

壹、課程說明

單元名稱	網路安全攻防戰
單元摘要	在網際網路蓬勃發展的今日，上網已成為現代人生活的一部份。雖然網路科技為人們的生活帶來了許多便利，但也連帶的產生了不少網路安全的問題。本單元將探討近年來受到大眾關切的線上交易安全、垃圾郵件、電腦駭客、網路釣魚及電腦病毒等網路安全議題。
設計者	林明璋 老師（國立北門高級中學）
學習目標	<ol style="list-style-type: none"> 1. 瞭解維護資訊安全的重要性。 2. 瞭解網路應用可能衍生的安全性問題。 3. 瞭解網路安全的防護概念。 4. 能運用網路安全防護工具進行防護。
課綱範圍	網路安全問題與防護
教學節數	6 節（300 分鐘）
先備知識	<ol style="list-style-type: none"> 1. 電腦作業系統的概念 2. 電腦應用軟體的基本操作 3. 區域網路的概念 4. 網際網路架構 5. 網際網路的應用服務
教學活動	觀賞影片、分組討論、實務操作練習、作業報告 （詳見教學活動計畫）
評量方法	<ol style="list-style-type: none"> 1. 分組報告 2. 課堂觀察 3. 上機實作 4. 作業報告
參考資源	<p><u>書籍</u></p> <p>➤ 電腦叛客(Cyberpunk)(1994)。原著：Katie Hafner、John Markoff</p>

／譯者：尚青松。天下文化

- 捍衛網路(1996)。原著：Clifford Stoll／譯者：白方平。天下文化。
- 系統與網路安全(2003)。謝續平等。行政院國家科學委員會科學技術資料中心。
- PC 防毒/防駭急救手冊(2002)。鮑友仲。學貫行銷股份有限公司。
- 網路安全應用實務(2006)。梁仁楷/嚴楓琪。網奕資訊。
- 電腦病毒技術分析與防範(2007)。韓筱卿、王建鋒、鍾瑋。松崗電腦圖書有限公司。
- 駭客攻防技術擂台(2007)。程秉輝/John Hawke。旗標出版股份有限公司。
- Windows 網路釣魚、側錄、間諜、詐騙、毒駭(2007)。程秉輝/John Hawke。旗標出版股份有限公司。

網站資源

- 【網路安全】<http://infotrip.ncl.edu.tw/law/security.html>
- 【網路安全診斷】<http://www.symantec.com/tw-ssc/>
- 【毒賣新聞】
<http://tw.trendmicro.com/tw/threats/vinfo/weeknews/>
- 【行政院國家資通安全會報（技術服務中心）】
<http://www.icst.org.tw>
- 【資安論壇】<http://forum.icst.org.tw/phpBB2/>
- 【國家資通安全通報應變網站】<https://www.ncert.nat.gov.tw/>
- 【國研院資通安全資訊網】<http://ics.stpi.org.tw/>
- 【行政院國家資通安全會報】
<http://www.nicst.nat.gov.tw/index.php>
- 【台大資通安全服務小組】<http://cert.ntu.edu.tw/>
- 【資安人科技網】<http://www.isecutech.com.tw/>

	<ul style="list-style-type: none"> ➤ 【清華大學資通安全篇】 http://net.nthu.edu.tw/security/ ➤ 【I Security 網路資訊安全健檢】 http://www.i-security.tw/default.aspx ➤ 【Microsoft 電腦網路安全基礎影片】 http://www.microsoft.com/taiwan/athome/security/videos/default.msp ➤ 【教師網路素養與認知網】 http://eteacher.edu.tw/default.asp
--	--

貳、教學活動計畫

教學活動	時 間	說 明
一、引起動機		
1. 播放影片 2. 針對討論題綱分組進行討論 3. 分組討論後繳交討論報告	15 分	<p>播放[網路上身]電影片段，說明網路資訊安全的重要性，並引發學生對資訊安全的興趣。</p> <p>【劇情簡介】：</p> <p>「網路上身」是一部以人類過度依賴電腦，以至於和周圍環境嚴重隔離的故事架構而發展出來的驚悚片。</p> <p>珊卓布拉克在片中飾演一個害羞內向的電腦程式分析師安琪拉，不和親戚朋友往來的她，是在家中工作的 SOHO 族，平常與外界的聯繫，完全憑靠個人電腦。</p> <p>一次工作完畢後，安琪拉在無意間下載了有關地下恐怖份子組織的磁碟片，裏面儲存了重要的致命資訊。毫不知情的安琪拉帶著磁片，前往墨西哥度假，在異國浪漫氣息濃厚的外地，和一名英俊的男子墜入情網，兩人在海上出遊的時候，這名神秘男子卻對安琪拉展開殺機。</p> <p>逃回都市的安琪拉發現自己所有『存在』的資料和證明，都被另一個陌生女子冒名頂替了，唯一能證明她身份的心理醫生，也在和她會面之後被暗殺了。</p> <p>處境危險而展開逃亡的安琪拉，因為恐怖份子捏造了一個犯罪紀錄的身份，逼得她無處可逃。現在，她必須運用自己的電腦長才，想出一套足以擊敗對方，而且重新奪回原來的生活和身份的致勝絕招……</p> <p>分組討論：(可參考下列討論題綱)</p> <ol style="list-style-type: none"> 1. 為什麼資訊安全會日益重要？ 2. 如何保護個人網路隱私權問題？ 3. 電腦病毒的困擾？ <p>【網路隱私權討論區】</p> <p>http://www.als.org.tw/forum/forum_sg.asp?id=18</p>

二、討論並列舉常見的網路安全事件		
1. 將學生分組 2. 上網查詢網路安全問題及事件 3. 分組進行討論 4. 列舉分組所收集到的網路安全事件的相關報導 5. 繳交新聞事件彙整報告	20 分	<p>分組上網查詢相關主題之網路安全問題與事件，依電腦病毒、垃圾郵件、駭客攻擊、間諜軟體、及網路蠕蟲、釣魚網站、及 P2P 下載安全等主題分組進行蒐集資料並進行小組討論。</p> <p>【參考網址】：</p> <ul style="list-style-type: none"> ➤ 毒賣新聞： http://tw.trendmicro.com/tw/threats/vinfo/weeknews/ ➤ 行政院國家資通安全會報（技術服務中心）： http://www.icst.org.tw ➤ 資安論壇：http://forum.icst.org.tw/phpBB2/ ➤ 國家資通安全通報應變網站： https://www.ncert.nat.gov.tw/ ➤ 國研院資通安全資訊網：http://ics.stpi.org.tw/ ➤ 行政院國家資通安全會報： http://www.nicst.nat.gov.tw/index.php ➤ 台大資通安全服務小組：http://cert.ntu.edu.tw/ ➤ I Security-輕鬆學資安【資安小撇步】： http://www.i-security.tw/learn/tips_list.asp?L=1 <p>網站內容提供案例事件的防範或解決方法，或相關法律建議。內容主要分為網路安全、人員與實體安全、系統安全、以及資料與存取安全四大類。</p>
三、網路應用服務所衍生的網路安全問題		
1. 介紹電腦病毒的危害並探討相關新聞事件。 2. 介紹駭客攻擊的危害並探討相關新聞事件。 3. 介紹間諜軟體的危害並探討相關新聞事件。 4. 介紹網路蠕蟲的危害並探討相關新聞事件。 5. 介紹釣魚網站的危害並探討相關新聞事件。 6. 介紹垃圾郵件的危害並探討相關新聞事件。 7. 介紹資料洩密的危害並探討相關新聞事件。		
1. 介紹電腦病毒的危害	10 分	<ul style="list-style-type: none"> ➤ 電腦病毒 <p>【介紹說明】—</p>

<p>2. 觀看預防病毒影片說明</p> <p>3. 探討新聞事件</p>		<p>電腦病毒在技術上來說，是一種會自我複製的可執行程式。在真實的世界中，大部份的電腦病毒都會有一個共通的特性－它們通常都會發病。當病毒發病時，它很可能會破壞硬碟中的重要資料，有些病毒則會重新格式化（Format）硬碟。就算病毒尚未發病，它也會帶來不少麻煩。首先病毒可能會佔據一些系統的記憶空間，並尋找機會自行繁殖複製，電腦效能將會變得比一般正常的電腦慢。</p> <p>自從 Internet 盛行以來，Java 和 ActiveX 的網頁技術逐漸被廣泛使用，一些有心人士於是利用 Java 和 ActiveX 的特性來撰寫病毒。以 Java 病毒為例，Java 病毒它並不會破壞硬碟上的資料，可是若使用瀏覽器來瀏覽含有 Java 病毒的網頁，Java 病毒則可能強迫 Windows 不斷的開啟新視窗，直到系統資源被吃光為止，最後也只有選擇重新開機一途了。所以在 Internet 革命以後，電腦病毒的定義就更改為只要是對使用者會造成不便的這些不懷好意的程式碼，就可以被歸類為病毒。</p> <p>【影片觀賞】－</p> <p>預防病毒與蠕蟲：了解病毒與蠕蟲會如何侵害您的電腦，並學習保護自己遠離電腦病毒的三大方法。MS_Video\virus.exe（來源：微軟）</p> <p>【新聞案例探討】－</p> <ul style="list-style-type: none"> ● 1999/04/26：CIH 病毒，又稱車諾比（Chernobyl）病毒，在 1998 年開始出現，透過感染檔案和檔案的分享進行散佈，並在每月的 26 日發作，刪除硬碟資料並破壞 BIOS。 ● 1999/03：梅莉莎病毒(Melissa)是第一隻會在企業網路中作怪的病毒。它會在 email 中加入寄件者熟人的名字作為偽裝。一旦 Outlook 軟體使用者開啟郵件後，該病毒便會自動從使用者聯絡簿中挑出 50 位收件人寄發毒信。造成全球受損金額高達 8000 萬美元，該病毒不會造成重大損害(不會刪除檔案)，但由於大量散播郵件導致許多系統當機。 ● 2005/8/11：針對微軟安全漏洞進行攻擊的新型線上病毒--幽靈病毒(WORM_ZOTOB.A)，在 8 月中旬，大舉入侵歐美，造成百餘件感染案例。幾天內，幽靈病毒不但變種到第四代，還迅速蔓延到亞洲，導致台灣與中國大陸共數十家企業遭感染。 ● 2007/11/23：近來越來越多隨身碟感染 USB 病毒事件，電腦無法開啟隨身碟…。除了隨身碟插入電腦後，無法從我的電腦中直接開啟，類似的情況還包括無法在我的電腦中點選
---------------------------------------	--	--

		硬碟進入、隨身碟出現 RECYCLER 資料夾、硬碟根目錄中出現 autorun.inf 檔案等等。
1. 介紹電腦駭客攻擊的流程 2. 影片欣賞：如何保護電腦上網的安全性 3. 探討駭客攻擊的新聞事件	10 分	<p>➤ 駭客攻擊</p> <p>【介紹說明】—</p> <p>駭客，它是英文 hacker 的中譯。基本上，駭客是利用存在於各類系統上的軟體或硬體弱點來入侵電腦。而「入侵」則表示下列三種情況之一：存取儲存在電腦中的資訊；暗地使用電腦的資源（如濫發垃圾信）；或是攔截在電腦系統之間傳送的資訊。</p> <p>駭客入侵系統的流程（請參考附件）</p> <p>【影片觀賞】—</p> <p>安全性概觀：學習如何改善電腦與線上個人資訊的安全性。 MS_Video\security.exe（來源：微軟）</p> <p>【新聞案例探討】—</p> <ul style="list-style-type: none"> ● 2000/3：駭客利用 DDos 的網路攻擊方式，引起 Yahoo、Amazon、CNN、eBay 等知名網站癱瘓 ● 2001/7：Amazon.com 旗下的 Bibliofind 遭駭客盜走顧客的信用卡資料 ● 2005/04：大考中心和國中基測電腦系統連續三年遭蘇姓電腦駭客入侵，竊取一百多萬筆考生資料，燒錄成光碟，轉賣給補習班。 ● 2005/05：某國小沈姓資訊組長利用學校 IP 透過某大學的代理伺服器連結，進入教師介聘作業系統，擅自修改積分與介聘分發志願相關資料。 ● 2006/2/25：就讀桃園縣某高中二年級的黃姓學生，涉嫌設計電腦鍵盤側錄程式，供劉姓主嫌植入他人電腦，以側錄並竊取線上遊戲玩家的帳號與密碼，共計有上千筆資料遭側錄。
1. 介紹間諜軟體對電腦的影響 2. 觀看保護電腦遠	10 分	<p>➤ 間諜軟體（木馬程式）</p> <p>【介紹說明】—</p> <p>所謂「間諜軟體」是一個統稱，泛指會在未經使用者同意</p>

