

# 資訊安全與病毒防護

- 網路犯罪
- 電腦病毒
- 資訊安全

台南市安順國中教師資訊素養研習……97/9/23

# 一、網路犯罪

台南市安順國中教師資訊素養研習

# 網路犯罪是什麼？

所謂『網路犯罪』是指利用電腦（網路）技術來從事犯罪的行為。

常見的案例，如：

- ✓ 利用一些非法的手段來竊取重要的資料。
- ✓ 專門在網路上登記知名企業的名稱作為網址，然後再以高價向企業兜售的『網路蟑螂』。
- ✓ 未經授權的複製或使用軟體的盜版行為。
- ✓ 在BBS站上惡意批評毀謗他人。

# 網路犯罪的特性：

網路具有快速傳播、大量傳播、成本低、無距離限制、隱密性高、無實體化等特性。由於網路的普及以致形成了許多新型態的網路犯罪。

- ✓散佈迅速
- ✓身份易藏
- ✓證據有限
- ✓毀證容易
- ✓適法困難
- ✓跨國管轄
- ✓偵查不易

--網路犯罪--

# 常見的網路犯罪行爲：

## ➤ 網路媒介及傳佈色情

例如：設立色情網站、一夜情交易中心、銷售色情光碟影片、利用聊天網站或其他方式進行援助交際、自拍或情色貼圖公然猥褻、散播情色資訊於網路公眾領域

## ➤ 網路販賣違禁、管制物品、盜版光碟、贓物、侵犯他人著作權及商標權

例如：在網路上販賣FM2、搖頭丸、毒品、其他禁藥、賣槍、販賣盜版光碟、贓物、仿冒品、交易偽鈔

## ➤ 教唆他人犯罪

例如：軍火教父、自殺手冊

## ➤ 網路詐欺

例如：網路銷售商品，收錢沒送貨。

網拍（eBay拍賣網）

網路購物（Yahoo! 奇摩購物通）

## ➤ 網路恐嚇

例如：網路千面人。

--網路犯罪--

## ➤ 毀謗侮辱、妨害名譽(偽造文書)

例如：公佈電話、地址、電子郵件帳號、散佈寫真、移植名星照片

## ➤ 駭客侵入與散佈電腦病毒

例如：截取銀行帳號，密碼、截取其他個人隱私資料、金融犯罪、木馬程式、窺伺資料、破壞或移植資料、駭客大戰、散佈電腦病毒。



## ➤ 網路賭博

例如：在網路上架設具有賭博功能之網站，公然煽惑不特定之人上網賭博。

## ➤ 散佈謠言

例如：轉寄未經求證或無事實根據的信件。

## ➤ 其他

例如：惡意程式--搶票程式癱瘓台鐵網路

例如：惡意郵件、惡意網頁（網路釣魚）

--網路犯罪--



# 認識網路釣魚：

網路釣魚多半是利用偽造電子郵件與網站作為「誘餌」，輕則讓使用者不自覺洩漏個人資料，成為垃圾郵件業者的名單；嚴重一點，電腦可能會被植入木馬程式，破壞系統或讓重要資訊遭竊。而最危險的情況是：誘騙使用者的銀行帳號密碼、信用卡號與身分證字號等機密資料，釣魚者再伺機偷竊金錢或有價資訊。

# 網路釣魚常見的幾種方式：

- 包含誤導訊息的彈出式視窗
- 模擬真實網頁網址的 URL 遮罩
- 擷取帳戶名稱及密碼的按鍵記錄程式
- 冒名常出現在線上的知名企業。

# 案例：

機密等級：C

網路釣魚

[www.vvest.com](http://www.vvest.com)

[www.west.com](http://www.west.com)

[www.paypal.com](http://www.paypal.com)

[www.paypal.com](http://www.paypal.com)

--網路犯罪--

# 抵禦網路釣魚：

- ❑ 特別留意詢問機密資訊的電子郵件，尤其是與財務相關的資訊。
- ❑ 網路釣魚的作者喜歡使用恐嚇的手法。例如：他們可能威脅要停用您的帳戶或延誤服務，直到您更新特定資訊，但請勿上當。您可以直接連絡商家，以確認要求的真實性。
- ❑ 不要透過電子郵件訊息內嵌的表單傳送機密資訊。
- ❑ 如果您需要在網路上提交公司信用卡號碼或其他機密資訊，請確認該網站是安全的。
- ❑ 定期檢查您的銀行、信用卡及簽帳卡明細，以確保所有交易都是正當的。若您感到懷疑，請連絡銀行及所有發卡公司。

--網路犯罪--

# 自我保護：

- ✓守密為先

在網路上不要輕易透露自己和家人的個人資料。

- ✓勇敢說不

勇敢的向不良資訊說不，例如色情、暴力、令人噁心的電子郵件、網站資訊等等。

- ✓懶得理你

收到奇怪或陌生的電子郵件、檔案、文字或圖片時，最好不理不睬。

- ✓存疑至上

網路背後的真實身分真偽難辨，自稱「辣妹」者，可能是怪老頭。

- ✓話不投機半句多

在聊天室和網友聊天時，如果出現令你不堪、粗俗等低級不入流的對話時，可以立刻離開。

--網路犯罪--

# 網路交友（二要三不）：

## ✓二要：

- 家長要關心放心。
- 親子要約法三章。

## ✓三不：

- 不私下交往，交友要公開。
- 不單獨與網友見面及提供個人隱私資料。
- 不露相，不要將自己的照片、地址、電話或信用卡、身分證等資料，在網路上洩露給任何人。

--網路犯罪--



# 相關法律規定：

## ◆網路色情：

散布播送販賣製造猥褻物品罪(刑法第235條)。  
兒童及少年性交易防制條例(第28條)。

## ◆線上遊戲虛擬寶物：

無故使用他人帳號、密碼入侵電腦、無故取得、變更、刪除電磁紀錄(刑法第358、359條)。

## ◆網路誹謗與公然侮辱：

公然侮辱罪、誹謗罪(刑法第309、310條)。

## ◆侵害著作權

著作權法相關罰則。



# 相關法律規定：

- ◆網路上販賣毒品禁藥：  
毒品危害防制條例相關處罰。
- ◆網路煽惑他人犯罪：  
煽惑他人犯罪(刑法第153)。
- ◆網路詐欺：  
普通詐欺罪(刑法第339條)。
- ◆網路恐嚇：  
恐嚇危害安全罪(刑法第305條)。
- ◆網路上販賣槍械：  
槍砲彈藥刀械管制條例。

