

# 12 網路安全與保護



腦中毒很麻煩，網拍帳號遭盜虧很大！如何悠遊在網路的世界，享受科技帶來的便利而不被「駭」，大家都關心哦！

## 12-1 惡意程式的問題

我們經常透過電腦來瀏覽網頁、接收信件、下載檔案，你知道這些動作，都可能使你的電腦遭到「惡意程式」的侵害嗎？為了保護資料的安全，我們應學會如何防範惡意程式的入侵。

### 12-1-1 認識惡意程式

**惡意程式**（malicious software, Malware）是泛指會對電腦系統或網路運作造成不良影響的惡意軟體，這種軟體通常會透過各種網路服務及儲存媒體進行傳播，例如檔案下載、電子郵件、即時通訊軟體（如：Yahoo!奇摩即時通）、隨身碟……等。**電腦病毒**、**特洛伊木馬程式**、**電腦蠕蟲**等，都屬於惡意程式，以下分別介紹。

#### 電腦病毒

**電腦病毒**（virus）是指具有破壞性或惡作劇性質的電腦程式。他多半會隱藏在檔案或磁碟中的特定磁區，藉由自我複製或感染電腦中的其它正常程式，來達到破壞電腦系統的目的。

電腦病毒依照其特性，大致可分為以下4類（表12-1）：



表12-1 電腦病毒的種類

病毒類型	說明	舉例
開機型 (系統型)	寄生在磁碟片的啓動磁區 (boot sector) 中；當電腦開機後，病毒便會常駐在記憶體中，影響電腦的正常運作	米開朗基羅病毒
檔案型	多半是寄生在副檔名為COM及EXE的執行檔；受到感染的檔案在執行後便會傳染給其它檔案，或常駐在記憶體中伺機發作	13號星期五病毒
混合型	兼具開機型及檔案型病毒的特性，除了會感染啓動磁區之外，還會感染執行檔	大榔頭
巨集型	通常寄生在含有VBA巨集的文件檔案（如.doc、.xls）上；當使用者開啟被感染的檔案後，此類病毒便會開始進行破壞電腦系統的運作	台灣No.1

## 特洛伊木馬程式

**特洛伊木馬程式**（Trojan horse）通常是將惡意的程式「依附」在電腦檔案中，一旦使用者開啟檔案，電腦就會感染惡意程式（圖12-1）。這種惡意程式通常是以竊取他人的私密資料為目的，因此大多不會破壞電腦系統，也不會影響電腦的正常運作，受害者的私密資料往往在不知不覺中，就落入了電腦駭客手中。



圖12-1 特洛伊木馬程式



## 電腦蠕蟲

電腦蠕蟲（worm）是會不斷地大量自我複製，並藉由網際網路的管道來散播（圖12-2），例如「Melissa」蠕蟲是透過電子郵件來傳播。由於電腦蠕蟲自我複製與散播的能力非常強，一旦發作，常會造成電腦、網路及郵件伺服器無法正常運作。