<p>離間諜軟體的影片說明</p> <p>3. 探討間諜軟體引發的新聞事件</p>		<p>的情況下進行廣告、收集私人資訊，或修改電腦設定等行為的軟體。間諜軟體在未知會或者未經使用者同意的情況下被安裝，可能會帶來資料洩漏的威脅。它們與病毒或蠕蟲不同，病毒或蠕蟲會施展廣泛攻擊及對主機和網路造成明顯的損害，間諜程式有時只會靜靜地隱藏在電腦中，而且不易被系統保護程式如防毒程式偵測到。</p> <p>間諜程式主要功能是收集電腦或開放式網路上的資料，然後透過網路傳送給第三者。這些資料可能是在硬碟內的檔案或個人資料，如在網路銀行網站輸入的登入名稱及密碼。</p> <p>【影片觀賞】—</p> <p>保護您的電腦遠離間諜軟體：</p> <p>了解關於間諜軟體是什麼，電腦可能被入侵的管道，入侵的徵兆，以及您能預防間諜軟體的三件事。MS_Video\Spyware6.exe (來源：微軟)</p> <p>【新聞案例探討】—</p> <ul style="list-style-type: none"> ● 1991：間諜軟體真正用於戰爭是在 1991 年的海灣戰爭中。開戰前，美國中央情報局派特工到伊拉克，將其從法國購買的防空系統使用的印表機晶片換上了植入間諜軟體的晶片。在戰略空襲前，又用遙控手段啟動了該間諜軟體病毒，致使伊防空指揮中心主電腦系統程式錯亂，防空系統的 C3I 系統失靈。 ● 1999：科索沃戰爭中，南軍聯盟使用多種間諜軟體實施網路攻擊，使北約軍隊的一些網站被垃圾資訊阻塞，造成電腦網路系統一度癱瘓。隨後，北約一方面強化網路防護措施，另一方面實施網路反擊戰，將大量反間諜軟體注入南軍電腦網路系統，致使南軍防空系統癱瘓。 ● 2003/01：印度和巴基斯坦兩國駭客以間諜軟體為武器展開激烈的網上“廝殺”，結果殃及全世界 100 多個國家的數十萬台電腦。 ● 2006/11：美國海軍學院電腦系統因遭間諜軟體攻擊而全面癱瘓，最終迫使該學院切斷網路服務數周之久。美軍聲稱，本次病毒入侵的目的是竊取美海軍演習的秘密資料。
<p>1. 介紹電腦蠕蟲的危害</p>	<p>10 分</p>	<p>➤ 網路蠕蟲</p> <p>【介紹說明】—</p> <p>電腦網路蠕蟲為一獨立程式（或程式集），其可進行自我</p>

<p>2. 觀看預防電腦蠕蟲影片說明</p> <p>3. 探討網路蠕蟲的新聞事件</p>		<p>複製，並透過網路連線、電子郵件附件、即時通訊（透過檔案共享應用程式），以及與其他惡意程式協同運作等方式散佈到其他電腦系統。有些網路蠕蟲亦可能讓您無法存取安全的網站，或是竊取已安裝遊戲和應用程式的使用授權。</p> <p>網路蠕蟲利用軟體漏洞，並以迅雷不及掩耳的速度發動攻擊，造成網路癱瘓無法運作及財務嚴重的損失，現今的蠕蟲攻擊隱藏著電腦犯罪行為，可能導致遠端使用者取得特定機器的主控權，進而利用該機器使用者的權限發動任意程式碼攻擊，或者竊取機密資料。</p> <p>【影片觀賞】—</p> <p>預防病毒與蠕蟲：了解病毒與蠕蟲會如何侵害您的電腦，並學習保護自己遠離電腦病毒的三大方法。MS_Video\virus.exe（來源：微軟）</p> <p>【新聞案例探討】—</p> <ul style="list-style-type: none"> ● 1988：Morris Worm 的攻擊事件，感染大量網際網路的主機。 ● 2001：CodeRed 蠕蟲更是令人震撼，在九小時內便攻擊 25 萬台主機，損失金額估計超過 20 億美元。 ● 2006/2/1：有位公司員工遭受電腦蠕蟲「WORM_GREW A」、「Nyxem」、「BlackMal」、「Mywife」的攻擊，該蠕蟲是透過電子郵件附加檔案、以及目前最受歡迎的 P2P 軟體所傳遞。蠕蟲發作時，刪除了他電腦內的重要公司文件，包括 WORD 文件、簡報檔案、PDF 等類型的檔案，無一倖免；更可怕的是，該蠕蟲能夠讓電腦的鍵盤及滑鼠無法動作，因此該名職員只能眼睜睜地看著重要文件檔案流失。
<p>1. 介紹釣魚網路的手法</p> <p>2. 網路釣魚引發的網路詐騙事件</p> <p>3. 影片觀看：了解網路詐騙須知</p> <p>4. 探討網路釣魚引發的新聞事件</p>	<p>10 分</p>	<p>➤ 釣魚網站</p> <p>【介紹說明】—</p> <p>網路釣魚，用一句話來形容最為貼切：「姜太公釣魚－願者上鉤」。Phishing 是模仿真實網站（例如讓網站看來像是「正常」的企業網站）所發出的電子郵件，以帳戶到期或出現重大問題要求確認等理由，欺騙使用者連結到電子郵件中由駭客偽造的網站。</p> <p>這些 Phishing 網站通常會唯妙唯肖地模仿合法的網站，部份網站甚至還有安全認證，讓使用者不易分辨出它的真假。通常這種 phishing 網站會向使用者要求一些之前就已提供給銀行做為身份認證用的資料，讓使用者填寫個人機密資</p>

<p>5. 真假網站大考驗</p> <p>看看釣魚網站的 實際範例</p>	<p>料，像是銀行帳號、身份證字號、出生年月日或帳戶密碼等。駭客取得這些機密資料後，就可進行後續的轉帳或其他惡意行為，造成使用者莫大的損失。</p> <p>網路騙術並不僅止於此，近來從 phishing 又衍生發展出更新更高段的詐騙招術－網址嫁接 (pharming)。</p> <p>Pharming 最早約莫出現在 2004 年，它藉由入侵 DNS (Domain Name Server) 的方式，將使用者導引到偽造的網站上，因此又稱為 DNS 下毒(DNS Poisoning)。Domain Name Server 的功能是將網址 (例如：www.google.com)，轉換成網站的 IP 位址 (例如：111.222.33.44)，一旦 DNS 被入侵，使用者便經 DNS 的 IP 轉換，不知不覺地被「導引」到一個偽造的網站，並讓駭客有機會竊取個人的機密資料。</p> <p>Pharming 和網釣同樣是利用假造電子郵件欺騙使用者造訪偽造的網站。兩者不同之處是，Pharming 採用了更高段的手法，讓使用者更難感覺出網站是偽造的。</p> <p>【影片觀賞】－</p> <ul style="list-style-type: none"> ● 網路詐騙須知：了解網路詐騙訊息如何使您受騙並傳送個人資料，以及保護自己遠離因網路詐騙而受騙的三種方法。 MS_Video\Phishing8.exe(來源：微軟) ● 保護您的線上隱私權：網際網路使您能方便地在線上購物、銀行交易與通訊，但也讓您面臨身分被竊的風險。只要採取一些基本的預防措施，就可以降低成為受害者的機率。 MS_Video\Privacy.exe(來源：微軟) <p>【新聞案例探討】－</p> <ul style="list-style-type: none"> ● 2004：一個德國的少年綁架了 Google.de。 ● 2005/01：紐約一家 ISP 公司 Panix 的網址，就嫁接到位於澳洲的網站。 ● 2007/04/03(內政部警政署刑事局新聞稿) 犯罪集團利用新型網路釣魚之方式，以假資料註冊與國內知名網路銀行、航空公司、旅行社、人力銀行、電腦科技公司等極為類似之網址，再於各大搜尋引擎公司購買關鍵字廣告，讓不知情的民眾點選連結至藏有木馬程式之網頁內，俟民眾電腦遭植入木馬程式後，隨即連結至正常之網站，使民眾受害後仍不自知。由於該木馬程式具有鍵盤側錄以及檔案竊取的功能，經刑事局調查後，已有民眾網路銀行、網路拍賣、網路遊戲等帳號、密碼以及金融轉帳之交易憑證檔案等資料遭盜，粗估損失即達數千萬元，受害情形嚴重。
---	---

		<p>【真假莫辨範例(釣魚網站)】—</p> <ul style="list-style-type: none"> ● Emule(假)：http://www.emule.org ● Emule(真)：http://www.emule-project.net ● 土地銀行(假)：http://www.landbank.com.tw ● 土地銀行(真)：http://www.landbank.com.tw ● Yahoo 拍賣(假)：http://tw.bids-yahoo.com/ ● Yahoo 拍賣(真)：http://tw.bid.yahoo.com/
1. 介紹垃圾郵件的 氾濫 2. 觀看處理垃圾郵件的影片說明 3. 討論發生垃圾郵件的重大新聞	10 分	<p>➤ 垃圾郵件</p> <p>【介紹說明】—</p> <p>將一份內容相同的電子郵件，未經收信人許可，大量寄給很多人。郵件內容多數是與收信人不相干的商業廣告。由於短時間內寄發大量郵件，常常造成系統負擔過重，導致收信人需花費金錢時間去處理這些垃圾郵件。</p> <p>【影片觀賞】—</p> <p>處理垃圾郵件：了解垃圾郵件的來源，哪一類的垃圾郵件訊息可能是危險的，以及您該如何做以協助減少您所收到的垃圾郵件。◦MS_Video\Spam6.exe(來源：微軟)</p> <p>【新聞案例探討】—</p> <ul style="list-style-type: none"> ● 2006/6/12：達文西密碼的電影上映，在全球造成了一股旋風，垃圾郵件業者也搭起了順風車，各種達文西密碼相關主題的垃圾郵件肆虐，例如主旨為『Get the Da Vinci Code on us』的郵件，會邀請收件人參加讀書俱樂部，並表示提供免費小說，誘使收件人上當。而參加了此類俱樂部並不會真的得到免費禮物，反而可能造成個人資料的外洩。 ● 2007/5/14：溫馨的 5 月母親節也成了垃圾郵件與病毒散佈者利用的對象，各式各樣以「母親節」為主題的垃圾郵件充斥氾濫，像網路訂花服務、母親節禮品購物網站廣告等。部分垃圾郵件甚至夾帶電腦病毒、或以偽裝成大型購物網站的連結騙取使用者密碼、銀行帳號等隱私資訊…
1. 介紹 P2P 下載的原理	10 分	<p>➤ P2P 下載 (Foxy、Emule、BT) 造成的資料洩密問題</p>