--網路犯罪--

# 相關法律規定：

## ◆網路駭客：

無故入侵電腦、無故取得刪除、變更電磁紀錄、無故干擾他人電腦及製作專供電腦犯罪之程式等行為予以處罰，將電腦安全、電磁紀錄之支配及電腦運作效能等法益正式納入刑法保護。

## ◆損害賠償：

因故意或過失，不法侵害他人之權利，需負損害賠償責任，網路犯罪構成侵權行為，侵權行為一經成立，就得對被害人負損害賠償責任，父母對未成年子女的侵權行為應負連帶賠償責任。

# 相關法律規定：

## ◆網路駭客：

無故入侵電腦、無故取得刪除、變更電磁紀錄、無故干擾他人電腦及製作專供電腦犯罪之程式等行為予以處罰，將電腦安全、電磁紀錄之支配及電腦運作效能等法益正式納入刑法保護。

## ◆損害賠償：

因故意或過失，不法侵害他人之權利，需負損害賠償責任，網路犯罪構成侵權行為，侵權行為一經成立，就得對被害人負損害賠償責任，父母對未成年子女的侵權行為應負連帶賠償責任。

# 案例：

機密等級：C



## 病患資料外洩 健保局:已緊急關閉網站

- 案例：消費者文教基金會指部分病患個人基本資料居然在網頁上「全都露」，中央健保局晚間表示，這個網站並非健保局的資料庫，是健保局試辦論質計酬提升品質改善方案所設置的網站，讓醫師可透過密碼輸入，隨時更新病患資料，不知為何遭到破解讓一般人也可連結，下午已緊急關閉網站。
- 法律意見：刑法第318-1條、個資法第5條、第27條第30條、民法第184條及第195條
- 資安管理：慎選委外廠商、妥善撰擬委外契約條款及政風人員積極參與

• 資料來源：大紀元報 2003/12/24

--網路犯罪--



# 案例：

機密等級：C



## 身家資料全上網 烏龍！

- 案例：某政府機關驚爆洩漏個人資料的大烏龍！一名余姓計程車司機因為車禍案件上網查詢，竟然在搜尋引擎查到自己的詳細資料，而資料來源居然是政府，反應後卻得到「你的權益哪裡受損」，消息曝光後，該政府機關坦承作業疏失，向當事人致歉。
- 法律意見：刑法第318-1條、個資法第4條、第7條、第17條及第27條
- 資安管理：權限設定、資料庫安全管理

• 資料來源：TVBS 2005/06/28

--網路犯罪--

# 案例：

機密等級：C



## 分享軟體闖禍 筆錄上傳外洩

- 案例：警方筆錄驚傳在網路被「上傳」外洩！刑事局發現有員警在公務電腦安裝「FOXY」的P2P分享軟體，想下載影音，卻造成筆錄等公務資料被上傳任人下載，至少有五個縣市警分局、八個派出所的九份筆錄外洩，將追究相關人洩密刑責。
- 法律意見：刑法第318-1條、個資法第27條及第30條
- 資安管理：資安意識、機關內不當軟體的使用、文件控管

• 資料來源：聯合報 2007/04/13

--網路犯罪--

# 案例：

機密等級：C



## 假網頁釣密碼 駭客盜領千萬

- 案例：刑事警察局科技犯罪防制中心發現，兩岸駭客設置俗稱「釣魚網站」的假網頁，並以銀行名義發出數十萬封以「銀行系統轉換，重新登錄」為標題的電子郵件誘使民眾登入，伺機植入木馬程式，竊取網路銀行帳號密碼等個人資料，再轉帳盜領存款。已知有五名網路銀行用戶遭轉帳盜領合計近千萬元。
- 法律意見：刑法第201-1條、第220條、第318-1條、第339-3條、第358條、第359條、著作權法第91條及商標法第61條等
- 資安管理：加強資安意識、手動輸入網址

• 資料來源：聯合新聞網 2007/02/08

--網路犯罪--



# 案例：

機密等級：C



## Freedom駭客程式 作者落網

- 案例：刑事局於2006年8月破獲「Freedom」穿越封鎖線駭客程式案，嫌犯為知名銀行資訊室電腦工程師，聲稱純為友人解決電腦被公司設限、上班時不能上網聊天「打發無聊」的問題而撰寫此程式，不知觸法。由於此程式著重隱藏及穿透防護功能，被認定是有攻擊性的木馬程式，警方依妨害電腦使用罪將他送辦。
- 法律意見：刑法第358條及第362條
- 資安管理：權限管理、電腦盤點、不隨意借用他人使用電腦

• 資料來源：台灣FTP聯盟 2006/08/30

--網路犯罪--

# 案例：

機密等級：C



## 離職員工扮駭客 竊機密搶生意

- 案例：2007年3月刑事局接獲報案，XX科技公司之電腦遭不明人士入侵，竊取該公司重要商業機密等資料。經查為曾任職於該公司之陳姓員工，離職後自行成立與該公司性質雷同的電子商務公司，因商業競爭之故，竊用該公司現任員工帳號、密碼入侵公司資料庫，並取得該公司競標國外廠商訂單，獲利初估超過500萬元。
- 法律意見：刑法第358條、第359條及營業秘密法
- 資安管理：資安意識、稽核檔保存、優質密碼設定

• 資料來源：聯合新聞網 2007/05/26

--網路犯罪--

# 案例：

機密等級：C



## 國內破獲首椿駭客提供資料竊取服務

- 案例：刑事局偵破首起「網路入侵服務」案件。  
一網路駭客集團以破一組帳號密碼3000元，兩組帳號密碼5000元的價格計費，提供客戶盜取密碼、入侵鍵盤紀錄等資料竊取服務。
- 法律意見：刑法第36章等罪
- 資安管理：資安意識、檔案病毒掃描