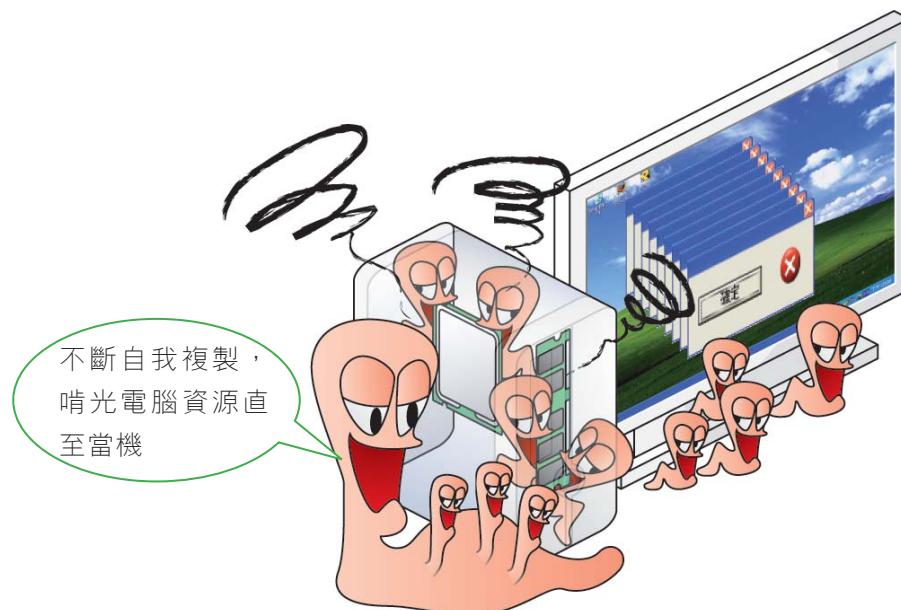


圖12-2 電腦蠕蟲

表12-2是惡意程式的特性比較。值得注意的是，目前所流行的惡意程式大多同時結合了多種特性，因此感染速度及破壞力更為強大。

表12-2 惡意程式比較表

特性比較 惡意程式	電腦病毒	特洛伊木馬程式	電腦蠕蟲
是否會感染其他檔案	✓		
是否需寄生在別的檔案或程式	✓	✓	
主要目的	惡作劇或破壞電腦系統正常運作	入侵他人電腦窺視或竊取資料	耗用電腦資源，使電腦無法正常提供服務

## 12-1.2 惡意程式的防範措施

常言道：「預防勝於治療」，要預防惡意程式，我們可以從**安裝防毒軟體及養成良好的電腦使用習慣**著手。

### 安裝防毒軟體

**防毒軟體**是一種可以偵測與刪除惡意程式的軟體（圖12-3），這種軟體所使用的防毒技術有很多種，目前較常見的是將電腦檔案與防毒軟體公司所蒐集到的**病毒碼**進行比對，以判別檔案是否已遭到惡意程式感染。

由於惡意程式不斷的變種與翻新，因此在安裝防毒軟體之後，還必須定期（例如：每次開機時）更新防毒軟體的**病毒碼**，才能有效防範惡意程式的入侵。

### 卡巴斯基



圖12-3 防毒軟體



### 參考案例

#### 木馬程式入侵，女子遭側錄

根據自由時報2008年12月1日報導，有名女子某天發現自己的出浴照，竟然被人張貼在部落格中，嚇得她花容失色！經過瞭解，原來她的電腦感染了「彩虹橋木馬程式」，駭客遙控她的視訊攝影機，錄下了她出浴的影像並將它張貼上網。

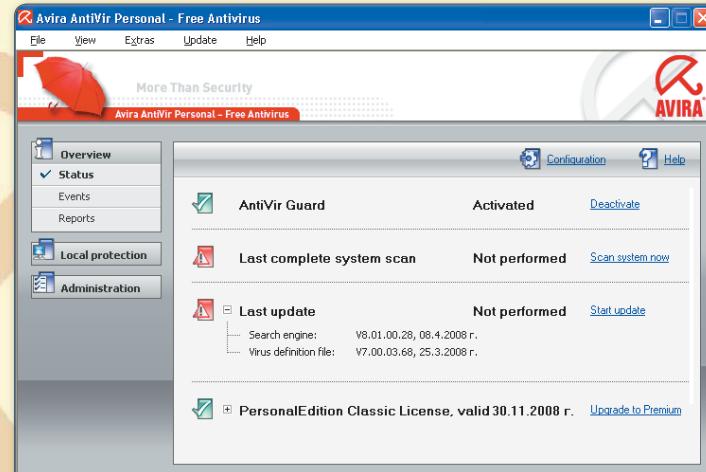
在感染木馬程式時，電腦多半不會出現特殊症狀，我們應養成定期掃毒的習慣，才能避免類似的事情發生。



## 免費防毒軟體－小紅傘

覺得一般防毒軟體太貴了嗎？不妨試試免費的防毒軟體「Avira AntiVir」（俗稱「小紅傘」）。小紅傘是免費的防毒軟體，其基本的防毒功能相當完備，因此受到許多人的愛用（圖12-4）。

