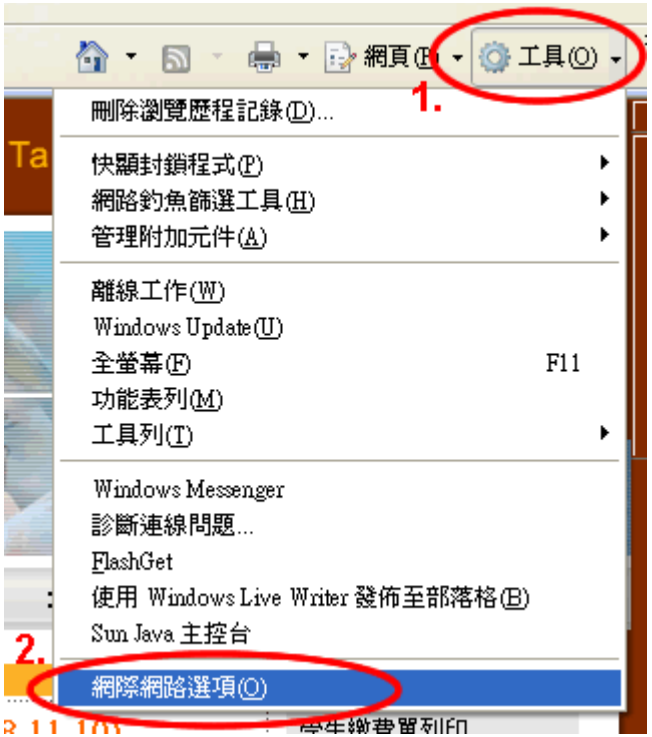
- 防範訣竅：
  - 教育員工提高警覺，不在桌面上放置重要文件，或使用可上鎖的抽屜等設備保管機密文件。

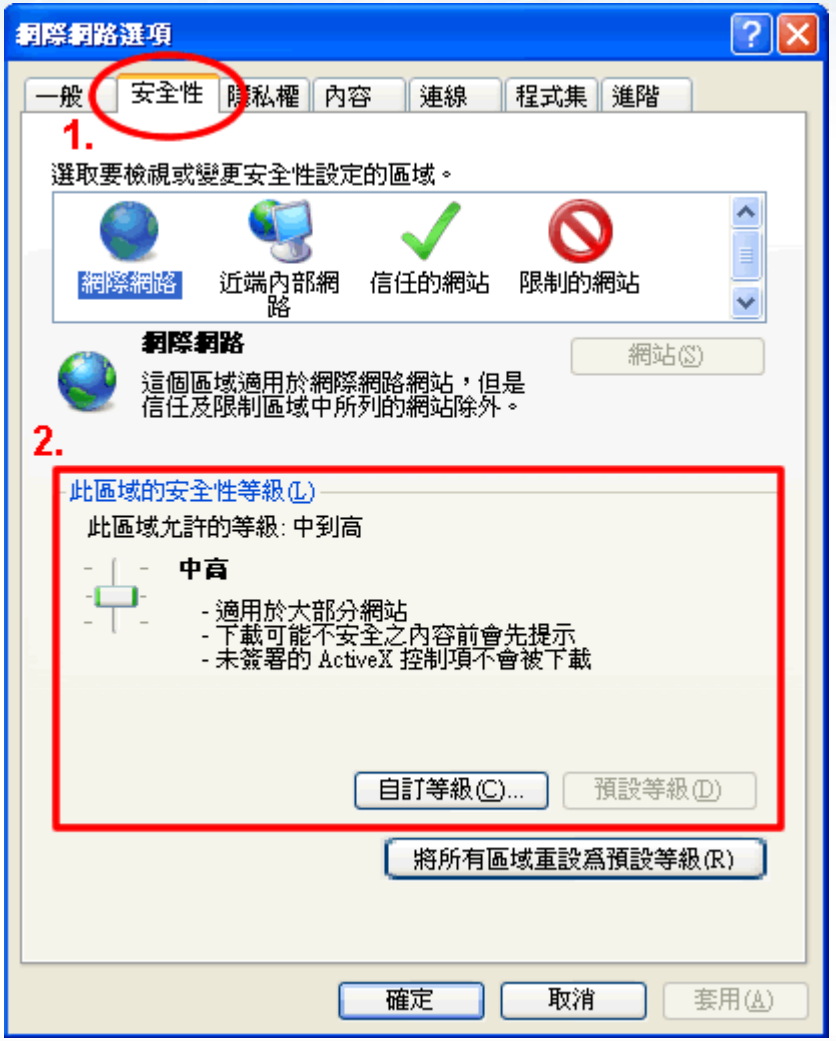
四、確保網路瀏覽器使用

- 許多微軟IE使用者將瀏覽器安全控制程度設定降低以方便網頁讀取，但這很可能讓網路瀏覽器成為惡意程式侵入電腦的管道。
- 當使用者瀏覽具有惡意程式的網頁時，可能因為安全控制程度設定值不高，自動下載惡意程式使電腦造成損害。

四、確保網路瀏覽器使用

- 防範訣竅：
  - 建議將讀取網頁瀏覽器安全層級設定為中安全性以上。





四、確保網路瀏覽器使用

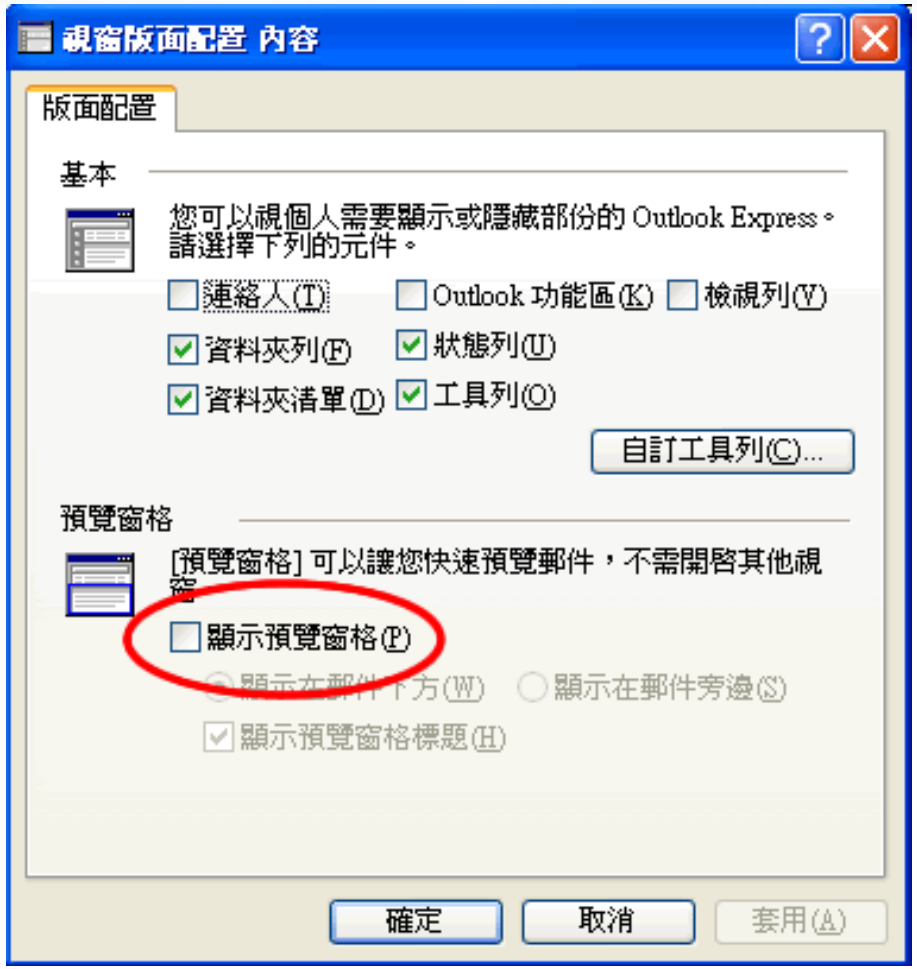
- 防範訣竅：
  - 對於經常使用且可信任的網站，可預先於工具列中設定該網址為可信任，以避免瀏覽器在高安全層級設定下，導致網頁無法正常讀取之困擾。
  - 改用其它較安全的瀏覽器軟體，如FireFox…等。