資料來源：刑事局新聞快訊 2007/01/05

--網路犯罪--



# 案例：

機密等級：C



## 玉山兵推機密 疑被中共駭走

- 案例：據了解，國防大學某主任教官上月違反資訊安全規定，將辦公室使用的USB隨身碟以及內存機密資料，帶回家中，在自家電腦上操作。該隨身碟再被插回到辦公室的電腦，經掃描發現有木馬程式，因而事發。
- 法律意見：刑法第358條及359條
- 資安管理：不正當的檔案存取行為、隨身碟使用的管理

• 資料來源：2007/04/09

--網路犯罪--

# 案例：

## 影音分享小心遭惡意程式感染

音樂，是用來感染人們的生活，而不是電腦。但是最近發現一個感染多媒體檔案的惡意程式，會將多媒體檔案加以修改，使其在播放時要求下載假的解碼器。

它會在檔案中植入惡意程式碼，感染常用的多媒體檔案格式，例如 MP3、WMA 及 WMV 影片檔。這個惡意程式也能夠將 MP2 和 MP3 檔案轉換為 Windows Media Audio (WMA) 格式。當使用者想要播放受感染的檔案時，電腦會顯示彈出式訊息，要求使用者下載某個解碼器以便播放該檔案。可想而知，所下載的檔案只不過是一個惡意程式。

當所謂的「解碼器」安裝之後，使用者必須再次選擇播放同一個檔案，此時就不再出現彈出式訊息，這可能讓使用者以為真的已在系統中安裝了解碼器。但這只是個開頭而已，如果多媒體檔案透過對等 (peer-to-peer) 網路分享時，任何從受感染系統下載音樂或影片檔的人，都暴露在同樣遭到感染的危險當中。

惡意程式已經假冒成多媒體檔案和解碼器，誘騙使用者下載惡意檔案。

--網路犯罪--

# 案例：

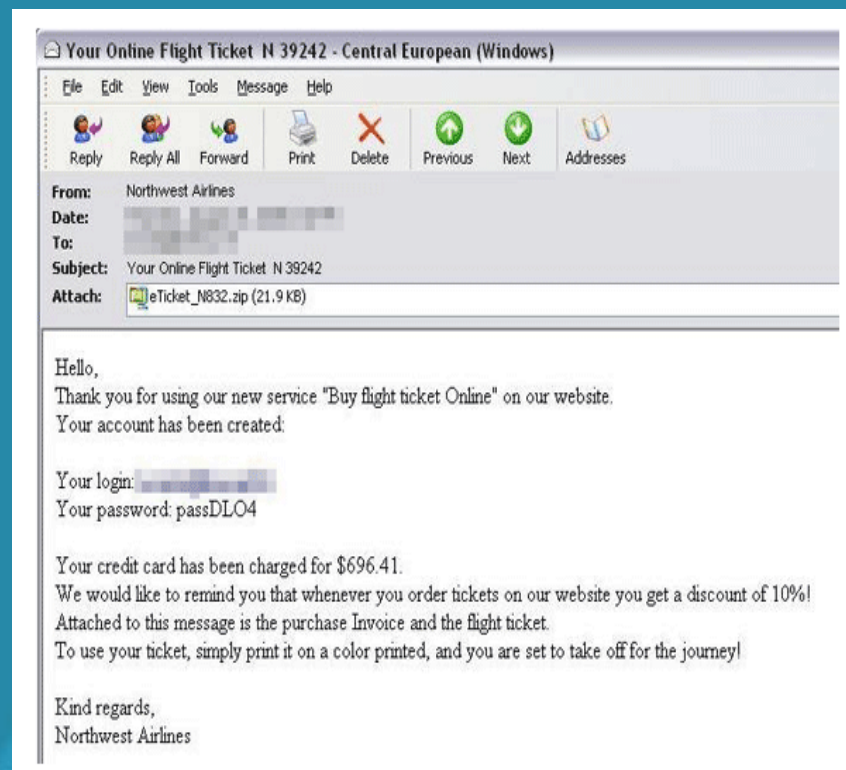
2008毒賣新聞 – 趨勢科技

電子機票耍流氓，強迫付錢買假防毒軟體  
流氓防毒軟體行銷策略愈來愈有創意  
，繼名人露點走光圖、微軟軟體版更新通知、綁架搜尋關鍵字之後，最新的手法是電子機票通知信件。

最近發現一封夾帶惡意程式的垃圾郵件，該郵件偽裝成美國西北航空所發出的電子郵件，信件標題是：

「Your online Flight Ticket N 39242」。這封垃圾郵件宣稱收件者在網路購買的機票已經用信用卡扣款完成，並獲得10%的折扣優惠。其中附件的電子機票並非真的機票，而是惡意程式。