圖12-4 小紅傘防毒軟體 ◉



除了小紅傘之外，網路中還有許多免費的防毒軟體及木馬掃除程式可供下載（表12-3～表12-4）。此外，我們也可以透過線上掃毒程式，來確認電腦中的檔案是否中毒。

表12-3 免費防毒軟體網站

軟體名稱	官方網站	語言
Avira AntiVir（小紅傘）	<a href="http://www.free-av.com/">http://www.free-av.com/</a>	英文
avast!	<a href="http://www.avast.com/index_cnt.html">http://www.avast.com/index_cnt.html</a>	中文
AVG Anti-Virus	<a href="http://free.avg.com/">http://free.avg.com/</a>	英文

表12-4 免費木馬掃除程式

軟體名稱	官方網站	語言
SpyBot Search & Destroy	<a href="http://www.safer-networking.org/ct/">http://www.safer-networking.org/ct/</a>	中文
Ad-Aware	<a href="http://lavarsoft.com/">http://lavarsoft.com/</a>	英文

## 養成良好的電腦使用習慣

要防範惡意程式的入侵，除了可以安裝防毒軟體之外，還必須養成良好的電腦使用習慣，才能減少電腦感染惡意程式的機會。

- **不使用來路不明的軟體**：來路不明的軟體（如網路流傳的盜版軟體）可能含有惡意程式。如果要下載軟體，應到軟體的官方網站或有公信力的網站下載。
- **不任意開啟來源不明的檔案**：網路上流傳的許多檔案經常含有惡意程式，我們應避免開啟來源不明的檔案。



<http://www.kaspersky.com/virusscanner> 卡巴斯基線上掃毒  
<http://housecall.trendmicro.com/apac/> 趨勢科技線上掃毒



● **避免瀏覽高危險群的網站**：色情網站及提供非法資源的網站（如盜版音樂交流網站）經常藏有惡意程式，我們應避免瀏覽這類高危險群的網站。

● **定期備份資料**：定期將資料備份在DVD、隨身碟等儲存媒體中（圖12-5），一旦電腦不幸遭惡意程式入侵，有助於重新找回遭破壞的資料。



### 12-1.3 電腦感染惡意程式的補救措施

如果電腦不幸遭到病毒、蠕蟲、特洛伊木馬等惡意程式的感染，可參照下列步驟來進行補救處理：

1. 使用防毒軟體進行電腦硬碟掃毒及解毒的工作。
2. 若防毒軟體無法解毒，可利用未受到病毒感染的電腦，上網查詢病毒相關資訊，並下載解毒程式。
3. 立刻關閉感染病毒的電腦，避免病毒感染其它檔案或造成更大的損害；若感染的病毒是透過網路傳播，應先拔除網路線，暫時阻斷電腦與外界的連結。
4. 重新開機，開機時按 **F8** 鍵，以安全模式進入Windows作業系統。
5. 使用解毒程式進行解毒的工作。

若進行以上所述的補救處理之後，電腦仍無法回復正常運作，便需請專業人員來協助處理。





## 如何防範USB病毒

我們常用的隨身碟、行動硬碟等外接式設備，通常使用USB埠來與電腦連接，這類設備雖然方便使用與攜帶，但要小心，它們是散播USB病毒的常見管道。

USB病毒會在外接式設備中建立自動播放檔（autorun.inf），當我們將感染到此種病毒的設備插到電腦上時，病毒檔案就會自動執行並傳染給電腦。電腦感染了USB病毒，可能會出現無法瀏覽檔案、無法連上網路等症狀。

USB病毒是透過autorun檔案來進行散播，我們可以連上『微軟下載中心』網站，下載並安裝停止作業系統自動播放功能的程式（圖12-6），來防範USB病毒的入侵。

**1<sub>step</sub>** 連上『微軟下載中心』網站

**2<sub>step</sub>** 在此輸入 "自動播放" 並搜尋

**3<sub>step</sub>** 按此下載停止自動播放的程式

The screenshot shows the Microsoft Download Center search results page. The search bar contains '自動播放'. A red arrow points to the search button labeled '進階搜尋'. Another red arrow points to the search results table, highlighting the first result: 'KB971029 : Windows XP 更新'.