五、正確的使用電子郵件

- 電腦病毒傳播最經常的途徑為電子郵件，不隨意開啟電子郵件附夾檔案為資安保全基本要件。

五、正確的使用電子郵件

- 防範訣竅：
  - 關閉郵件預覽功能。
  - 檢視→版面配置→



五、正確的使用電子郵件(二)

- 防範訣竅：
  - 除非使用者相當確定信件來源與信件夾帶的附件內容為何，否則決不輕易開啟或執行電子信件裡的附件檔案。
  - 安裝防毒軟體。

五、正確的使用電子郵件

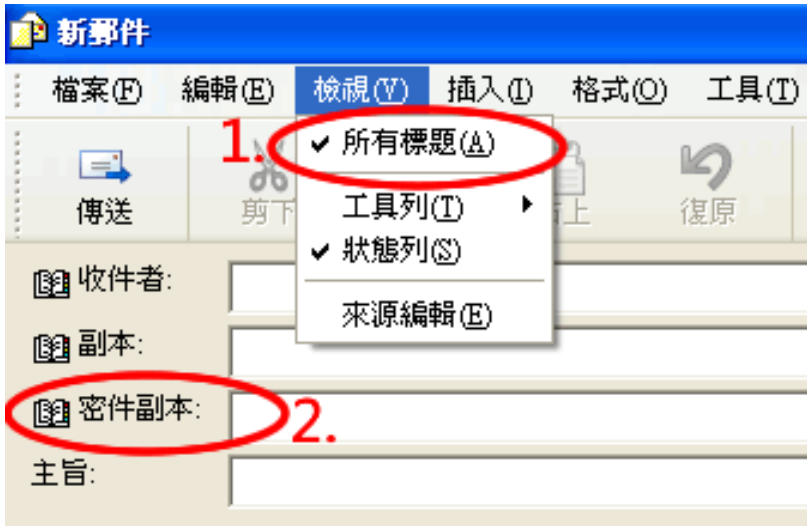
- 除了上述的防範訣竅，對於電子郵件的正確使用與資訊安全、權益維護，還包括下列幾點：
  - 不要將電子郵件密碼告知任何人，即使對方是系統管理者。
  - 不要將電子郵件帳號轉借他人使用。
  - 不要使用電子郵件傳輸任何不當資訊，包括不法、暴力、色情、違法交易、侵犯隱私或威脅他人的資料。

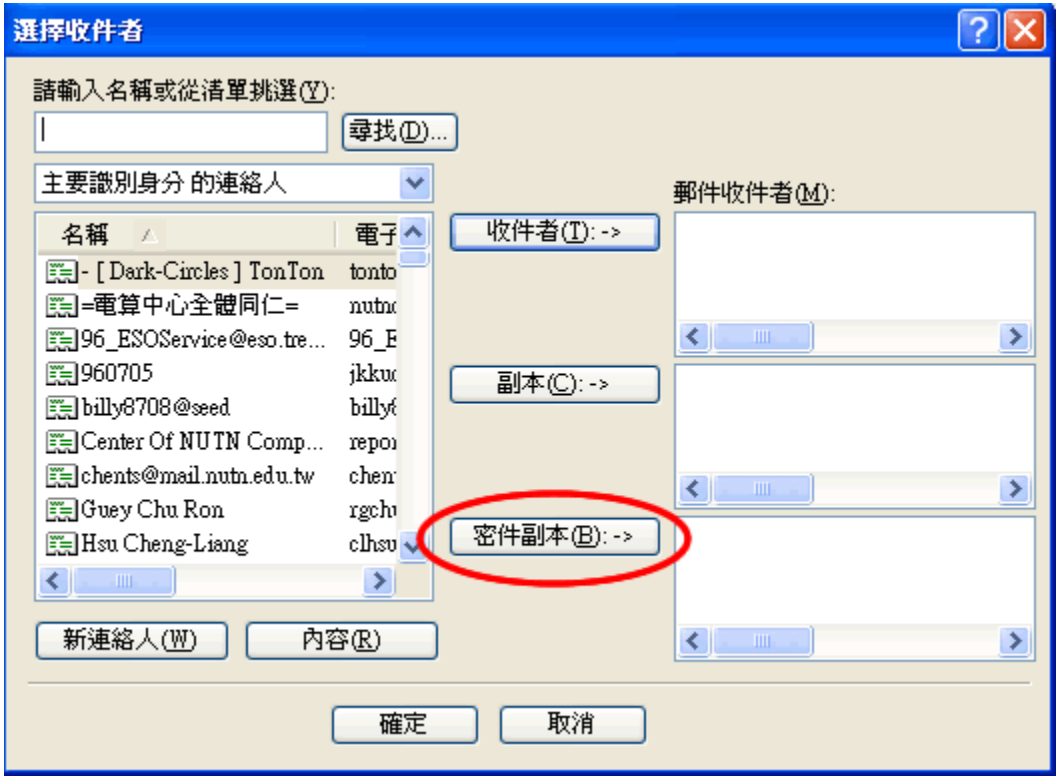
五、正確的使用電子郵件

- 不要轉寄不明網路謠言及發送廣告信。
- 避免在電子郵件夾帶大容量檔案，以免造成收件人收信時間冗長的困擾。
- 轉寄或回覆郵件時，勿隨意修改作者原始文字。
- 郵件中如含有他人之個人隱私資訊，在轉寄時應先取得同意。

五、正確的使用電子郵件

- 同時寄件給多人時，為保護各收信人資訊，最好使用「密件副本」方式傳送。





六、確認防毒軟體隨時運作

- 防毒軟體的偵測與防範功能只有在該軟體有在運作、且有時常更新病毒碼情形下，才會產生效用。

六、確認防毒軟體隨時運作

- 防範訣竅：
  - 不關閉、不刪除防毒軟體。
  - 隨時注意防毒軟體的病毒碼是在最新的狀態。
  - 定期執行掃毒。

七、勿隨意安裝未經許可的電腦軟體

- 網路上有許多免費分享的實用軟體或遊戲，但通常提供企業使用的軟體並非永久免費的。
- 任意下載、安裝網路上的免費軟體、或來路不明的軟體，也是感染電腦病毒、間諜軟體與特洛依木馬程式的主要途徑。
- 某些合法軟體因為不明軟體的使用產生衝突情況，也可能因此造成電腦系統部故障。