2. 探討 P2P 引發的洩密實際新聞事件		<p>【介紹說明】—</p> <p>P2P (peer to peer) 利用點對點分散式網路架構傳輸型態進行網路資源分享，下載檔案的同時也提供他人下載檔案。它讓使用者可以直接連接到其他使用者的電腦，進行文件的共用與交換，但也因為這樣的特性，使得資料洩密的風險大增。常見的 p2p 軟體如 BT、Emule、Ezpeer、Kazza、eDonkey 等。</p> <p>【新聞案例探討】—</p> <ul style="list-style-type: none"> ● 2007/05：警方人員因為對電腦資訊欠缺警覺，使用點對點分享軟體造成偵訊筆錄資料外洩情事。 ● 2008/04/25：<u>玉山兵推疑洩密·六軍團全都露</u> 玉山兵推傳出推演資料外洩。透過安裝分享軟體，在電腦上鍵入簡體字搜尋，就可以在中國網站取得被翻譯成簡體字的國軍旅級兵推機密資料。兵推演習視同作戰，這項計畫遭對岸掌控，形同國防部被對岸反兵推，是極為嚴重的國防洩密案，將使台灣陷入空前的國安危機。 ● 2008/05/06：<u>分享軟體惹禍 網路報稅資料大規模外洩</u> 納稅人只要在電腦下載分享軟體，用網路報稅就會有資料外洩的風險，已有不少納稅人的報稅資料在網路上全都露。這是民國八十八年財政部推網路報稅以來，最大規模的報稅資料外洩情形。財政部財稅中心澄清並非遭駭客入侵系統，應是民眾電腦中的 P2P 下載軟體將資料分享、流出，因此也呼籲採用網路報稅的民眾不要使用 P2P 軟體。
<p>四、說明網路安全防護的基本概念【防毒、防諜、防駭】</p> <p>網路上處處隱藏危機，目前<u>電腦病毒</u>、<u>垃圾信件</u>、<u>間諜軟體</u>、及<u>網路釣魚</u>、<u>駭客入侵攻擊</u>可以說是現今網路安全議題上的五大威脅。面對這些網路應用所帶來的威脅，如何能夠安全地上網，基本的防毒、防諜、防駭的上網安全概念就必須先建立起來。</p>		
1. 介紹網路安全的基本概念	5 分	<p>※資安六大心法【六億六千萬】：</p> <p>六個注意</p> <ol style="list-style-type: none"> 1. 注意遵守資通安全規定 2. 注意密碼安全性原則 3. 注意隨時修補系統安全性漏洞 4. 注意隨時更新病毒碼 5. 注意保護使用資料安全 6. 注意電子郵件及網路使用規定

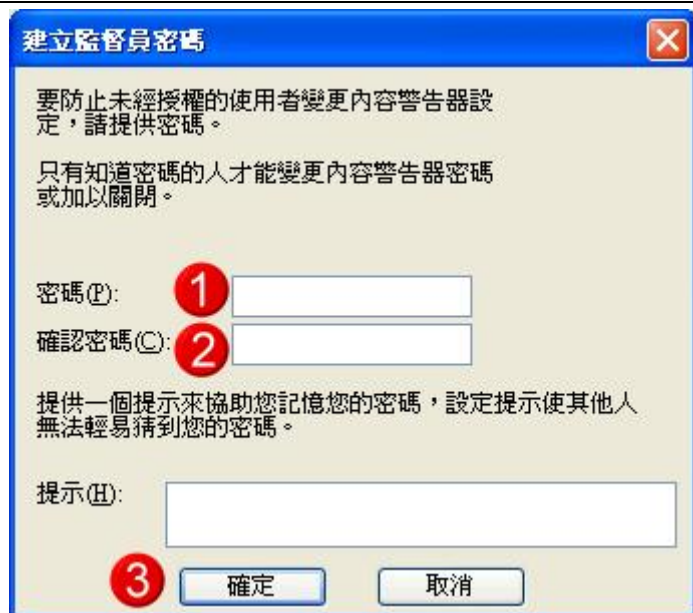
		<p>六個千萬</p> <ol style="list-style-type: none"> 1. 千萬不要開啟或回覆來歷不明電子郵件 2. 千萬不要下載或執行來歷不明軟體或檔案 3. 千萬不要洩露個人帳號密碼 4. 千萬不要用非信任電腦處理公務 5. 千萬不要隨意透露個人資料 6. 千萬不要忘記定期作資料備份
<p>1. 防毒概念－針對電腦病毒防護原理</p> <p>2. 病毒與漏洞攻擊的防治方法</p>	8 分	<p>一、電腦病毒【防毒】</p> <p>俗話說『禍從口出、病從口入』，在網際網路的世界中也是如此。電腦病毒常伴隨著檔案的交換或電子郵件進入電腦系統，當使用者執行遭病毒感染的電腦程式或開啟帶有病毒的電子郵件，其電腦系統就可能會被電腦病毒感染而中毒。</p> <p>『預防重於治療』是對電腦病毒的最佳防護。在電腦上加裝防毒程式是讓電腦永保安康不可或缺良方。防毒程式透過病毒碼的比對，對寫入電腦系統的檔案或電子郵件加以掃描，如發現病毒則立即隔離處理或加以刪除，防範電腦被病毒感染。因此，使用者必須定期更新病毒碼，如此防毒程式方能有效的針對最新的病毒加以防護。</p> <p>除了運用防毒軟體加以防護之外，良好的使用習慣也是非常重要，如：不下載來源不明的檔案、不安裝來路不明的軟體、不執行功能不明的程式、不任意開啟陌生來路的電子郵件，將電腦被病毒感染的機率降到最低，更是經濟有效防護電腦病毒的好方法。</p> <div style="border: 1px dashed black; padding: 10px;"> <p>網路威脅一：病毒與漏洞攻擊</p> <p>防治法：</p> <ol style="list-style-type: none"> 1. 安裝防毒軟體。 2. 經常更新病毒定義檔。 3. 更新作業系統的修補程式。 4. 電腦的使用者權限不要設在「電腦系統管理員」等級，並設定適當的登入密碼。 5. 不開啟來路不明的郵件。小心開啟郵件附加檔 </div>

<p>1. 說明垃圾信件的原理與運作方式</p> <p>2. 垃圾信件的防治方法</p>	<p>8 分</p>	<p>二、垃圾信件</p> <p>「垃圾信」(spam)指的都是不請自來，或者是未經收件者同意的電子郵件。通常這類郵件都是毫無目標以大量的（甚至可能是以數百萬或數千萬筆名單）方式在網路上傳送。</p> <p>從網路發展以來，垃圾信早就成為網路上的「萬惡淵藪」。舉凡病毒、間諜程式，網路釣魚等，全部都會透過垃圾郵件在傳播。此外，垃圾郵件還充斥著各種色情、瘦身減肥等誇大不實廣告，還有各種詐騙訊息。</p> <p>目前市面上已經有許多的軟體都附有郵件過濾功能（例如防毒軟體或新版的 Outlook），雖然說無法百分之百正確過濾所有的郵件，但是只要有正確的觀念和使用習慣，還是可以幫你解決垃圾郵件所帶來的許多困擾。</p> <div style="border: 1px dashed black; padding: 10px; margin-top: 10px;"> <p>網路威脅二：垃圾信件</p> <p>防治法：</p> <ol style="list-style-type: none"> 1. 不讀取任何垃圾郵件 2. 安裝郵件過濾軟體（或者啟動防毒軟體的信件過濾功能） 3. Yahoo、MSN 等網路式信箱，記得啟動過濾功能。遇垃圾郵件並記得回報。 </div>
<p>1. 說明間諜軟體與木馬程式的運作原理與威脅</p> <p>2. 間諜軟體與廣告軟體的防治方法</p>	<p>8 分</p>	<p>三、間諜軟體（木馬程式）【防諜】</p> <p>網路上也有間諜！</p> <p>使用者可能因為電腦潛藏「間諜軟體(spyware)」而主動將資料送出卻毫不知情。間諜軟體可能藏身於其他免費軟體之中，伴隨著免費軟體的安裝而藏身於電腦之中，或在網頁瀏覽的過程中不慎下載安裝，或因電子郵件的開啟執行而被安裝。</p> <p>間諜軟體可收集電腦的系統資訊，或者使用者的網路瀏覽記錄或習慣，甚至個人資訊如：姓名、電子郵件帳號、身分證字號、銀行帳號、信用卡卡號等。隨時將所收集的資訊傳送給收集者。</p> <p>面對間諜軟體的威脅，使用者應利用「反間諜軟體(anti-spyware)」，檢測個人電腦上是否存在有間諜軟體，一經發現應考慮立即加以移除，啟動對間諜軟體的即時監測功能，或執行反間諜軟體所提供之疫苗防護功能，並定期更新偵</p>

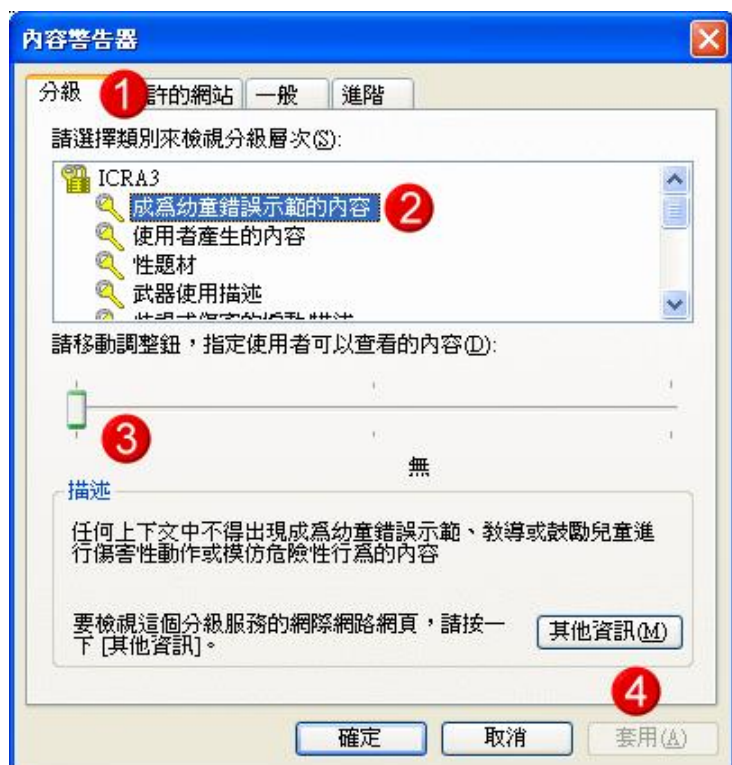
		<p>測碼定期檢測，以降低電腦系統被間諜軟體入侵之可能性。</p> <p>網路威脅三：間諜軟體和廣告軟體</p> <p>防治法：</p> <ol style="list-style-type: none"> 1. 安裝防諜軟體。 2. 電腦上至少要有兩套以上的防諜軟體。 3. 安裝任何軟體之前仔細看清使用條款，並注意安裝過程。 4. 不安裝來路不明的軟體。 5. 不上不明的網站。
<ol style="list-style-type: none"> 1. 說明釣魚網站的運作原理 2. 針對釣魚網站的防治對策 	8 分	<p>四、釣魚網站(phishing)</p> <p>網路釣魚是近幾年來才興起的一種網路騙術，目的通常都是要騙取使用者的帳號及密碼等個人的機密資料，進一步利用這些資料從事網路犯罪，特別是詐財，例如以金融帳號進行竊盜。</p> <p>網路釣魚的手法其實和日常生活中的手機或簡訊詐財很像：利用垃圾郵件（spam），通知使用者去更新帳號密碼等個人資料。當然的，依照這些通知所連到的網站通常是假造的。</p> <p>許多更精密的偽造手法實在讓人防不勝防，例如用所謂的「網址嫁接」（pharming）技術，在 DNS（域名系統）上下毒之後，讓你完全無法知道你連上的是假的網站。</p> <p>網路威脅四：網路釣魚</p> <p>防治法：</p> <ol style="list-style-type: none"> 1. 任何主動寄來要求輸入帳號和密碼的訊息，絕對不要相信。 2. 不要信任任何的垃圾郵件及來路不明的垃圾傳訊。 3. 不小心洩露資料時，要立即更改帳號的密碼。 4. 檢查網站是否為釣魚網站： http://www.google.com/safebrowsing/diagnostic?site=http:// 5. 回報釣魚網站：http://www.antiphishing.org/