以下就是這封垃圾郵件的畫面擷取圖：



--網路犯罪--



# 案例：

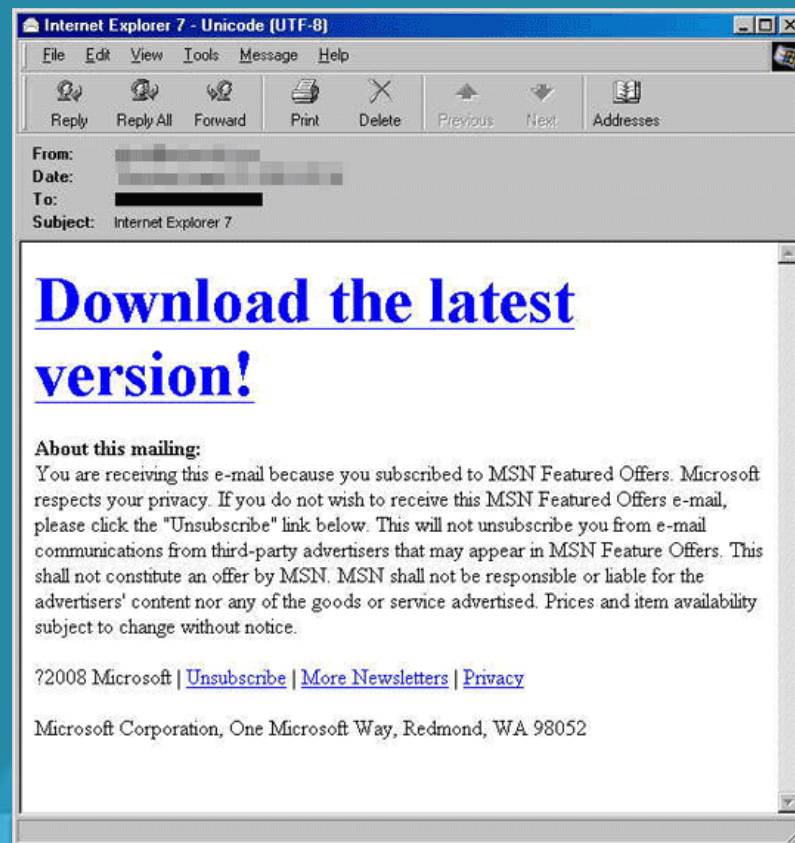
2008毒賣新聞 – 趨勢科技

IE7.0、Yahoo Messenger 最新版本下載，有詐  
網路上出現一些垃圾郵件，分別假冒微軟與 Yahoo 發送Internet Explorer 7.0與Yahoo Messenger最新版本連結。

其中假冒微軟發出的信件，有另一樣本是冒充惡意成是移除工具，以下是這些電子郵件的螢幕擷取畫面：

當使用者按下連結時，就會下載惡意檔案到自己系統上。爲了增加可信度，垃圾郵件作者還新增了一些 MSN Featured Offers 取消訂閱的東西。

另外，有一種垃圾電子郵件使用熱門的即時訊息 (IM) 應用程式 Yahoo! Messenger 來複製惡意程式。



--網路犯罪--



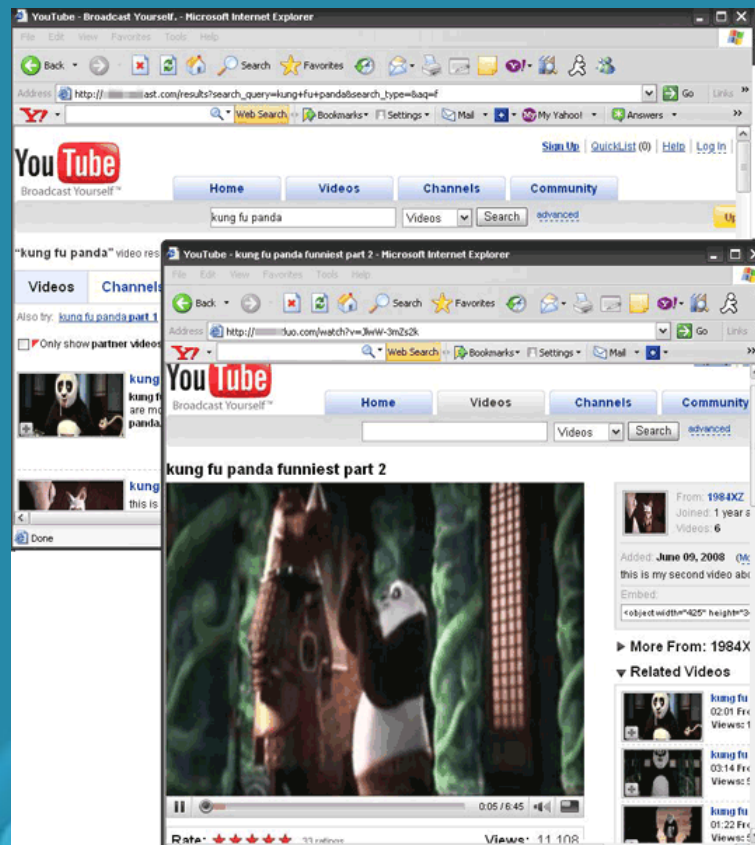
# 案例：

2008毒賣新聞 – 趨勢科技

偽造的 YouTube 網站，可以看功夫熊貓的精彩預告，也可以偷登入者的資料。釣客可能藉此取得 YouTube 使用者名稱及密碼，並使用這些資訊販賣登入資料給廣告商或其他欲增加點擊率的人。

右圖是偽造的 YouTube 視訊網頁螢幕擷取圖，可以看功夫熊貓的精彩預告，也可以竊取登入者的資料。

這個花俏的社交工程手法意味著使用者實際上可以搜尋及觀賞影片，卻不知道自己已經進入惡意網域中。事實上，當使用者最後登入 YouTube 時，瀏覽器會重新導向至真正的 YouTube 網站。



--網路犯罪--

## 二、電腦病毒

台南市安順國中教師資訊素養研習

# 電腦病毒是什麼？

電腦病毒像生物病毒一樣，會自我繁殖增生、會透過接觸傳染，不同之處它是個電腦程式，可以自行執行、自行重製的程式。換句話說，透過一些不合法的指令，病毒自己會傳染給其他的程式或文件。現在的電腦病毒利用網路的無遠弗屆，在短短時間內就有可能進入上網者的電腦，傳染範圍遍及全球，威力更強。

電腦病毒可分為：[開機型病毒]、[檔案型病毒]及[巨集病毒]等等，廣義來說可分為蠕蟲、特洛伊木馬程式。

--電腦病毒--

# 蠕蟲（Worm）：

蠕蟲或稱病蟲，是指某些惡性程式碼會像蠕蟲班在電腦網路中流竄並大量複製，透過系統漏洞或是電子郵件，到另外一台電腦上自我繁殖。入侵的蠕蟲通常會執行惡意的動作，如刪除檔案、存取個人資料，或使用你的電腦攻擊其他電腦。

--電腦病毒--

# 特洛伊木馬程式（Trojan）：

特洛伊木馬程式名稱源自希臘神話特洛伊木馬屠城記，它是個惡意程式，但是偽裝成有用的軟體，例如偽裝成遊戲、解壓縮工具和電子郵件附件等，一旦開啓後，便會產生無法預期的傷害。有些只是煩人的動作，例如傳送電子郵件到通訊錄中的每個人。有些則會造成嚴重破壞，甚至竊取密碼和資料。如神話中所述的一樣，看起來像是一件禮物，其實卻是一些突擊特洛伊城的希臘士兵。