七、勿隨意安裝未經許可的電腦軟體

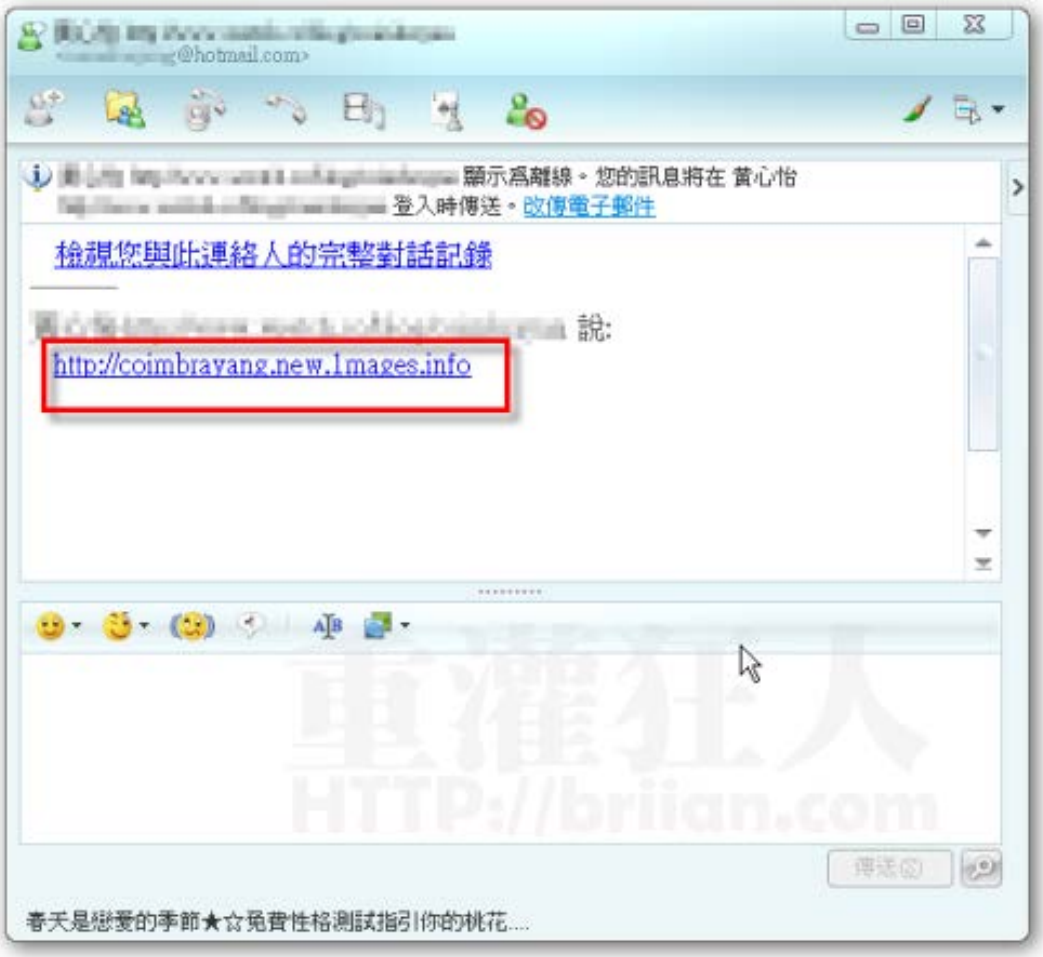
- 防範訣竅：
  - 絕對不下載、安裝未經許可的軟體。

八、謹慎使用即時通訊軟體

- 即時通訊軟體（如Line、Yahoo即時通…等）雖然是快速且方便的網路溝通工具，但也有可能成為電腦病毒傳遞途徑，也可能遭受其它惡意程式與網路釣魚的攻擊，使用即時通訊系統時必須小心謹慎。

八、謹慎使用即時通訊軟體

- 存在的風險
  - 病毒威脅
  - 垃圾訊息
  - 檔案交換
  - 洩密
  - 工作效率的影響



八、謹慎使用即時通訊軟體

- 正確的運用方法：
  - 登入密碼最好不要用「儲存密碼」記錄於系統內。
  - 不任意傳遞與分享單位重要資訊或檔案。
  - 不任意接收來路不明之分享檔案和連結。
  - 使用者必須秉持以公事使用之目的使用即時訊息。
  - 隨時更新使用端程式。

九、確保軟體在更新狀態

- 當軟體被使用一段時間後，通常會出現一些小問題或安全漏洞，這些漏洞也是駭客容易利用的弱點，**零時差攻擊**即目前駭客最喜歡利用的手法。
- 因此信譽好的軟體商通常會設計更新或修補程式來修正這些問題。

九、確保軟體在更新狀態

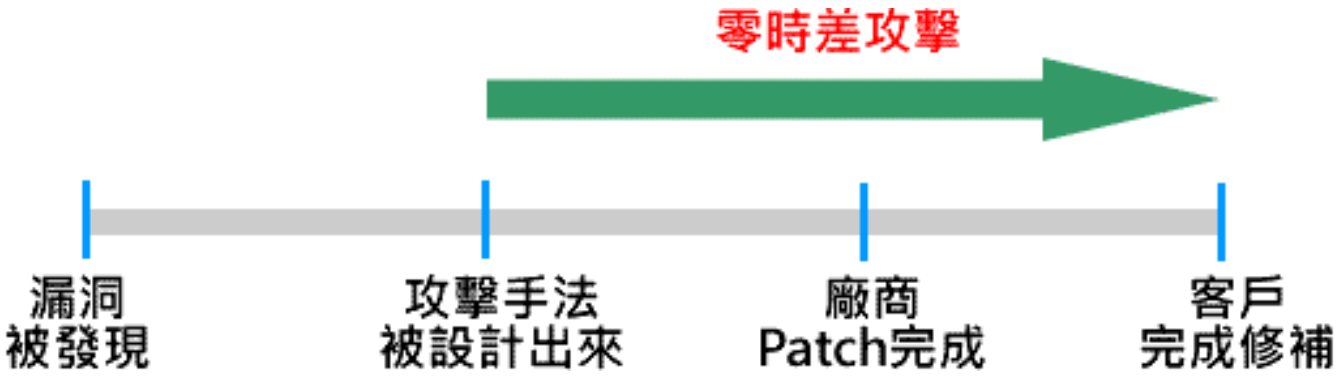
- 防範訣竅：
  - 檢查以下重要應用程式或軟體是否為最新版本：
    - 作業系統(Windows XP 或2000、Mac、Linux…等)
    - 網頁瀏覽程式(IE、FireFox…等)
    - 辦公室應用軟體(Office、Adobe PDF…等)
    - 電子郵件收發軟體(如outlook、outlook express…等)
  - 大部分的軟體都會提供一項「自動更新」功能，啟動自動更新功能為最方便也最迅速的一種定時更新方法。