<p>1. 說明網路攻擊原理與駭客入侵的概念</p> <p>2. 防止駭客入侵的防治對策</p>	<p>8 分</p>	<p>五、網路攻擊事件【防駭】</p> <p>透過網際網路，使用者可以自由的瀏覽網站、下載資料，當使用者透過網路獲取資訊時，必須慎防他人也透過網路入侵自己的電腦，竊取甚至破壞儲存於電腦中的資料，造成無法彌補的損失。</p> <p>面對複雜多變的網路攻擊，「防火牆(Firewall)」是防護個人電腦安全的最佳利器。運用防火牆可以阻絕外部不請自來的網路連線，大幅降低電腦系統被駭客入侵或被網路蠕蟲(Internet Worms)感染的可能性，在系統漏洞未能即時補強之前，為電腦系統提供絕佳的隔離屏障。除此之外，防火牆亦可管控電腦系統對外的連線，讓使用者更清楚電腦軟體和外部網路的連線狀況，對異常的連線企圖提出警告，避免資料不慎外洩。</p> <p>簡單來說，防火牆可提供電腦系統內外雙向的安全防護，是電腦上網時不可或缺的安全防護工具，使用者可將內建於系統的防火牆加以開啟，或從網路下載免費的防火牆軟體，或採購防火牆軟體安裝於電腦上，為電腦上網做好最基本的防護工作。</p> <div style="border: 1px dashed black; padding: 10px; margin-top: 10px;"> <p>網路威脅五：駭客入侵攻擊</p> <p>防治法：</p> <ol style="list-style-type: none"> 1. 安裝個人防火牆，以加強個人電腦安全防護。 2. 執行作業系統與應用軟體之弱點補強作業，修補軟體漏洞以防範惡意電子郵件攻擊。 3. 不明郵件一律刪除，以避免遭受駭客攻擊。 4. 不任意下載或安裝不明軟體，如電腦遊戲或工具軟體等，以防駭客入侵。 5. 不在安全防護不足之網際網路環境中使用電子交易，如網咖等，以防資料遭竊聽冒用。 </div>
<p>五、介紹常見的網路安全防護工具</p>		
<p>1. 說明網站分級的重要性。</p> <p>2. 介紹分級團體定義的分級規定。</p>	<p>20 分</p>	<p>1. 網站內容分級的概念：隨著網際網路資訊日益成長及用戶年齡層向下延伸，兒童及青少年透過此複雜且多樣化的媒體而涉足不當資訊內容的可能性已逐漸升高，如暴力或色情的文字、圖片或甚至影片等。</p>

<p>3. 介紹 IE 的分級設定「內容警告器」之操作</p> <p>4. 介紹網站內容分級過濾軟體</p>		<p>因此，針對網站內容分級建立一個合宜的機制，使得每個網路的使用者都能看到適合的內容。</p> <p>2. 介紹 RSACi 分級：是由美國史丹佛大學所發展制訂，原本是針對電視電影媒體等傳媒所設計，將需過濾的內容分為性、裸露、語言、暴力四個類別，再將不同的類別分為 0 到 4 共 5 個等級，級數愈高內容傷害程度也越大。</p> <p>3. 網路內容分級協會「ICRA」（Internet Content Rating Association）就是依此發展出「RSACi 過濾系統」，用來保護兒童與青少年阻隔於情色暴力之外。</p> <p>4. 透過與「網際網路內容分級協會」（ICRA，其前身為 Recreational Software Advisory Council，RSACi）的合作，Microsoft 提供了一種方法來限制使用者能檢視的網站類型。針對分級設定，無需安裝任何軟體，只要在 IE 瀏覽器做好設定就行了。</p> <p>【IE 分級設定說明】</p> <p>1. 進入 IE 之後，下拉「工具」選單。</p> <p>2. 點選「網際網路選項」。</p> <p>3. 浮現一個「網際網路選項」視窗，點選「內容」頁籤。</p> <div data-bbox="710 1529 1337 1825" data-label="Image"> </div> <p>4. 選擇「內容警告器」，點選「啟用」按鈕。</p> <p>◆ 如果是第一次設定「內容警告器」，會跳出一個「建立監督員密碼」的視窗，要你設定密碼。</p>
--	--	--

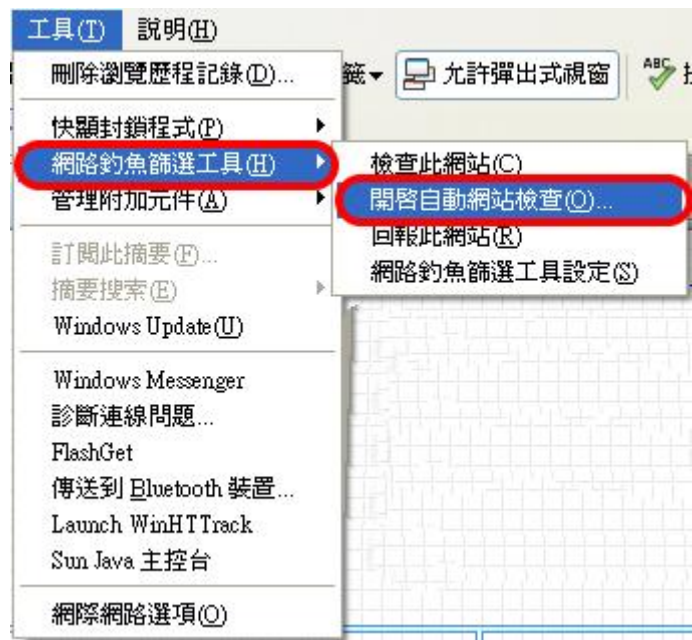


5. 點選「分級」頁籤。
6. 你可以看到上方有個要過濾的類別選項，選擇要過濾的類別
IE6 有 4 個類別：分別為性、語言、裸露、暴力。
IE7 有 13 個類別：幼童、使用者產生內容、性、武器、歧視、毒品、酒精、菸草、恐懼恫嚇、裸露、語言、暴力、賭博
※當第一次啟動內容警告器時，它會採用最保守的設定。您可以依據自己的意願修正這些設定值。
7. 移動下方的滑桿可以調整容許讓使用者可以閱覽網站與清單中的類別，設定限制的標準最大的容許範圍在哪裡。



8. 設定完畢之後，按下「套用」，將這個分級設定套用在 IE 瀏覽器上。

		<p>參考網址：</p> <ul style="list-style-type: none"> ➤ 【ICRA 官方網站】 http://www.fosi.org/icra/ ➤ 【台灣網站分級推廣基金會 TICRF 的分級服務— 免費提供『網頁過濾軟體』】 http://www.ticrf.org.tw/chinese/rating-institution.htm
1. 介紹釣魚網站的危害 2. 介紹防堵釣魚網站的方法 3. 介紹 IE7「網路釣魚篩選工具」設定 4. 介紹網路釣魚軟體的安裝與設定	25 分	1. 釣魚網站的安全威脅 <p>現在網路購物興盛，多半使用線上刷信用卡的方式付款，雖然大多數購物網站都有安全的機制；但是假冒各購物網站與銀行官網的「釣魚網站」詐騙手法還是常常出現。</p> 2. 防堵釣魚網站 <p>釣魚網站(Phishing)詐騙手法層出不窮，偽造一個正規經營的商業網站，利用網站的域名和網頁的相似度，降低使用者的警戒心，再誘騙使用者輸入帳號密碼，盜竊使用者的所有個人資料。使用者常常很容易一時疏忽，導致個人損失慘重。</p> <p>如果我們不是很小心地辨識釣魚網站或是害怕自己信用卡帳號密碼被偷，可以利用一些防釣魚網站的工具來幫我們監視你上網購物的網站是不是真的該網站而不是被導引到詐騙網站上。</p> 3. 軟體防護 <p>使用 IE7「網路釣魚篩選工具」</p>



Internet Explorer7 網路釣魚篩選器顯示可疑網站的警示



【軟體 1】

刑事局科技犯罪防制中心特別研發與設計惡意程式清除軟體「GK 1.0」，提供民眾協助掃除本案木馬程式與鍵盤側錄等惡意程式（GK1.0 自動分析電腦是否遭植入惡意程式，並清除相關惡意程式檔案與註冊機碼。

- 軟體名稱：惡意程式清除軟體「GK 1.0」
- 軟體用途：掃除木馬程式與鍵盤側錄等惡意程式
- 軟體性質：Freeware
- 版本代碼：1.0
- 檔案大小：597 KB
- 原創公司：刑事局科技犯罪防制中心
- 下載位址：

http://www.cib.gov.tw/news/news02_2.aspx?no=343



【軟體 2】

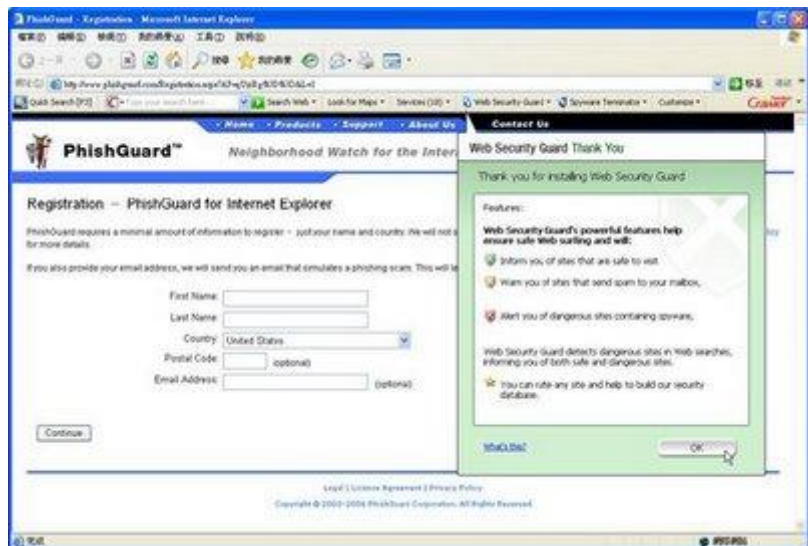
防止「網路釣魚」的工具- PhishGuard，它可以監視瀏覽器IE(Internet Explorer)的連結狀況，一發現連結到了釣魚網站，就會馬上跳出訊息和聲音提醒使用者，避免不小心上鉤。

- 軟體名稱：PhishGuard
- 軟體用途：防止「網路釣魚」的工具
- 軟體性質：Freeware
- 版本代碼：2.1.131

- 檔案大小：3.17MB
- 作業系統：Windows 98/ME/NT 4.0/2000/2003/XP
- 原創公司：PhishGuard Corp.
- 官方網址：<http://www.phishguard.com>
- 下載位址：
<http://www.phishguard.com/installers/PhishGuard-IE.exe>