--電腦病毒--



# 防毒軟體介紹：

2007世界防毒軟體排名：

金獎：BitDefender

銀獎：Kaspersky

銅獎：F-Secure Anti-Virus

第四名：PC-cillin

第五名：ESET Nod32

第六名：McAfee VirusScan

第七名：Norton AntiVirus

第八名：AVG Anti-Virus

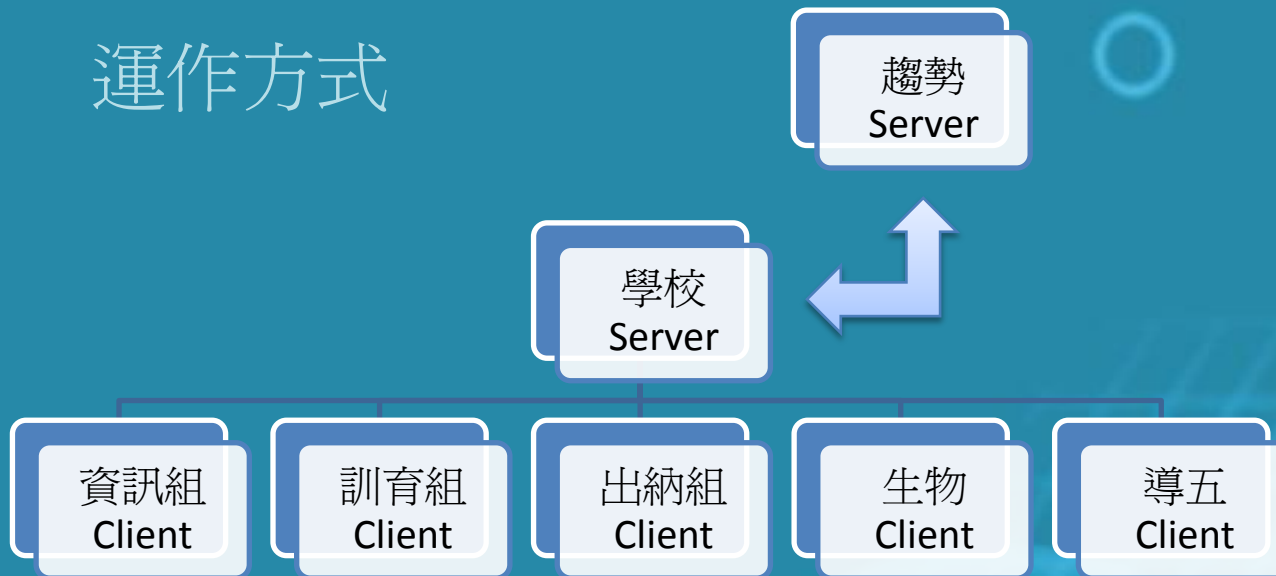
第九名：CA Antivirus

第十名：Norman Virus Control

--電腦病毒--

# 學校的防毒軟體—OfficeScan 8：

## 運作方式



--電腦病毒--



# 安裝 OfficeScan 8 :



The screenshot shows the web interface for Trend Micro OfficeScan 8. At the top, there is a header bar with the 'TREND MICRO OfficeScan' logo on the left and the 'TREND MICRO' logo on the right. The main content area has the 'TREND MICRO OfficeScan' title in large, bold letters. Below the title, a message in Chinese asks the user to enter a password to access the Web console. There is a password input field with a placeholder character 'I' and a '登入' (Login) button. Below this, a light gray box contains a message in Chinese stating that the user can provide a link to the client installation program. The link is provided for the '針對用戶端' (For Client) and is 'https://163.26.14.10:4343/officescan/console/html/ClientInstall/'. At the bottom of the page, a footer line contains the copyright information: '版權所有 © 1998-2007 Trend Micro Incorporated / 趨勢科技股份有限公司。保留所有權利。'.

TREND MICRO OfficeScan

TREND MICRO

**TREND MICRO**  
**OfficeScan**

請輸入密碼以存取 Web 主控台。

密碼：

您可以提供使用者下列用戶端安裝程式連結：

**針對用戶端：**  
<https://163.26.14.10:4343/officescan/console/html/ClientInstall/>

版權所有 © 1998-2007 Trend Micro Incorporated / 趨勢科技股份有限公司。保留所有權利。

--電腦病毒--

# USB防護-- Wow! USB Protector :

中央研究院資訊科學所『自由軟體鑄造場』，於2008年2月釋出 Wow! USB Protector 隨身碟病毒偵測軟體。採用開放原始碼 GPL3 授權，供個人或企業自由使用與研究。

Wow! USB Protector 是一款自動偵測隨身碟是否含有惡意程式的自由軟體。可以偵測出常見的隨身碟病毒，提供即時捕捉隨身碟病毒或可疑程式的功能，是一款輔助防毒軟體的安全工具。目前有繁體中文與英文介面，支援 Windows 2000/XP/2003/Vista 32bit/64bit 作業系統。使用 Ruby 程式語言撰寫、支援系統常駐、自動更新惡意程式病毒碼、合法程式白名單、可疑程式警訊等功能。

--電腦病毒--

# 免費的線上掃毒：

除了在電腦中安裝防毒軟體之外，也可以利用『線上掃毒』服務來防護你的電腦：

✓ 微軟體線上免費掃毒：

<http://onecare.live.com/>

✓ 趨勢線上免費掃毒：

<http://housecall.trendmicro.com/>

✓ 賽門鐵克線上免費掃毒：

<http://security.symantec.com/>

✓ 卡巴斯基線上免費掃毒：

<http://www.kaspersky.com/virusscanner>

--電腦病毒--

# 三、資訊安全

台南市安順國中教師資訊素養研習

# 資訊安全的重要：

隨著電腦運用的普及與網際網路的蓬勃發展，以帶給人類急速而巨大的衝擊，改變了人類生活模式，但也衍生了嚴重的電腦入侵問題，全球正為著充斥電腦駭客而苦。輕者造成使用者和維護者的不便，重者可能會威脅國家安全。