零時差攻擊

- 何謂零時差攻擊(Zero Day Attack)？有兩種解釋：
  - Software Cracks
    這牽涉到聰明的crackers(怪客)能透過管道，例如透過軟體開發者或販售部門，早就事先取得了軟體進行破解，因此可以在產品正式出現在市面上不到一天(0 day)，得以進行漏洞攻擊。（早就分析透徹得出破解之道）

零時差攻擊

- Remote Exploits
  0-day也是指有心人士搶在軟體廠商尚未公佈漏洞及補丁之前，先發現到漏洞再利用漏洞攻擊目標得逞。



零時差攻擊

- 過去大家認為只有執行檔(.exe)才會夾帶惡意程式，現在已大為改觀，MS Word檔、甚至是PowerPoint檔都可能被駭客利用。
- 近年來越來越多的駭客攻擊是透過社交工程手法，以笑話、政治、健康、色情等引人好奇的內容，甚至是假冒名義寄送經特殊設計之 Word 文件檔案，誘使收件人開啟以達成功入侵之目的，同時再利用尚未公佈之弱點設計「零時差攻擊」，以達成即使是在弱點完整修補之電腦上，亦能夠成功入侵之目的。

零時差攻擊

- 面對此類結合**社交工程**與**零時差攻擊**的新興威脅，建議使用者除了勿任意開啟來路不明的電子郵件外，在檢視可疑電子郵件中所附的Word 文件時，可先利用附屬應用程式之WordPad閱讀，或至微軟公司網站下載Word Viewer 2003安裝後再閱讀。
- 或是降低電腦使用者的使用權限，避免賦予最高權限等做法，以降低「**零時差攻擊**」之風險。