使用步驟：

1. 安裝好 PhishGuard 之後，會跳出一個「PhishGuard Registration」視窗，按一下〔Get Key〕，連回連上官方網站免費取得一組序號。
2. 連回 PhishGuard 官方的註冊網頁之後，填入簡單的個人資料以及 E-mail 帳號，隨後就會收到一封內含註冊碼的郵件，將註冊碼填入前一個步驟內的方框中，然後按下〔Continue〕就可以受到 PhishGuard 的安全保護了。




3. 官方網站詳細安裝說明：
<http://www.phishguard.com/products.htm>

【軟體 3】

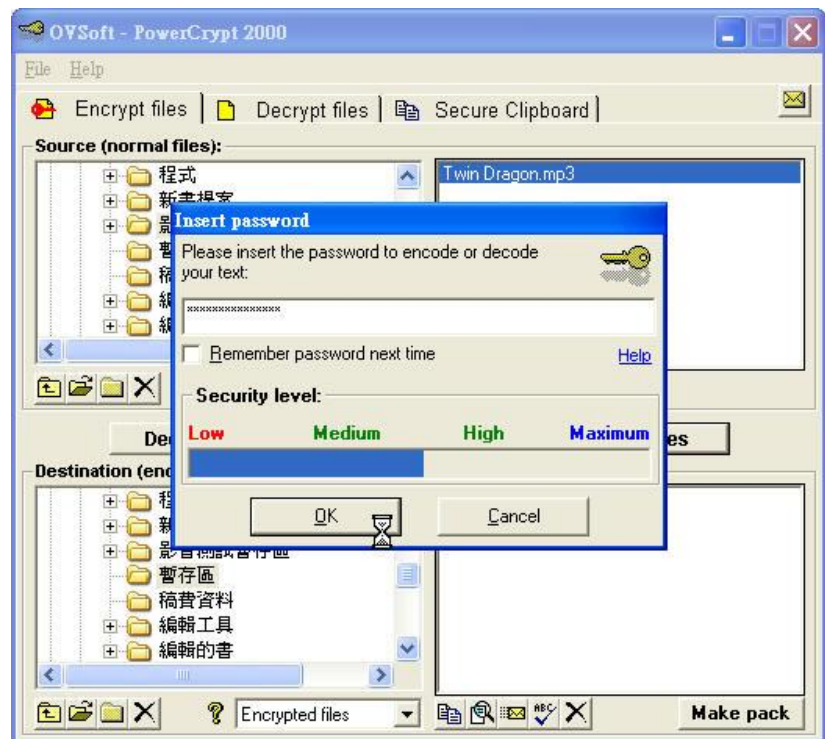
Netcraft 除了是知名的網路調查機構與資安機構外，和一般使用者關係較密切的「防釣魚網站工具列」（有效阻絕防木馬網站）推出以來，受到不少好評。它最主要的功能就是將所有安裝本工具列用戶碰到的網站寫進資料庫，並過濾出釣魚（惡意程式騙取使用者帳號密碼和個人資料）、木馬網站，並給予危險的標示，將釣魚網站阻絕掉。

		<ul style="list-style-type: none"> ● 軟體名稱：Netcraft Toolbar ● 軟體用途：防木馬、釣魚網站的 Netcraft 工具列 ● 軟體性質：Freeware ● 檔案大小：3.04MB ● 作業系統：Windows 2000/XP ● 原創公司：Netcraft ● 官方網址：http://news.netcraft.com/ ● 下載位址： for IE：http://toolbar.netcraft.com/ for Firefox： https://addons.mozilla.org/en-US/firefox/addon/1326 <p>【回報釣魚網站】</p> <p>➤ 微軟 IE7 回報網址： https://phishingfilter.microsoft.com/feedback.aspx?result=none&URL=釣魚網站的網址</p> <p>➤ Google 網路釣魚回報網頁： http://www.google.com/safebrowsing/report_phish/</p> <p>➤ Yahoo! - Phishing Report Form http://help.yahoo.com/fast/help/us/security/cgi_phishing</p>
1. 說明網路安全面臨的資料遺失風險 2. 針對資料備份的策略與軟體應用	15 分	1. 資料遺失常因硬體故障、水災、火災、安全性漏洞或誤刪重要檔案而發生。 2. 不論資料遺失的原因為何，做好資料備份預防措施以降低其影響，就像是買保險一樣，可以讓您的遺失資料迅速恢復。 <p>【軟體】</p> <p>資料備份精靈是一套全中文介面的檔案備份工具，非常適用在個人工作室以及公司行號的電腦資料備份，軟體可以設定備份的時間，時間一到自動備份您的資料，並且可以指定您所要備份的類型，您不至於備份到您不想備份的檔案，相當的方便，</p>

		<p>無限的備份清單，不管硬碟上有多少檔案，都可以完整的備份，以及區域網路端備份… 等等，簡單的使用者介面，輕鬆上手，備份不求人，不管是我的最愛・以重要的 Outlook Express 郵件等等，都可以備份起來。</p> <ul style="list-style-type: none"> ● 軟體名稱：資料備份精靈 ● 軟體用途：檔案備份工具 ● 軟體性質：Freeware ● 版本代碼：2.05 Beta ● 檔案大小：364 KB ● 作業系統：Windows 2000/XP/2003/Vista 32 位元 ● 原創公司：紅淚網 HolaNet ● 下載位址：http://hola.idv.tw/ 
<p>1. 說明網路傳輸的資料加密保護</p> <p>2. 資料加密策略與軟體應用</p>	<p>15 分</p>	<p>1. 資料加密機制：使用加密軟體，進行資料加密，確保沒有授權的使用者無法讀取資料，以確保電腦上機密資料的安全。</p> <p>2. 資料加密形式很多。您可以加密個別的檔案、資料夾，如果想要的話，還可以加密整個硬碟。某些加密形式可以讓檔案隱形。Windows 作業系統也提供某些加密功能，但是您也可以下載保護周全的 128 位元加密軟體。</p> <p>【軟體】</p>

使用 PowerCrypt 將電腦中重要的檔案加密的操作方式很簡單，只要幾個簡單的步驟就可以很輕鬆將檔案加密處理後，儲存至指定的位置，此外你也可以使用它直接為文字內容加密，讓原本看似正常的文章內容直接變成亂碼，不知情的人開啟時還以為檔案已損毀，大大的增加重要檔案的安全性。

- 軟體名稱：PowerCrypt 2000
- 軟體用途：檔案、文字資料都能加密的工具
- 軟體性質：Freeware
- 版本代碼：44
- 檔案大小：1.6 MB
- 作業系統：Windows 95/98/ME/NT/ 2000/XP
- 原創公司：Ovsoft
- 官方網址：<http://www.ovsoft.com/>
- 下載位址：<http://www.ovsoft.com/ftp/freeware/pcrypt44.exe>



安裝使用步驟：

1. 首先請下載並安裝 PowerCrypt 2000，並將之開啟後，先切換至 [Encrypt files] 活頁標籤，在左上方視窗中點選要加密的檔案，這時右上方視窗即會出現該檔案的名稱。

		<p>2. 接著選取加密的檔案，然後在左下方視窗的「Destination(encrypted files):」空白框中選定選擇加密後的檔案儲存的資料夾位置後，按下〔Encrypt files〕。</p> <p>3. 接著會出現「Insert password」對話盒，在空白欄位中輸入指定的密碼，Security level 的長度越長加密性也越高，確認後按下〔OK〕。</p> <p>4. 密碼確認的對話，請再次輸入相同的密碼，確認後按下〔OK〕，等待檔案加密動作完成。</p> <p>5. 接著你就可以看到檔案資料已經被加密備份在你預設的資料夾中，如果你把 PowerCrypt 刪除，就會無法辨識此種檔案，就算利用解密的檔案設法開啟，也必須透過正確的密碼才能夠開啟檔案。</p> <p>※注意： PowerCrypt 對檔案執行加密動作，是直接複製一個加密好的檔案在你指定的資料夾內，若是想要完全機密，記得要把原始檔刪除。</p>
<p>1. 介紹垃圾郵件傳送病毒的危害</p> <p>2. 垃圾郵件過濾軟體與防堵策略</p>	20 分	<p>1. 垃圾郵件處理：電子郵件已經成為人們不可或缺之基本工具，然而隨著垃圾郵件的氾濫，垃圾郵件已成為信件處理揮之不去的困擾。</p> <p>2. 垃圾郵件不只造成時間的浪費，而且有時會因此漏掉正常信件而造成嚴重的損失或困擾。</p> <p>【軟體 1】</p> <p>SpamDog 是一套與 Outlook (Express) 完全結合的垃圾郵件過濾軟體，其中最大的特色在於完全不須要改變您使用信件的習慣，就可以達到去除垃圾郵件的目的。SpamDog Lite 採用完全單機的版本，也不需要連網路即可使用。</p> <ul style="list-style-type: none"> ● 軟體名稱：垃圾郵件剋星 - SpamDog Lite ● 軟體用途：垃圾郵件辨識、郵件追蹤、郵件防毒功能 ● 軟體性質：Freeware ● 版本代碼：1.02

- 檔案大小：860 KB
- 作業系統：Windows 98/ME/2000/XP/2003/Vista
- 原創公司：Softworking.com 軟體工廠
- 官方網址：<http://www.softworking.com/>
- 下載位址：
<http://www.softworking.com/Download/SpamDogLite.zip>



【軟體 2】

SpamPal 是套免費的垃圾郵件過濾軟體，他是安裝在使用者端，適用於獨立的郵件軟體。例如：Outlook, Outlook Express 或 Eudora。

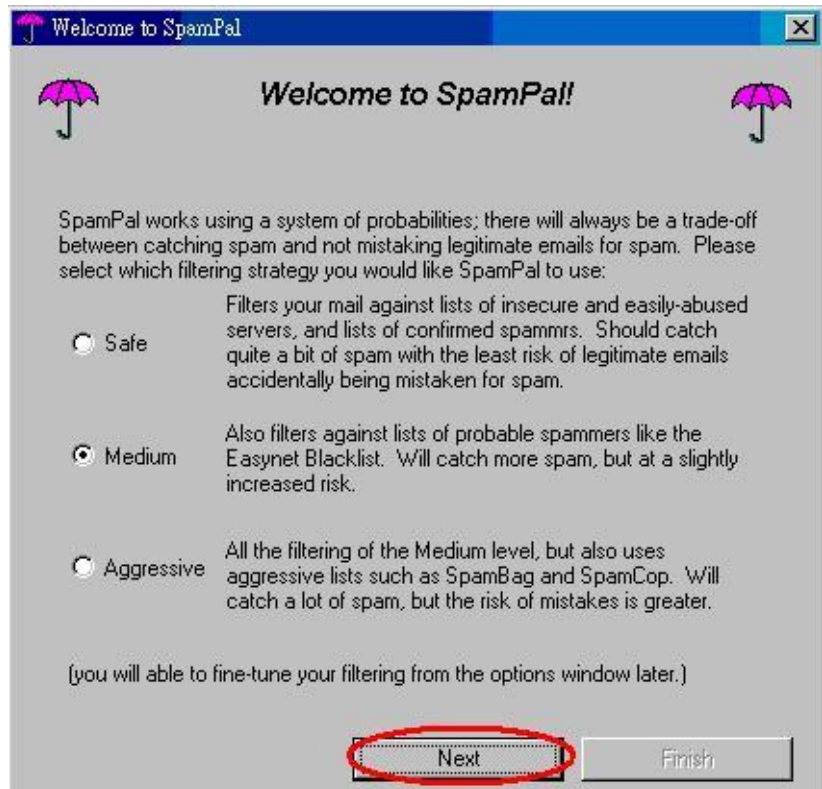
- 軟體名稱：SpamPal
- 軟體用途：垃圾郵件過濾軟體
- 軟體性質：Freeware
- 版本代碼：1.594
- 檔案大小：787 KB
- 作業系統：Windows 95/98/ME/NT/2000/XP/2003
- 原創公司：SpamPal
- 官方網址：<http://www.spampal.org/>
- 下載位址：<http://www.spampal.com/spampal.exe>