因此，我們必須做好資訊安全防護措施，唯有在確保資訊安全的前提下享受資訊便利，才是面對資訊世紀來臨得正確態度，進而迎接未來更大得挑戰與衝擊。

-- 資訊安全 --



# 資訊安全的種類：

## 一、實體安全：

門禁管制、資訊線路之管制、消防設備、媒體出入管制及災害、設備定期維護等都包括在內。

## 二、資料安全：

檔案保管人與維護人清單、檔案的備份、訂定檔案資料使用權限、檔案機密分級、研討檔案遭損壞之風險接受程度、資料的加密及解密。

# 資訊安全的種類：

## 三、程式安全：

範圍包括已正式啓用的程式及模組的異動管理、個人電腦硬碟使用管理、網路監控管理、終端機使用權限管理、線路及線路接頭控制、密碼的規則與變更期限都包括在內。

## 四、系統安全：

網路作業環境若遭人蓄意破壞，將無法正常發揮作用，因此事先必須詳細規劃並設定好網路使用者所能使用的資源、帳號和密碼，之後也必須時常監控網路環境的變化。

# 資訊安全的威脅：

當網際網路成為資訊大量流通管道，許多令人擔憂的問題也隨之而來，在網路上由於流通廣泛且迅速，因此資訊的正確性、合宜性與私密性都是使用者不安的來源。

- ★駭客侵入電腦系統，竊取或竄改資料甚至更動系統設定。
- ★合法使用電腦人員有意或無心，造成資料的毀損、竊取或系統破壞。
- ★資料在傳輸中被截取、窺竊或變更。
- ★電腦感染與傳遞病毒。

-- 資訊安全 --

# 資訊安全素養：

良好的電腦使用習慣，正確的電腦安全素養，可避免無謂的災難發生。檢驗一下都做到了嗎？

- ✓ 定時的電腦硬體保養與清潔維護。
- ✓ 安裝防毒軟體，每日更新病毒碼。
- ✓ 不隨便下載、安裝不明的程式。
- ✓ 使用帳號權限管理電腦與文件加密。
- ✓ 自動執行作業系統更新（ Windows update ）。
- ✓ 瀏覽器的安全層級與隱私設定。
- ✓ 啓用防火牆，並依個人需求來設定。
- ✓ 定時的備份資料。
- ✓ 注意資訊安全新聞，學習新的知識與技術。