十、正確使用可攜式媒體

- 自動播放不等於自動執行。
- USB病毒利用自動播放的特性去誘導出自動執行的動作，進而去執行(開啟)惡意的程式。
- 有效避免自動執行的方法：

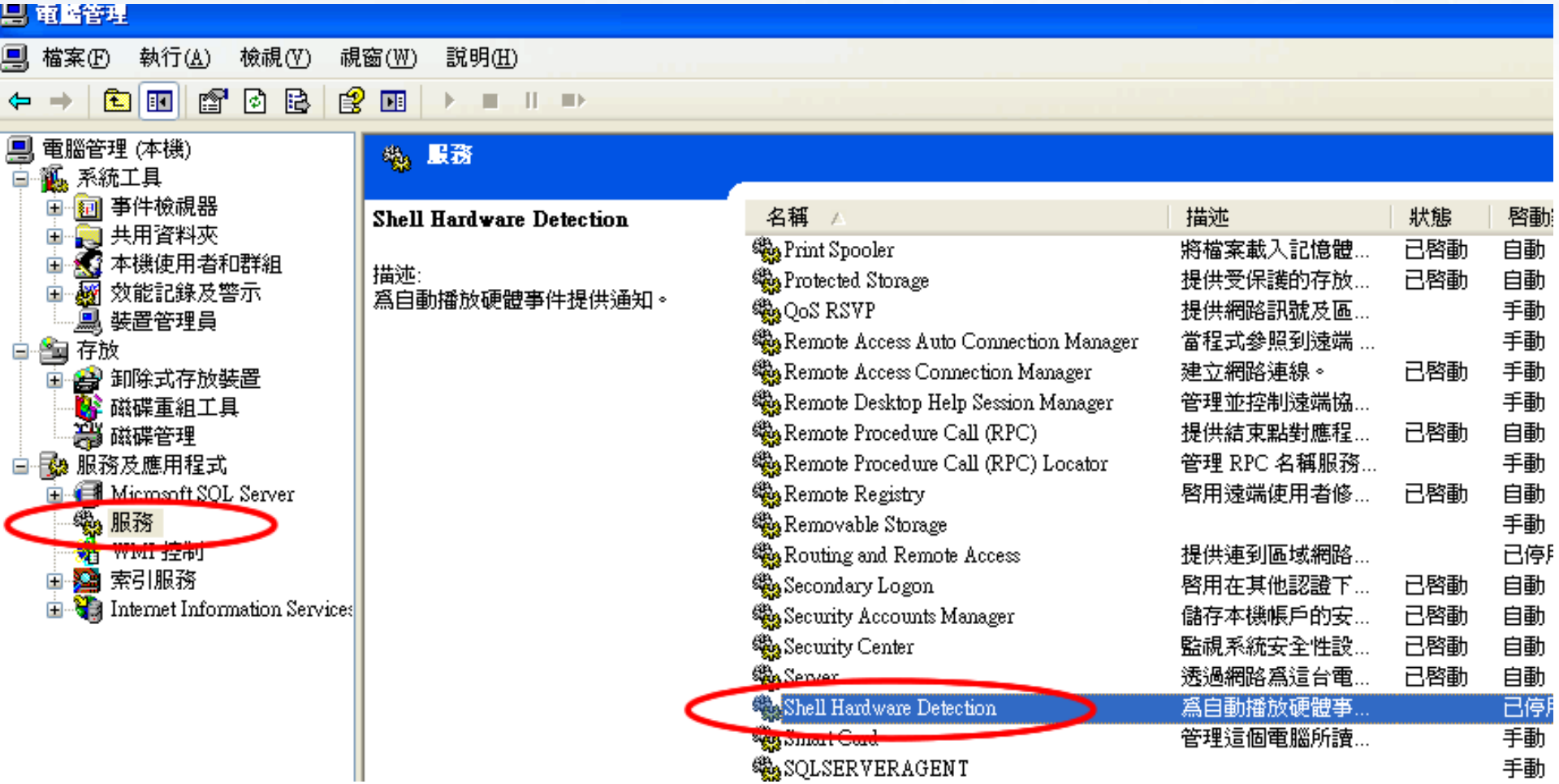
十、正確使用可攜式媒體

- 檔案總管操作法
  - 開始→我的電腦(按右鍵)→檔案總管
    或是利用快捷鍵：視窗鍵 ＋ E
  - 點選左邊窗格USB媒體，開啟檔案

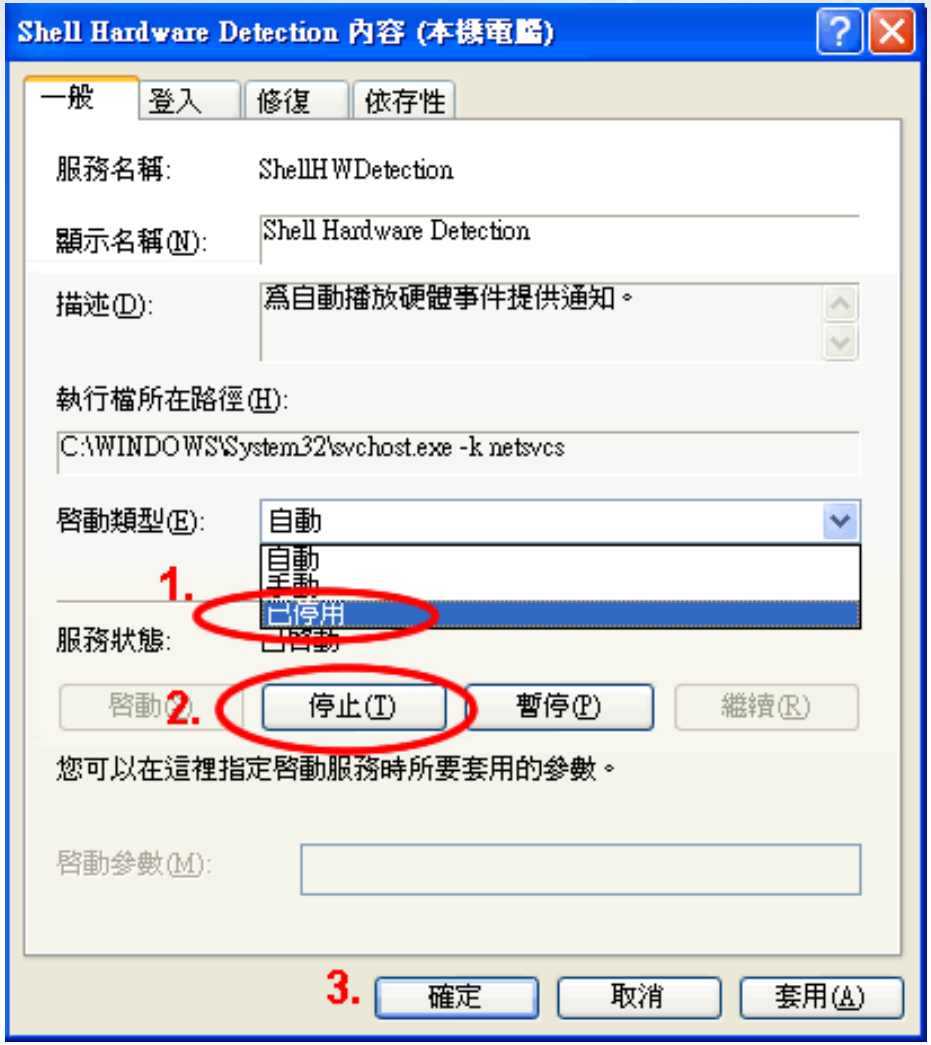
十、正確使用可攜式媒體

- 電腦管理服務設定法
  - 開始→我的電腦(按右鍵)→管理→電腦管理→服務及應用程式→服務
  - 停用Shell Hardware Detection服務

十、正確使用可攜式媒體

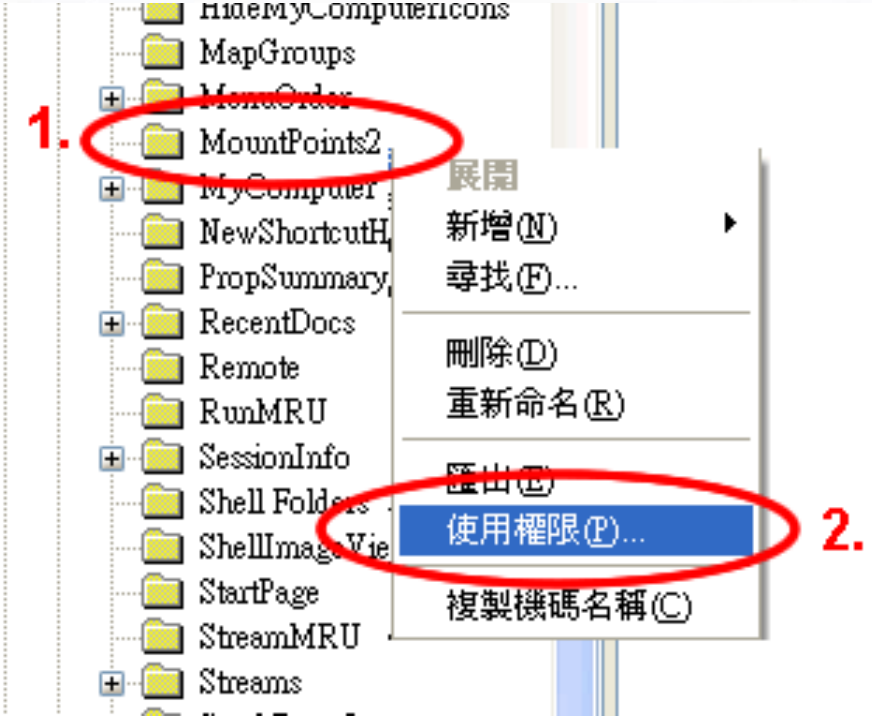

電腦管理
檔案(F) 執行(A) 檢視(V) 視窗(W) 說明(H)
電腦管理 (本機)
系統工具
事件檢視器
共用資料夾
本機使用者和群組
效能記錄及警示
裝置管理員
存放
卸除式存放裝置
磁碟重組工具
磁碟管理
服務及應用程式
Microsoft SQL Server
服務
WMI 控制
索引服務
Internet Information Services
服務
Shell Hardware Detection
描述:
為自動播放硬體事件提供通知。
名稱
描述
狀態
啓動
Print Spooler 將檔案載入記憶體... 已啓動 自動
Protected Storage 提供受保護的存放... 已啓動 自動
QoS RSVP 提供網路訊號及區... 手動
Remote Access Auto Connection Manager 當程式參照到遠端 ... 手動
Remote Access Connection Manager 建立網路連線。 已啓動 手動
Remote Desktop Help Session Manager 管理並控制遠端協... 手動
Remote Procedure Call (RPC) 提供結束點對應程... 已啓動 自動
Remote Procedure Call (RPC) Locator 管理 RPC 名稱服務... 手動
Remote Registry 啓用遠端使用者修... 已啓動 自動
Removable Storage 手動
Routing and Remote Access 提供連到區域網路... 已停
Secondary Logon 啓用在其他認證下... 已啓動 自動
Security Accounts Manager 儲存本機帳戶的安... 已啓動 自動
Security Center 監視系統安全性設... 已啓動 自動
Server 透過網路為這台電... 已啓動 自動
Shell Hardware Detection 為自動播放硬體事... 已停
Smart Card 管理這個電腦所讀... 手動
SQLSERVERAGENT 手動

十、正確使用可攜式媒體


Shell Hardware Detection 內容 (本機電腦)
一般
登入
修復
依存性
服務名稱:
ShellHWDetection
顯示名稱(N):
Shell Hardware Detection
描述(D):
爲自動播放硬體事件提供通知。
執行檔所在路徑(H):
C:\WINDOWS\System32\svchost.exe -k netsvcs
啓動類型(E):
自動
自動
手動
已停用
1.
服務狀態:
已啓動
啓動(S)
2.
停止(T)
暫停(P)
繼續(R)
您可以在這裡指定啓動服務時所要套用的參數。
啓動參數(M):
3.
確定
取消
套用(A)