SpamPal 安裝使用：2 個步驟

- 安裝設定 SpamPal
- 設定所使用的郵件軟體

● 安裝設定 SpamPal

1. 下載後點選安裝，基本上跟著指示一步步做選預設值即可
2. 安裝完成後會跳出第一次 SpamPal 使用設定精靈首先必須選擇垃圾郵件防護程度，選預設”中等”即可



接下來會有 3 個選項，基本上除了第一個選項一定要移除外其他的預設即可(第一個選項如果打勾，所有來自中國、台灣、韓國的郵件會一律被當成垃圾郵件)

3. 安裝設定完成後，在右下角會出現一把粉紅色雨傘，按左鍵點選打開 SpamPal 視窗

視窗分成 3 個：

左上角是顯示每天郵件過濾的情況

右上角是顯示使用對外黑名單伺服器查詢的狀態

下方則是顯示利用 Pop3 或 IMAP4 下載郵件時連線的情況，當沒有連線時出現空白為正常。

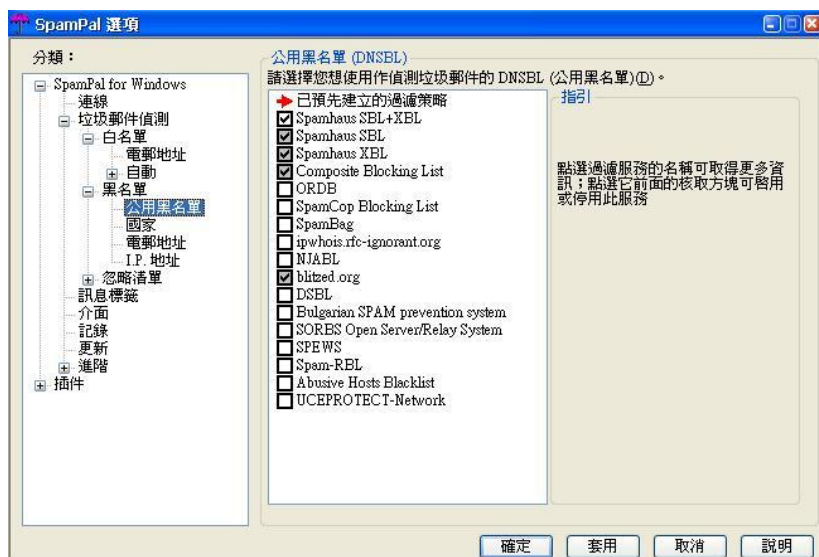
過濾操作總結					最近的 DNSBL 查詢				
日期	# 操作	垃圾郵件	已通過	已放到白名單	名稱	# 查詢	陽性	陰性	命中率
星期二 24 四月 2007	215	123	92	82	Spamhaus SBL+XBL	246	84	162	34.1%
星期一 23 四月 2007	0	0	0	0					1.682s
星期日 22 四月 2007	0	0	0	0					
星期六 21 四月 2007	0	0	0	0					
星期五 20 四月 2007	0	0	0	0					
星期四 19 四月 2007	53	27	26	23					
星期三 18 四月 2007	41	22	19	16					
星期二 17 四月 2007	48	28	20	14					
星期一 16 四月 2007	127	91	36	34					
星期日 15 四月 2007	0	0	0	0					
星期六 14 四月 2007	92	17	75	3					
星期五 13 四月 2007	0	0	0	0					
星期四 12 四月 2007	0	0	0	0					
星期三 11 四月 2007	0	0	0	0					

4. 進階設定，雖說啟動後有精靈協助基本設定，但建議在使用前進入選項檢查並調整，才不會在第一次使用時就把一些正常信件也歸成垃圾郵件。

選擇「工具」中的「選項」，幾個必須檢查設定的項目

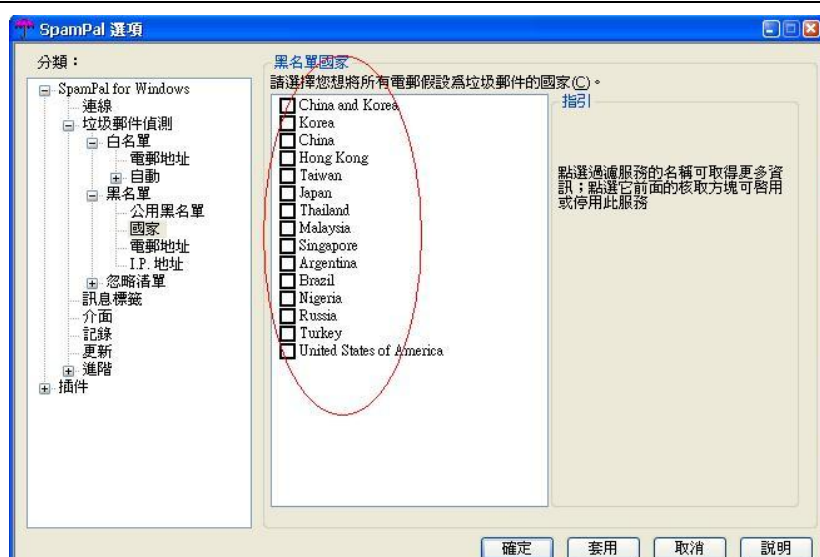
5. **黑名單下的” 公用黑名單”**：

基本上你可以全選，但是會影響郵件過濾時間，目前使用起來 Spamhaus XBL+ XBL 黑名單伺服器比較準，建議勾選。



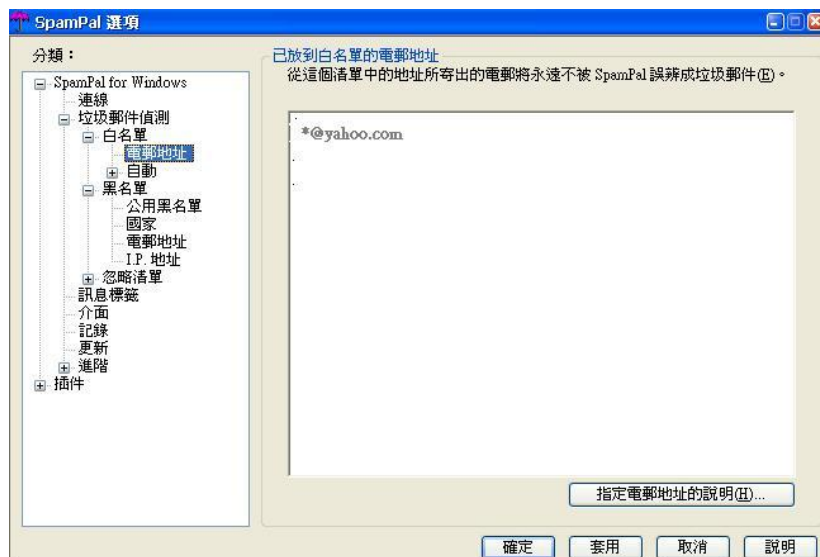
6. **黑名單下的” 國家”**：

確認都沒有打勾，如果你打勾，表示你認為來自那個國家所有的郵件全部都是垃圾郵件。



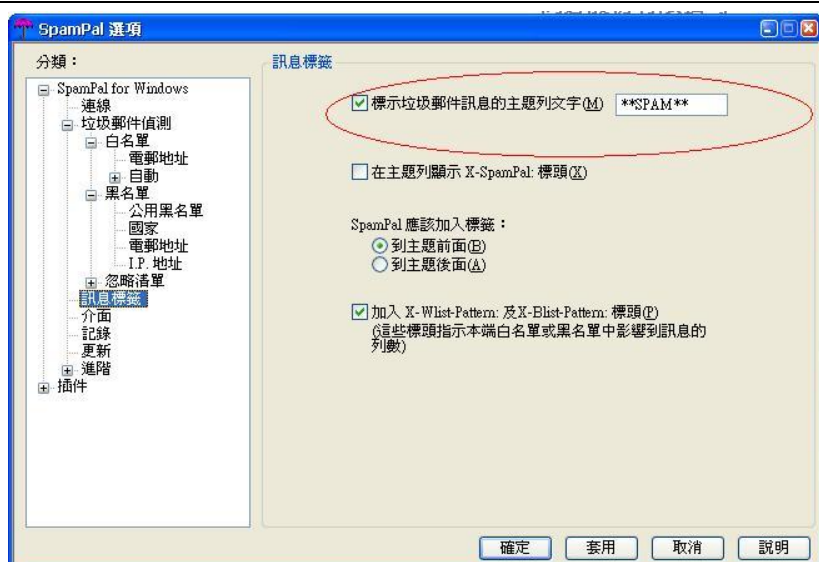
7. 白名單下的”電郵位置”：

記得打入你確認不是垃圾郵件的位置 eg: *@yahoo.com 表示所有來自 Yahoo.com 的信件全部視為正常郵件，如果不建入信任的郵件地址，第一次使用會有誤判的情況發生。

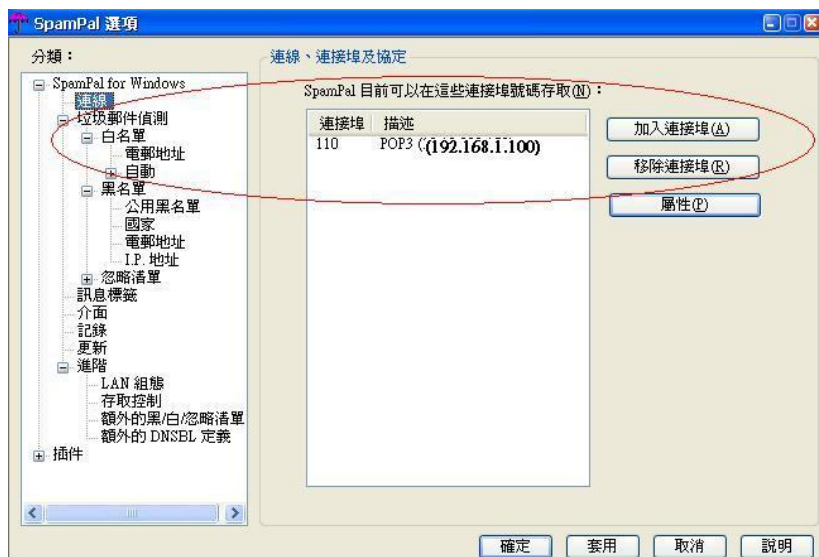


8. 訊息標籤：

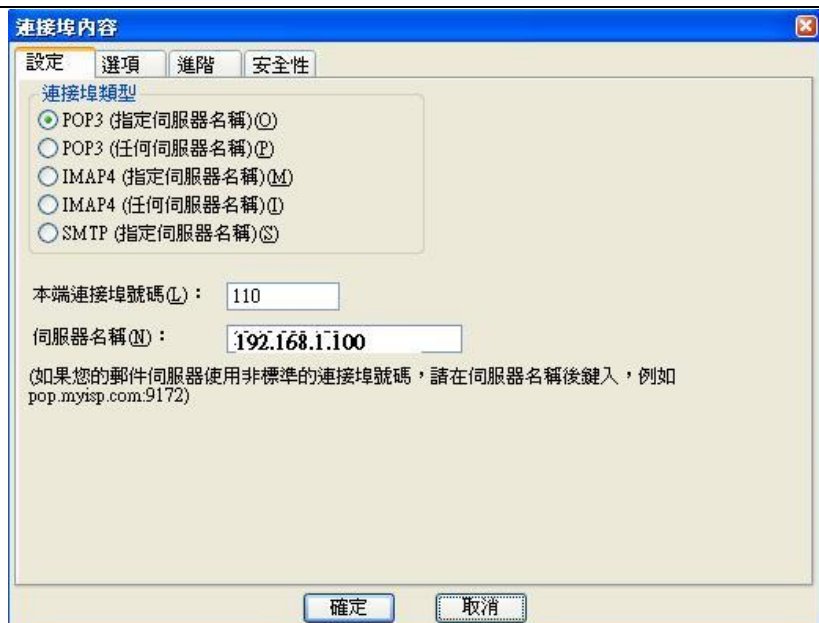
預設為**SPAM**，可不用更改，系統一旦認為垃圾郵件，會將郵件主旨地方加上 **SPAM** 文字。郵件軟體則利用此標籤把垃圾郵件放入垃圾桶中。