-- 資訊安全 --

# 帳戶權限管理：

開始/控制台/使用者帳戶



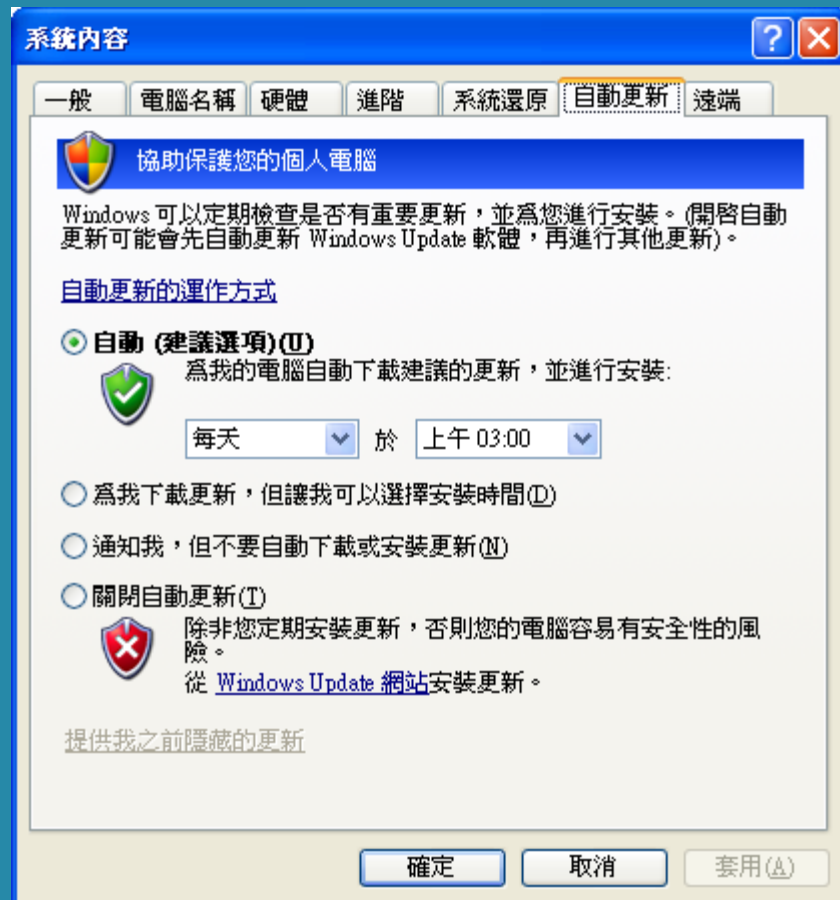
-- 資訊安全 --



# Windows Update：

在『桌面』找到『我的電腦』  
我的電腦按右鍵選擇『內容』

在『自動更新』頁籤中  
選擇『自動』或選擇『為我下載更新』



--資訊安全--

# 安全性設定：

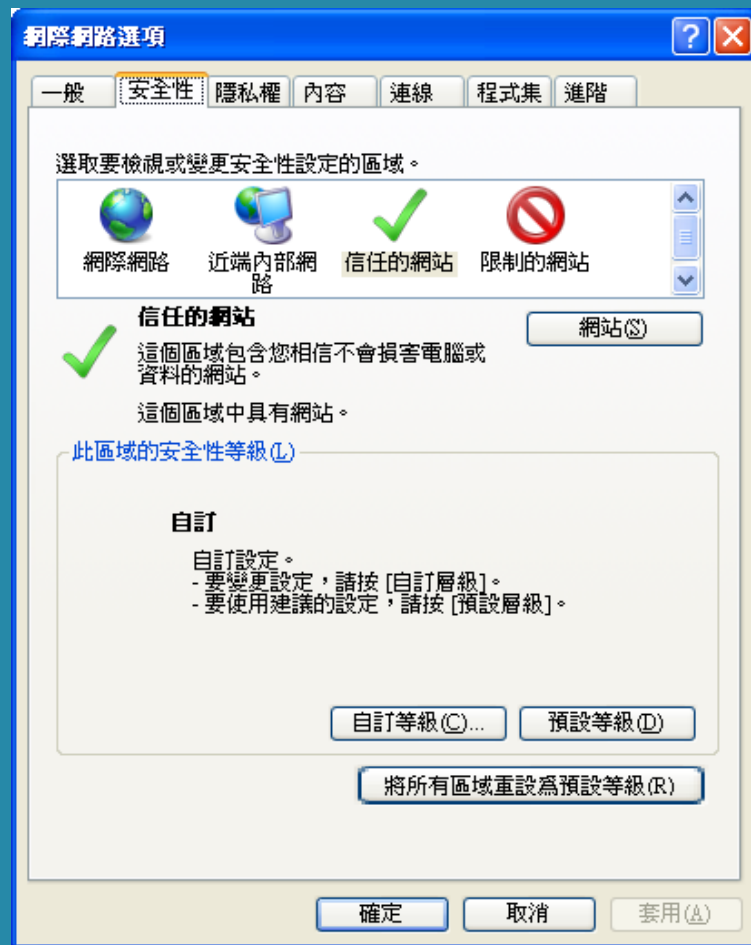
瀏覽器/工具/網際網路選項

在『安全性』頁籤中  
設定『網際網路』的安全性等級

選擇『信任網站』

可以『新增信任網站』

如：<http://edit.good.nat.gov.tw>  
<https://ebank.bot.com.tw>



--資訊安全--

# 認識防火牆（ Firewall ）：

『防火牆』的功用像是學校警衛，在出入口做進出管制。它可以做成硬體網路設備，放置網際網路出入連結點（亦稱為閘道），管制網路連線、保護不當內部網路與電腦。也有安裝在個人電腦的防火牆軟體，可以保護電腦、限制不當連線、防範非法入侵。

需要設定一些規則，然後『防火牆』根據設定來決定，是否將網路的資訊阻絕或允許它進入你的電腦。

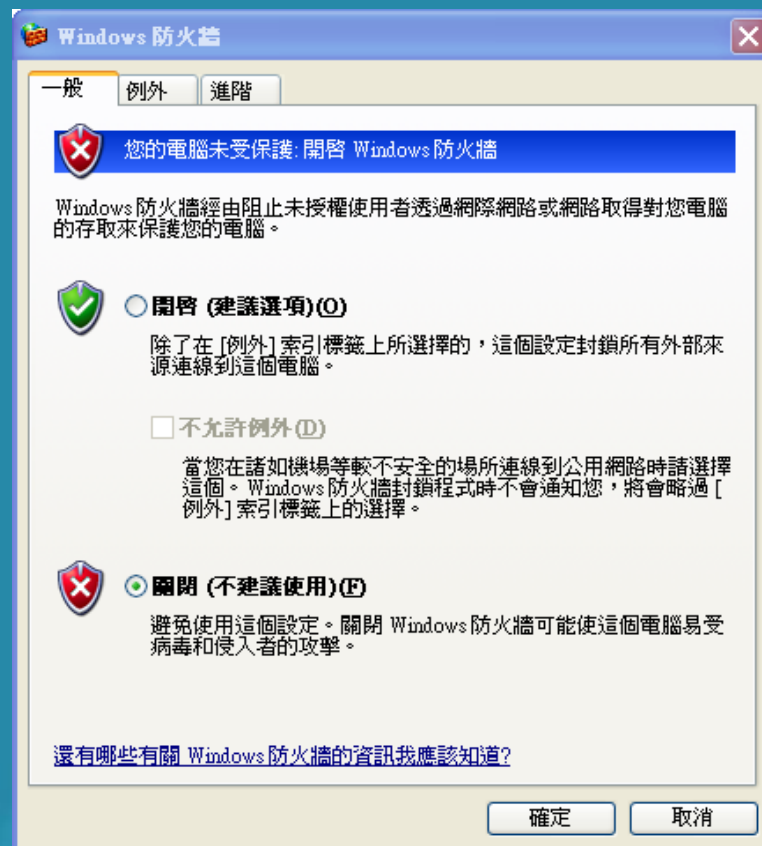
# 個人防火牆設定：

控制台/資訊安全中心/Windows防火牆

在『一般』頁籤中  
開啓『防火牆』

在『例外』頁籤中  
設定你要開放的『程式和服務』

在『進階』頁籤中  
設定『新增其他的連線』



-- 資訊安全 --

# 資訊隱私權：

資訊隱私權[Information Privacy]泛指個人或公司型號拒絕或限定收集和使用他們資訊的權利。

網路世界的浩瀚，往往讓使用者誤以為自己是隱形的。事實上在網路使用過程中，每一個路徑都會被記錄下來，例如電子郵件在傳送和接收過程中，可能會被暫存、截取或是轉送。因此，[保密防諜]之心不可無。