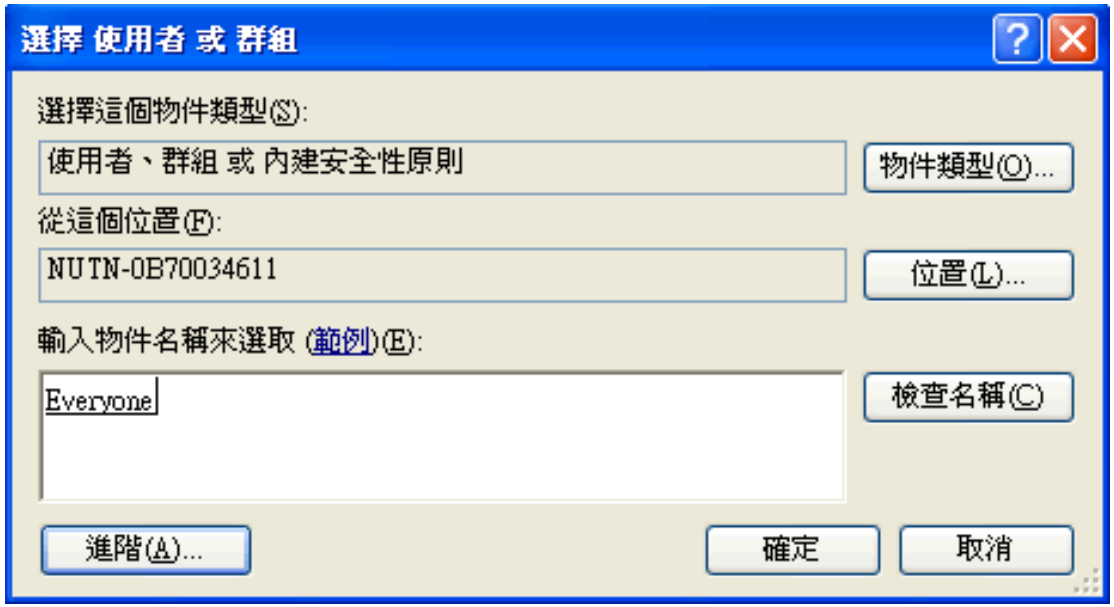
十、正確使用可攜式媒體

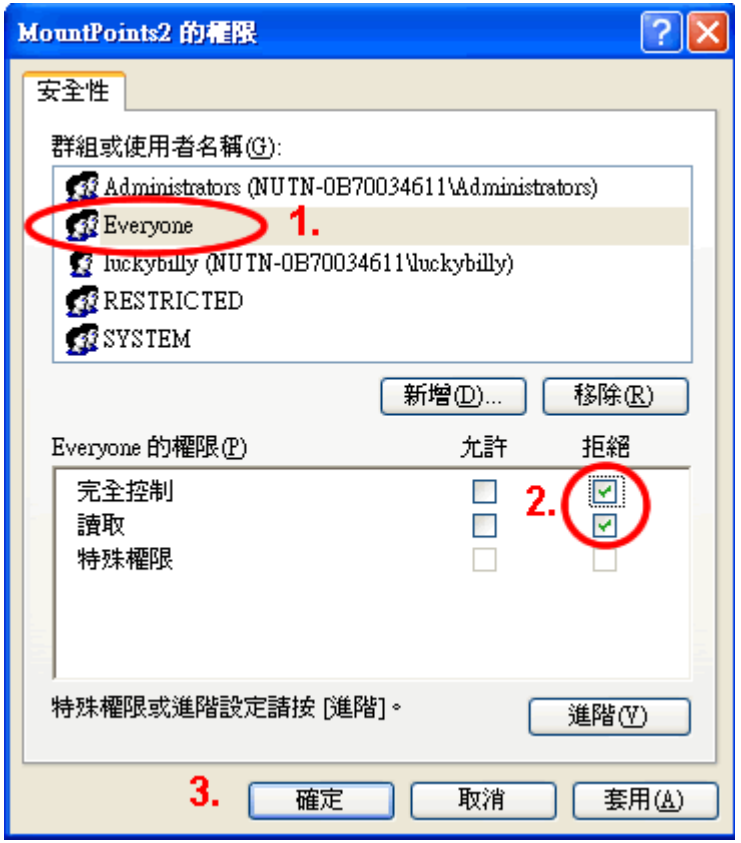
- 修改MountPoints2機碼
  - 開始→執行→輸入regedit進入登錄編輯程式。
  - 找到機碼名稱HKEY_CURRENT_USER\Software\microsoft\Windows\CurrentVersion\Explorer\MountPoints2
  - 點選MountPoints2，按右鍵選擇「使用權限」



十、正確使用可攜式媒體

- 新增使用者Everyone。
- 設定使用者Everyone的完全控制權限為「拒絕」，選取套用/確定後離開。





關閉USB自動執行

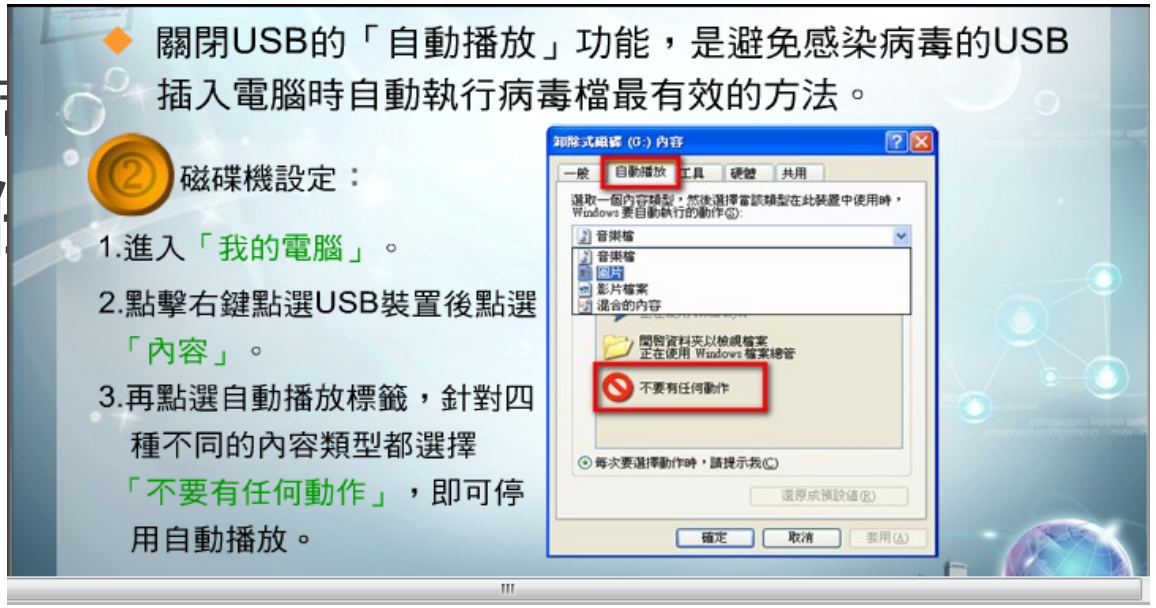
方法一：插入這些USB裝置的時候，請先**按住鍵盤的【Shift】鍵**（一直按著不要放開）。