9. 設定郵件伺服器來源（最重要的設定）在選項中的「連線」：把所有預設連線移除，按「加入連接埠」



範例中是使用 POP3，選擇 POP3 指定伺服器，在下方伺服器名稱中打入 你要連線伺服器的名稱(使用 DNS 解析) 或是 直接打 IP 位置。其他選項可不動，按確定即可。



SpamPal 正式設定完成。進入第二步驟→設定所使用的郵件軟體

● 設定所使用的郵件軟體

基本上不論 Outlook, Outlook Express 設定的方式都大同小異，這裡簡單說一下設定的方式

1. 設定郵件伺服器

在 Outlook Express 上方工具中選 “帳戶”，設定郵件伺服器移除原設定，新增郵件→在伺服器的設定中，把 POP3 伺服器的位置打入” 127.0.0.1”，SMTP 伺服器則打入原連線郵件伺服器即可（同 SpamPal 設定郵件伺服器來源）

在下方打入郵件伺服器的 ID 及 PW。其他設定和一般郵件設定無異。

		<p>開機時, SpamPal 會自動啟動, 當要收郵件時, 自動會先重 SpamPal 過濾再送到 Outlook。</p> <p>2. 所有的被認定的垃圾郵件在主旨上會被標成”**SPAM**”，這時再利用 Outlook 工具中郵件規則，把所有主旨中含有”**SPAM**”的字串，全部放入垃圾桶 或是特定的目錄匣中。</p>
<p>1. 介紹防毒軟體的功用與目的</p> <p>2. 介紹常見免費的軟體</p>	<p>20 分</p>	<p>1. 防毒軟體 Anti-Virus：防毒軟體是設計和研發來提供個人電腦必備的保護的完整安全解決方案。</p> <p>2. 它可以對抗像病毒、間諜軟體、廣告軟體、惡意軟體、鍵盤記錄程式和駭客攻擊…等各種威脅。</p> <p>【軟體 1】</p> <p>Norton Security Scan：偵測並消除病毒和網際網路蠕蟲 免費偵測更新和定期掃描</p> <p>Spyware Doctor™入門版：偵測並移除間諜軟體、廣告軟體、木馬病毒以及鍵盤記錄程式包含智慧更新與排程以保護您的電腦</p>

- 軟體名稱：Google Pack 軟體集
- 軟體用途：病毒、蠕蟲、木馬、間諜軟體防護
- 軟體性質：Freeware
- 原創公司：Google
- 官方網址：<http://pack.google.com/>
- 下載位址：
http://pack.google.com/intl/zh-tw/pack_installer.html



Google 特別版服務

Google Pack 在此，為您提供 Norton Security Scan 特別版服務，協助您評估電腦安全風險的漏洞。

- 偵測並移除病毒、病蟲及木馬程式
- 警告您電腦上有間諜程式及煩人的廣告軟體 *
- 介面容易使用，方便您執行並排程掃描作業

- 「全系統掃描」可執行系統與硬碟的深入掃描，以偵測現有的病毒、間諜程式與其他威脅
- 提供掃描結果摘要，告知您被偵測並修復的檔案，或需要您注意的地方
- 會為您啟用偵測更新 **

*Norton Security Scan 會偵測但不會移除間諜程式或廣告軟體。

**若是從 Google Pack 中移除 Norton Security Scan 的話，則自移除之日起六 (6) 個月內，賽門鐵克可隨時視情況停止 Norton Security Scan 服務。

【軟體 2】

AntiVir 是一套由位於德國的 Avira 公司發展出。Avira 在專精於安全領域長達 20 年，公司有超過 250 位以上的員工，並且擁有高達三千萬的用戶。近年來，AntiVir 軟體效能與防毒能力日益卓越，在許多防毒軟體的評鑑都有不錯的表現。

- 軟體名稱：Avira AntiVir Personal 小紅傘

- 軟體用途：防毒軟體
- 軟體性質：Freeware
- 版本代碼：8.1.0.326
- 檔案大小：23.89 MB
- 作業系統：Windows 2000/XP/Vista
- 原創公司：Avira
- 官方網站：<http://www.avira.com/>
- 官方推廣網站：<http://www.free-av.com/>
- 下載位址：
http://www.free-av.com/en/download/1/avira_antivir_personal_free_antivirus.html
- 教學資源：【Spock's 網路筆記本】
<http://blog.pixnet.net/spock/post/7678503>



【軟體 3】

「avast! Antivirus」是一套內建繁體中文語系的免費授權（家用、非商業使用）防毒軟體，雖然免費，不過防毒能力也是名列前茅，且內建的 HTTP、EMAIL 防護之外，還有 P2P 防護、MSN、即時通等聊天工具的安全防護、網路攻擊防護…等等，相當完整唷！

- 軟體名稱：Avast! Antivirus
- 軟體用途：防毒軟體
- 軟體性質：Freeware
- 版本代碼：4.8.1277
- 檔案大小：24.64 MB
- 作業系統：Windows 2000/XP/Vista
- 原創公司：ALWIL Software

- 官方網址：http://www.avast.com/index_cnt.html
- 下載位址：
<http://www.avast.com/cnt/download-avast-home.html>
- 教學資源：【重灌狂人】<http://briian.com/?p=523>



【軟體 4】

AVG Anti-Virus Free 是一套老牌的防毒軟體，他不僅提供免費版供個人使用，而且亦整合了 Avg Anti-Spyware，可以說是掃毒和掃間諜程式的功能兩者兼具。

- 軟體名稱：AVG Free Anti-Virus
- 軟體用途：防毒軟體
- 軟體性質：Freeware
- 版本代碼：8.0.138.1332
- 檔案大小：46.13 MB
- 作業系統：Windows 2000/XP/Vista
- 原創公司：AVG Anti-Virus
- 官方網址：<http://free.grisoft.com/ww.homepage>
- 下載位址：
<http://free.grisoft.com/ww.download?prd=afe>
- 教學資源：【海芋小站】
<http://inote.tw/2008/04/avg-anti-virus-free-80.html>

		 <p>【檢測病毒網站】</p> <p>VirusTotal 是一款可疑檔案分析服務，通過各種知名反病毒引擎，對您所上傳的檔案進行偵測，以判斷檔案是否被病毒、蠕蟲、木馬、以及各類惡意軟體感染。</p> <p>網址：http://www.virustotal.com/zh-tw/</p> <p>【防毒軟體定期評比】</p> <ul style="list-style-type: none"> ➤ 【AV-Comparatives】 http://www.av-comparatives.org/ ➤ 【Virus.gr】 http://www.virus.gr/ ➤ 【Malware-Test Lab】 http://www.malware-test.com/
<p>1. 說明間諜軟體的危害</p> <p>2. 介紹針對間諜軟體的偵測與移除程式</p>	<p>15 分</p>	<p>1. 間諜軟體會在未經使用者同意的情況下進行廣告、收集私人資訊，或修改電腦設定等行為的軟體；特徵在於不會大量地繁殖，通常也不會刻意去破壞系統。</p> <p>2. 它們的目的是神不知鬼不覺地偷取資料並且做進一步的”利用”。更有可能讓駭客可以遠端操控您的電腦，方便他進一步滲透到您的公司內部。</p> <p>【軟體 1】</p>

Windows Defender (Beta 2) 是一個免費的程式，可協助您的電腦避免由間諜軟體及其他有害軟體所帶來的快顯視窗、效能低落及安全性威脅等侵擾。Windows Defender (Beta 2) 目前僅提供英文版、德文版及日文版。反間諜軟體無法找到駭客工具程式、及病毒（這應用軟體只可作為防毒軟體的補充，並不能代替防毒軟體）。

- 軟體名稱：Microsoft Defender Beta2
- 軟體用途：反間諜軟體
- 軟體性質：Freeware
- 版本代碼：1593 Beta 2
- 檔案大小：4.9 MB
- 作業系統：Windows 2003/XP SP2
- 原創公司：Microsoft
- 官方網址：
<http://www.microsoft.com/taiwan/athome/security/spyware/software/default.aspx>
- 下載位址：
<http://www.microsoft.com/taiwan/athome/security/spyware/software/default.aspx>



【軟體 2】

Ad-aware 是一款相當不錯的「廣告」移除程式，它會掃描您的系統中的廣告連結，舉凡免費軟體所附掛的廣告軟體、回報

		<p>連結都可以偵測的出來，如果有發現的話，均可將之移除！</p> <ul style="list-style-type: none"> ● 軟體名稱：Ad-Aware 2008 Free ● 軟體用途：廣告移除程式 ● 軟體性質：Freeware ● 版本代碼：7.1.0.8 ● 檔案大小：18.27 MB ● 作業系統：Windows 2000/XP/Vista ● 原創公司：Lavasoft ● 官方網址：http://www.lavasoft.de/ ● 下載位址：http://lavasoft.com/single/trialpay.php ● 教學資源：【海芋小站】 http://inote.tw/2007/01/lavasoft-ad-aware-se-personal.html 
<ol style="list-style-type: none"> 1. 說明防火牆的原理與運作方式 2. 介紹免費的軟體防火牆 3. 練習安裝並進行觀察防火牆的偵測封包進出狀況 	20 分	<ol style="list-style-type: none"> 1. 防火牆 Firewall：防火牆是指一套用來明顯區隔兩個(或以上)網路之間的一組軟硬體裝置，使網管人員得以事先制定種種安全規則，針對網路交通及安全程度，進行過濾控制和調整。 2. 最大的目的在於防止網路遭受入侵。主要功能為阻擋試圖透過網際網路進入你電腦的駭客。 3. 駭客進入你的電腦系統的原因有：破壞你的電腦檔案、偷竊電腦內儲存的資料、以及未經你的允許操

控你的電腦。

【軟體 1】

費爾個人防火牆專業版可以為你的電腦提供全方位的網路安全保護。在這駭客橫行的網路時代，使用者若不做好完善的保護動作，被入侵的代價是很慘痛的。費爾個人防火牆專業版是一套功能不錯且免費的防火牆程式。

- 軟體名稱：費爾個人防火牆專業版
- 軟體用途：軟體防火牆
- 軟體性質：Freeware
- 版本代碼：3.0
- 檔案大小：4.10 MB
- 作業系統：Windows 95/98/ME/2000/XP
- 原創公司：Filseclab
- 官方網址：<http://www.filseclab.com/cht/>
- 下載位址：
<http://www.filseclab.com/cht/products/firewall.htm>





【軟體 2】

Comodo Firewall—免費、功能強大的防火牆

網路上危機伺服，你是否擔心自己的電腦會遭到駭客的入侵，變成人家的犯罪跳板呢？Comodo Firewall 是由著名的系統安全供應商— Comodo Inc 所開發的一套免費網路防火牆，它具有一般市售防火牆的多數功能，如封鎖特定通訊埠、封鎖特定軟體網路存取權限、監控網路使用情形、安全等級調整等，這些一般在商業軟體上才看得到的功能，在 Comodo Firewall 可是做得相當完整，一點也不含糊喔。