-- 資訊安全 --



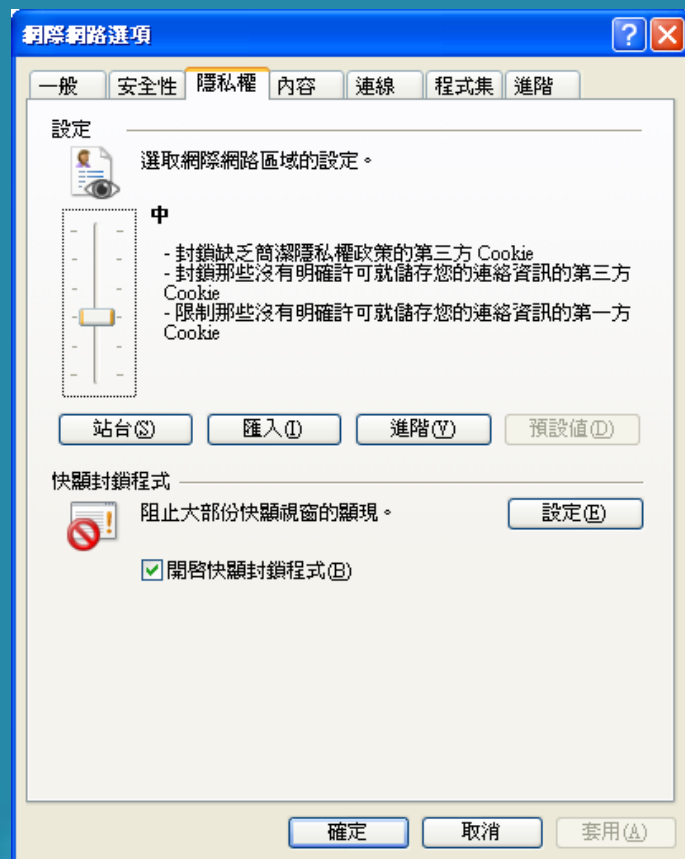
# 隱私權設定：

瀏覽器/工具/網際網路選項

在『隱私權』頁籤中  
設定『允許』或『封鎖』的站台清單

開啓『快顯封鎖程式』  
可以設定『允許快顯得網站清單』

如：\*.tn.edu.tw  
\*.nat.gov.tw  
\*.k12.edu.tw



--資訊安全--

# 資料備份：

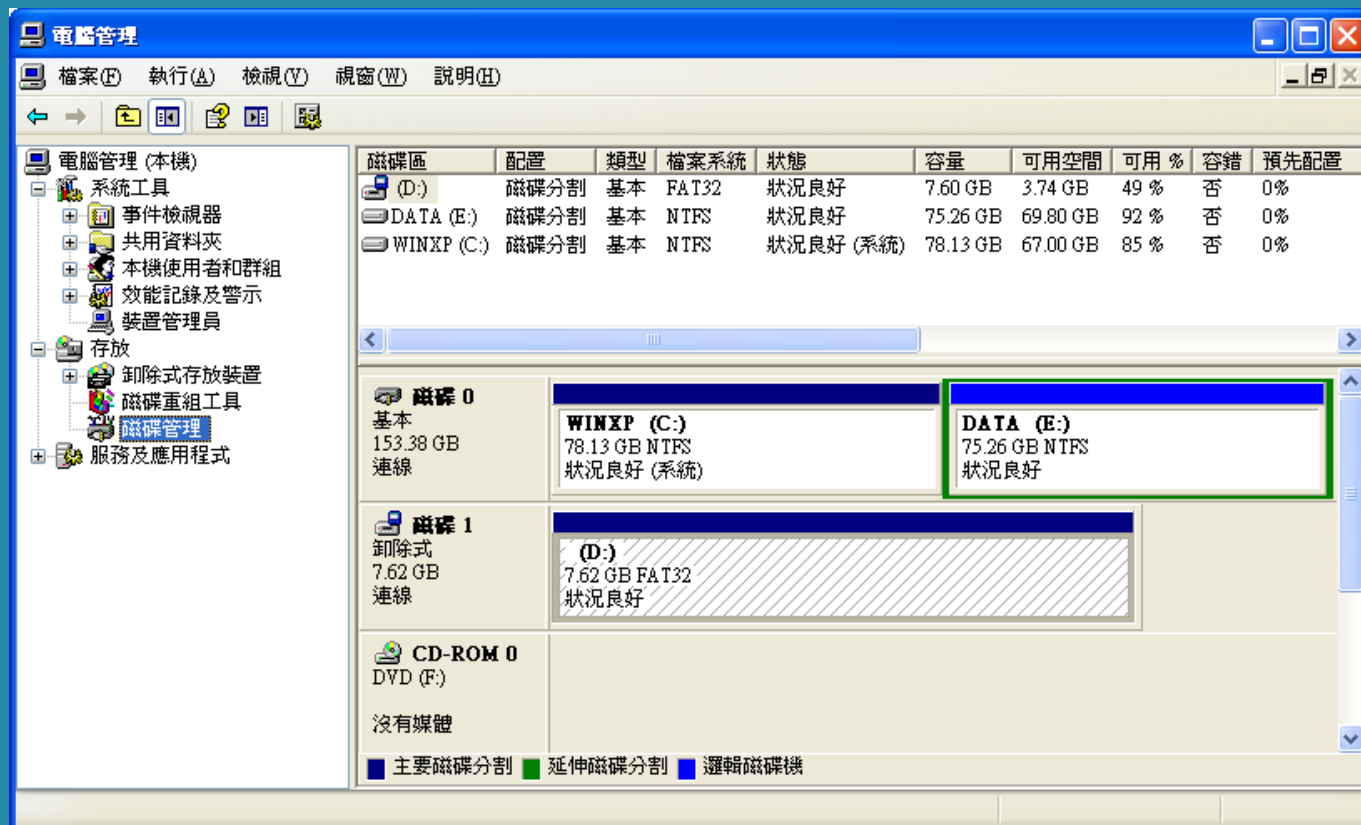
資料備份，顧名思義就是將相同的資料儲存兩份以上。如果沒有經常的備份檔案，就有檔案遺失的風險。將硬碟的資料備份到其他磁碟上，在一般的情況下，並不會耗掉太多的時間。任何一種儲存媒介如硬碟、隨身硬碟、隨身碟、光碟等都有缺點，儲存資料的安全性不可能百分之百，而平常勤於備份就可以降低這個風險。

# 備份的方法：

- ✓ 使用Windows XP系統內建的『製作備份』工具軟體。
- ✓ 使用Ghost或其他工具來製作映像檔。
- ✓ 重要資料應該異地備份。
  - 一般來說會將硬碟分割為C和D兩個分割區
  - C：為系統安裝區    D：為資料存放區
  - 異地備份：將資料另存於隨身(硬)碟、網路硬碟、光碟片.....

# 電腦管理：

在『桌面』找到『我的電腦』按右鍵選擇『管理』



--資訊安全--

# 參考資料：

- 內政部警政署刑事警察局
- 台北市政府警察局少年警察隊
- 資訊教育（台灣出版社）
- 資訊教育（勁園文化）
- 國中新電腦（巨岩校園文化）
- 國家資通安全會報技術服務中心
- 趨勢科技（<http://tw.trendmicro.com/>）