等到右下角的安全地移除硬體圖示出現後，你才可以放掉【Shift】鍵

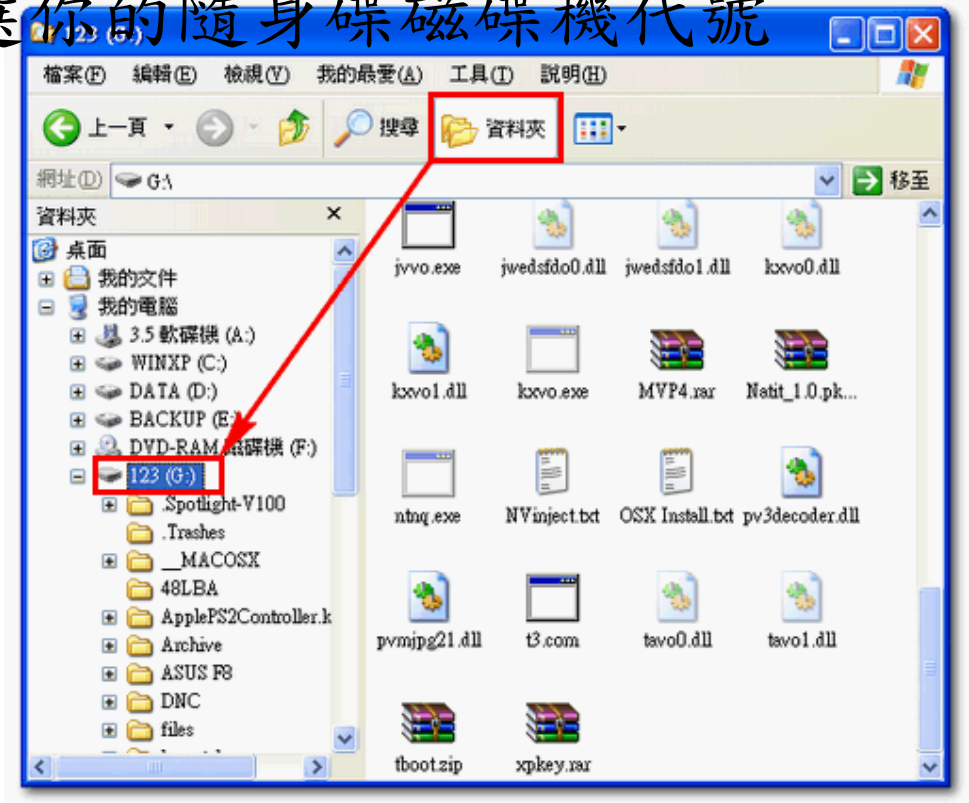
※小提示：按左邊的【Shift】鍵吧！

關閉USB自動執行

- 方法二：「我的電腦」/選「USB裝置」，按右鍵/「內容」/「**自動播放**」
- 針對四個不同
  擇「**不要有任**



用【我的電腦】來開啟隨身碟，
「**不要直接在隨身碟的磁碟機點二下來開啟它**」
選上方的「資料夾」工具列，這時候左邊就會多出來一個「資料夾」的視窗，請你由左邊的視窗點選你的隨身碟磁碟機代號



防護軟體簡介

- 安裝三種防護軟體
  - 防毒軟體：
    Avira AntiVir PersonalEdition
  - 防木馬、間諜程式軟體：
    Ad-Aware Spyware Doctor
  - 隨身碟掃毒軟體：
    WowUSBProtector、USBcleaner、
    SafeUSB、kavo_killer4.14、
    USB_WriteProtector

駭客入侵與安全防護

- 認識駭客入侵和攻擊方式
- 建立網路安全防護網
- 防火牆

駭客入侵與安全防護

- 駭客入侵電腦的方式有千百種，就像病毒一樣無孔不入，防治病毒可以利用防毒軟體來幫忙，而防止駭客入侵，也可以建立一套安全防護網，讓駭客無法越雷池一步。

8-3.1　認識駭客入侵和攻擊方式

- 駭客為何要入侵別人電腦？有些是為了好玩惡作劇，有些是想竊取資料，有些則是進行惡意攻擊.....等等。總而言之，駭客就是網路上不友善的敵人，所以只能做好防治工作，減少駭客入侵的機會。
- 前一小節介紹了一些網路知識，例如：搜尋網路上有哪些電腦，以及電腦開啟了哪些通訊埠，這些都是駭客尋找攻擊目標的基本方法。
- 駭客入侵與攻擊的方式大致可分為直接入侵Windows系統、攻擊系統漏洞、破解密碼、竊取密碼、轟炸郵箱、植入木馬程式等方式，分別說明如下。

直接入侵Windows系統

- 對於不設防Windows系統，駭客想要進行入侵，將像是探囊取物一般，如入無人之境。若上網的電腦設定了分享硬碟或資料夾，而又沒有設定密碼，則駭客在取得入侵電腦的IP位址，以及確定其為Windows系統後，就可以直接入侵到系統中。
- 而設有密碼的資料夾，駭客也可能找出破解的方法。

破解密碼與竊取密碼

- 破解密碼是在電影中經常看到的情節，而破解密碼也是網路駭客的基本技倆。破解密碼是入侵者和被入侵者的攻防戰，越複雜的密碼當然就越難破解。
- 猜測法是駭客破解密碼的主要方法之一，若帳號是Admin、Administrator、Guest、Users、電腦名稱.....等等，而密碼是123456、abcde、111111、與帳號相同、出生年月日.....等等，駭客很容易就可以猜中，據說猜中率高達25%。
- 除了猜測法，駭客可能會使用其他的技巧，直接取得帳號與密碼，例如：更改登錄檔、植入木馬程式等。

攻擊系統漏洞

- 利用作業系統本身的安全漏洞，是駭客進行攻擊的主要方式之一，不論是Windows或Linux都有一些安全漏洞。
- 駭客會不斷的檢測作業系統有哪些漏洞，當發現漏洞之後，就可以肆無忌憚地進行攻擊活動。
- 修正程式是作業系統開發廠商用來彌補漏洞的更新程式，若電腦中的作業系統是Windows XP、2000或Server 2003，一定經常出現系統更新的畫面，其中一定包含了安全性修正程式，Windows 2000的SP2（Service Pack 2）、SP3與Windows XP的SP2（Service Pack 2）等程式，是微軟發現系統漏洞後所發佈的修正程式。

轟炸郵箱

- 轟炸郵箱是駭客的入門能力，多數駭客都會使用這種方式來攻擊網路上的郵件信箱。駭客隱藏了自己的基本資料和IP位址，並且使用SMTP伺服器（例如：Yahoo Mail）或轉向寄信（透過代罪羔羊的電腦IP），然後大量郵寄信件給攻擊目標信箱，使其塞爆信箱容量。
- 駭客也可能使用郵件炸彈程式，不斷發送小郵件給攻擊目標信箱，當被攻擊的電腦收到這種郵件時，可能會當掉或關閉，造成郵件管理程式癱瘓，而無法使用。

植入木馬程式

- 特洛依木馬（Trojan Horse）程式簡稱為木馬程式，是一種可以潛入電腦中執行，而不被使用者發現的程式。
- 木馬程式一旦被植入電腦中，就會開啟一道通訊埠，俗稱為“後門”，等待遠端的駭客下達指令並許多任務，例如：**轉向入侵、遠端遙控、偷取封包、偷取密碼、複製檔案、刪除檔案**等等。
- 駭客如何將木馬程式植入電腦中呢？除了應用前面的系統漏洞外，還可以透過E-mail夾帶和方式，引誘更新程式），另外也可能放在FTP站上傳播或使用。