- 軟體名稱：Comodo Firewall
- 軟體用途：軟體防火牆
- 軟體性質：Freeware
- 版本代碼：2.4.16.174
- 檔案大小：8.45 MB
- 作業系統：Windows 2000/XP
- 原創公司：SpamPal
- 官方網址：<http://www.personalfirewall.comodo.com>
- 下載位址：
http://www.personalfirewall.comodo.com/download_firewall.html



參考網址：

- 【資安論壇－『軟體防火牆評比大集合』】
<http://forum.icst.org.tw/phpBB2/viewtopic.php?t=8651>
- 【Firewall Leak Tester 軟體防火牆評比 2006/03】
http://www.firewallleaktester.com/tests_overview.php
- 【Firewalls' ratings】
<http://www.matousec.com/projects/firewall-challenge/results.php>

附件一：駭客入侵系統的流程

目的	入侵步驟	應用技巧
找出網路目標與主機的位址與名稱。駭客會無所不用其極盡可能的收集最多的目標。	資料收集	利用網路工具程式，或從員工身上得知。
辨識目標主機與網路程式的廠商與版本包含是否有經過版本升級，這些資訊可作為後續攻擊的參考。	弱點掃描	利用SATAN scan網路弱點 利用 Netview 攔截網路封包，猜測 root 密碼。
更進一步找出目標主機的使用者帳號或是未受保護的網路分享檔案資料。	弱點刺探	列舉 user 帳號，空白密碼，利用 cracker 程式猜測密碼。
利用以上所收集到的資料嘗試登入目標主機，以取得系統使用者帳號，與存取權限。	取得初步的權限	密碼猜測工具，網路監聽程式，緩衝區溢位攻擊。
駭客會更進一步的想辦法提升權限至系統管理員的權限。	提升權限至 root	側錄 user 使用電腦習慣，使用密碼破解工具（例如，敲鍵盤側錄程式）。
破壞該主機的資料例如更換網頁內容，或刪除資料庫。	進行破壞	利用現存 OS 或 Server 應用程式的漏洞以跳板方式繼續攻擊其他主機。
這一類的駭客是以竊取客戶信用卡等私人資料為目的，因此他會長期潛伏在系統內，直到他找到有價值的資訊為止。	建立後門	新增帳號，建立定時自動執行程式，植入後門程式（如特洛伊木馬程式）。
有經驗的駭客在入侵後會抹去系統的紀錄檔，讓人無從查出他的蹤跡。	消滅蹤跡	刪除記錄檔(log file)，隱匿攻擊程式，甚至更換系統程式為後門程式。
如果嘗試各種方式都無法入侵主機，黔驢技窮的駭客就會使出三流的方法，癱瘓目標主機。	癱瘓或破壞目標	IP Spoofing, DDOS(阻斷攻擊)，郵件炸彈攻擊，這些程式是以發出大量偽造的封包，塞爆網路流量並癱瘓網路主機。

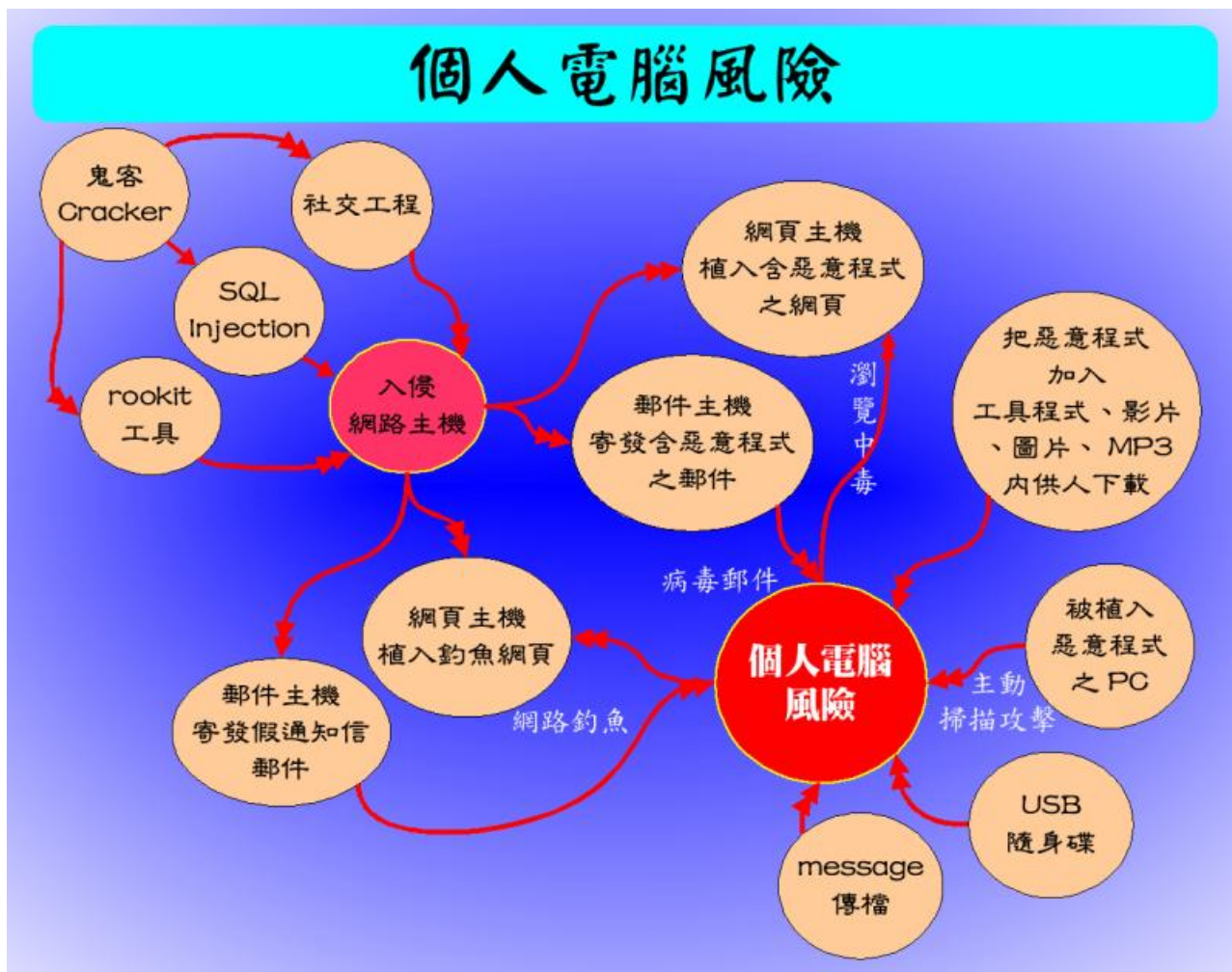
附件二：微軟影片說明

下載網址：

<http://www.microsoft.com/taiwan/athome/security/videos/downloads.msp>

檔案名稱	描述
保護您的電腦遠離間諜軟體 Spyware.zip (7.2 MB)	觀賞此影片以了解資訊關於間諜軟體是什麼，電腦可能被入侵的管道，入侵的徵兆，以及您能預防間諜軟體的三件事。
網路詐騙須知 Phishing.zip (8.7 MB)	了解網路詐騙訊息如何使您受騙並傳送個人資料，以及保護自己遠離因網路詐騙而受騙的三種方法。
處理垃圾郵件 Spam.zip (8.2 MB)	了解垃圾郵件的來源，哪一類的垃圾郵件訊息可能是危險的，以及您該如何做以協助減少您所收到的垃圾郵件。
讓電腦保持在最新狀態 Update.zip (8.2 MB)	了解更多使用 Office Update、Windows Update、以及自動更新以獲得您的電腦的最新的安全性和軟體更新。
保護您的線上隱私權 Privacy.zip (8.2 MB)	網際網路使您能方便地在線上購物、銀行交易與通訊，但也讓您面臨身分被竊的風險。只要採取一些基本的預防措施，就可以降低成為受害者的機率。
使用線上新聞群組 Newsgroups.zip (8.4 MB)	了解更多有關如何加入線上新聞群組和社群的資訊，包括如何搜尋與您分享相同興趣的群組、張貼問題、尋找解答、以及得到協助。
安全性概觀 Security.zip (9.1 MB)	觀賞此影片以開始學習如何改善電腦與線上個人資料的安全性。
預防病毒與蠕蟲 Viruses-worms.zip (9.5 MB)	了解病毒與蠕蟲會如何侵害您的電腦，並學習保護自己遠離電腦病毒的三大方法。
教導您的小孩有關上網的安全 Childsafety.zip (9.7 MB)	學習您該如何協助您的孩子更安全的瀏覽網際網路的更多資訊。

附件三：個人電腦的風險（圖片來源：台南縣教網中心）



附件四：網路攻防戰安全防護一覽

攻防教戰手則	具體作法	效果
安裝 工具軟體	IE7 「內容警告器」設定	網站內容分級；保護兒童與青少年阻隔於情色暴力之外。
	IE7 網路釣魚篩選工具	避免網路釣魚
	惡意程式清除軟體「GK 1.0」	掃除木馬程式與鍵盤側錄等惡意程式
	安裝 PhishGuard 軟體	防止網路釣魚
	安裝資料備份精靈軟體	資料備份，以防資料遺失
	安裝 PowerCrypt 2000	將資料加密，增加重要檔案的安全性
	安裝垃圾郵件剋星－SpamDog Lite	垃圾郵件辨識、郵件追蹤、郵件防毒功能
	安裝 SpamPal 軟體	垃圾郵件過濾功能
	Norton Security Scan	偵測並消除病毒和網際網路蠕蟲
	Spyware Doctor™入門版	偵測並移除間諜軟體、廣告軟體、木馬病毒以及鍵盤記錄程式
	Avira AntiVir Personal 小紅傘	防止電腦病毒
	Avast! Antivirus (防毒軟體)	防止電腦病毒
	AVG Free Anti-Virus (防毒軟體)	防止電腦病毒
	Microsoft Defender Beta2	反間諜軟體
	Ad-Aware 2008 Free	廣告移除程式
	費爾個人防火牆專業版	防止網路遭受入侵。為阻擋試圖透過網際網路進入你電腦的駭客
	Comodo Firewall	封鎖特定通訊埠、封鎖特定軟體網路存取權限、監控網路使用情形、安全等級調整等
軟體更新 設定	任何防毒及防間諜軟體都必須經常更新病毒／間諜軟體的定義檔	維持軟體的防毒效能
	Windows 系統漏洞修補程式	修補漏洞以加強電腦安全防護
	正確的 Windows 使用者帳號登入密碼設定	避免漏洞攻擊
	維護垃圾信過濾軟體的黑／白名單	提高垃圾信的過濾效能，並且避免誤刪正常的郵件

使用者習慣	不開啟垃圾郵件及垃圾郵件內容的連結	防止受騙，避免感染病毒、間諜軟體，及網路釣魚
	不開啟來路不明的郵件。小心開啟郵件附加檔案	避免電腦病毒與漏攻擊
	不輕信任何帳號／個人資料更改的通知信函	避免網路釣魚
	發現被網釣時，立即更改密碼及帳號資料	避免被網路釣魚後的可能受害
	安裝免費軟體時注意授權條款及安裝過程	避免安裝間諜軟體及廣告軟體
	不下載或執行來路不明的軟體或檔案	避免電腦病毒或木馬程式
	避免上非法網站	防止間諜軟體及木馬病毒、避免網站惡意攻擊碼
	定期作資料備份	避免資料遺失