建立網路安全防護網

- 在沒有任何防範措施的情況下，遭受駭客入侵便不足為奇，而若能提高網路安全的警覺性，設定必要的安全防護網，則駭客想要入侵，就不是那麼簡單了。
- 隨時小心駭客就在身邊，被駭客入侵的機會就可以減低很多，例如：上網的時候盡量不要讓別人知道IP位址；應用網路上的芳鄰分享檔案時，務必以帳號與密碼來控管使用權限。
- 只要具備上述基本的安全防護措施，就可以讓駭客不易入侵！而想要建立更健全的防護網，則必須安裝防火牆、防毒軟體、入侵偵測系統等軟體。

防火牆：

- 防火牆（Firewall）是一種網路安全機制，在電腦與Internet之間建立一個保護措施，通常用來防止內部網路以外或內部網路的未授權存取，因此可以確保電腦免於遭受網路上的駭客入侵，防止資料被人蓄意破壞或竊取，所以防火牆又稱為安全邊緣閘道。
- 根據安全需求，可以採用軟體防火牆，或硬體防火牆來保障網路安全，Windows XP內建了簡易防火牆功能，稱為網際網路防火牆（Internet Connection Firewall，簡稱ICF），對於個人或家庭使用者來說，其攔截入侵功能已經足夠。
- 許多防毒軟體也具有防火牆的功能（例如：PC-cillin），安裝防毒軟體並設定防火牆功能，也可以杜絕駭客的入侵。

入侵偵測系統：

- 入侵偵測系統（Intrusion Detection System，簡稱IDS）是一種採用隱形保全偵防技術的預警系統（例如：Dragon、RealSecure），可以監控通訊過程是否違反安全機制，並於發生網路危險狀況時，發出警告通知與即時阻止等防護措施。

資訊安全

人人有責

教育體系資訊安全事件案例

教育體系單位	新聞日期	新聞標題	新聞來源	新聞網址
某大學講師	98.09.16	假冒恩師發出求救e-mail 大學講師匯款被騙	中廣新聞網	http://n.yam.com/bcc/society/200909/20090916567932.html
玄奘大學	98.08.09	網po露鳥照 大二生辯研究同志	蘋果日報	http://tw.nextmedia.com/applenews/article/art_id/31848632/IssueID/20090809
大學考試入學分發委員會	98.08.09	同學冒填志願資優生落榜	自由時報	http://www.libertytimes.com.tw/2009/new/aug/9/today-life1.htm
	98.08.09	《大學分發會亡羊補牢》資安不足擬改採自然人憑證	自由時報	http://www.libertytimes.com.tw/2009/new/aug/9/today-life1-2.htm
	98.08.09	冒填志願者明送辦可處刑三年以下	聯合報	http://www.udn.com/2009/8/9/NEWS/NATIONAL/NAT4/5066396.shtml
	98.08.08	明星高中同學交惡冒填志願害他落榜	聯合報	http://mag.udn.com/mag/campus/storypage.jsp?f_MAIN_ID=12&f_SUB_ID=31&f_ART_ID=207257
亞洲大學	98.07.17	女大學生當駭客 改情敵選課	自由時報	http://www.libertytimes.com.tw/2009/new/jul/17/today-so12.htm
義守大學	98.07.17	好玩幫同學退選課 惡作劇生被起訴	TVBS	http://www.tvbs.com.tw/news/news_list.asp?no=aj100920090716131732
國科會	98.06.27	國科會網站洩1.8萬個資 身分證字號學號全都露「離譜」	蘋果日報	http://tw.nextmedia.com/applenews/article/art_id/31742117/IssueID/20090627
台中縣教育處	98.06.01	台灣多所學校師生個資外洩 百度查得到	資安人	http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=4981
	98.05.30	數百教師個資 百度看光光	聯合報	http://mag.udn.com/mag/campus/storypage.jsp?f_ART_ID=196607
台中高農	98.05.06	火燒拍打電擊? 高職生虐鳥PO網	聯合報	http://blog.udn.com/taichungnews/2920138
某高中	98.05.04	分享畢旅全裸照 慘遭破解永流傳	自由時報	http://www.libertytimes.com.tw/2009/new/may/4/today-so9.htm

教育體系資訊安全事件案例

教育體系單位	新聞日期	新聞標題	新聞來源	新聞網址
稻江科技學院、政大	97.11.23	學生個資外洩 稻江、政大急撤網頁	自由時報	http://www.libertytimes.com.tw/2008/new/nov/23/today-life9.htm
彰化縣政府教育處	97.11.19	彰化縣府網站 洩原民學生個資	自由時報	http://www.libertytimes.com.tw/2008/new/nov/19/today-complain2.htm
中興大學	97.10.24	男友的前女友 惡搞我選課 中興大學學姊報復學妹 上網刪除選課資料 觸五年罪刑 學妹不提告「算了吧」	聯合報	http://eteacher.edu.tw/FocusDetail.asp?id=1412
國中基測、高雄縣市及台北縣等多所國中校務系統與網站	97.06.26	基測個資外洩案》竄改3推甄生成績 交換個資	聯合報	http://www.udn.com/2008/6/26/NEWS/SOCIETY/SOC1/4400762.shtml
	97.06.26	17歲駭客 竊80餘所國中個資	中時電子報	http://blog.udn.com/ajwin/1989786
	97.06.25	國中基測考生資料外洩案 高中生駭客涉案	中央社	http://www.epochtimes.com/b5/8/6/25/n2168156.htm
	97.06.25	遭駭客入侵 高市教育局加強網路機密維護	中央社	http://wwwga.epochtimes.com/b5/8/6/25/n2168264p.htm
	97.06.18	基測個資外洩 教育部：制度面確實需檢討	中廣新聞網	http://n.yam.com/bcc/garden/200806/20080618055484.html
	97.06.18	保障國中基測個資 呂木琳:資安認證盡量做	中央社	http://news.chinatimes.com/2007Cti/2007Cti-News/2007Cti-News-Content/0,4521,130503+132008061801141,00.html
	97.06.17	國中基測資料外洩 31萬考生遭販售	資安人	http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=4467
	97.06.14	基測考生個資傳外洩 教部調查	台灣時報	http://www.twtimes.com.tw/html/modules/news/article.php?storyid=10354
	97.06.13	31萬基測考生個資 驚傳外洩	NOWnews	http://www.nownews.com/2008/06/13/545-2289164.htm

教育體系資訊安全事件案例

教育體系單位	新聞日期	新聞標題	新聞來源	新聞網址
台東縣興隆國小	98.04.05	色情入侵教育網站 興隆國小無計可施	資安之眼	http://www.itis.tw/node/2674
某科技大學女學生	98.04.03	轉貼猥褻文章 女大生罰萬元	聯合報	http://tw.myblog.yahoo.com/jw!_otax4eFBQTAWONNaXAPzA--/article?mid=1319&prev=-1&next=1314
彰化縣國中小校長	98.03.21	4校長涉賣10萬學生個資	自由時報	http://www.libertytimes.com.tw/2009/new/mar/21/today-fo2.htm
	98.03.21	何必找校長? 學生個資 2元買得到	自由時報	http://www.libertytimes.com.tw/2009/new/mar/21/today-fo2-2.htm
某大學博士生	98.01.13	PO性愛影片 博士生害博士女友	聯合報	http://blog.urmay.com/index.php/viewnews-15866.html

資料來源:NII協進會 執行長 吳國維