( <http://www.microsoft.com/downloads/Search.aspx?displaylang=zh-tw> )

↑ 圖12-6 下載停止自動播放功能的程式



1. 志成愛玩線上遊戲，某天他下載別人分享的「自動練功程式」來使用，卻使得自己的虛擬寶物被盜取一空。請問這是因為該程式中可能含有下列何者？ (A)特洛伊木馬程式  
(B)編碼程式 (C)電腦蠕蟲 (D)防毒軟體。
2. 惡意程式通常會透過下列哪些管道來傳播？①電子郵件，②即時通訊軟體，③螢幕，  
④隨身碟 (A)①②③ (B)①②④ (C)①②③④ (D)②③。

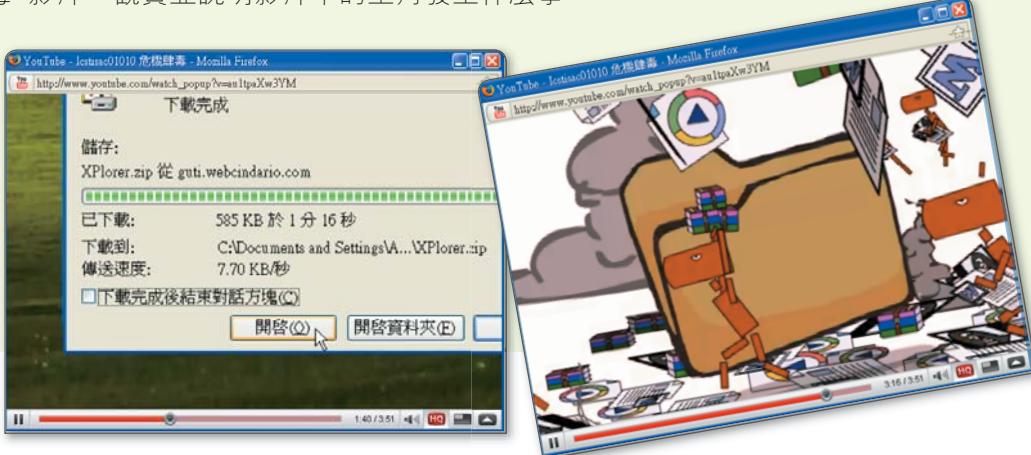
接下頁...



<http://www.dali.tcc.edu.tw/usbcleaner/> 提供防範USB病毒的資訊



3. 請連上<http://www.youtube.com/icstwebmaster>網站，開啟「國家資通安全會」提供的 "危機肆毒" 影片，觀賞並說明影片中的主角發生什麼事。



## 12-2 駭客入侵的問題

「駭客」是什麼人？他們可不是電影「駭客任務」中的人物，而是現實世界中的電腦犯罪者。根據美國FBI估計，全球每年因駭客攻擊所造成的損失，高達數千億美金；更令人憂心的是，駭客的犯罪率正逐年上升。以下將介紹駭客常用的攻擊手法，以及防範駭客入侵的措施。

### 12-2-1 駭客攻擊的手法

**駭客** (hacker) 一詞原來是指**熱衷鑽研電腦或網路破解技術的人士**，並不一定有惡意破壞他人電腦的意圖。但因現今報章雜誌、電影等都習慣以「駭客」代表電腦犯罪者，因此與蓄意破壞或犯罪的**怪客** (cracker) 已有混用的情形。

駭客通常具有相當豐富的電腦知識，犯罪者動機很多，如挾怨報復、為了獲取不法利益，或是為了證明自己的功力等。以下介紹幾種駭客常用的攻擊手法：

- **入侵網站**：透過網際網路入侵他人網站，竊取資料或篡改網站的內容。
- **網頁掛馬攻擊**：是指駭客在網頁中植入惡意程式，使用者只要連上這些網頁，電腦就可能感染惡意程式。





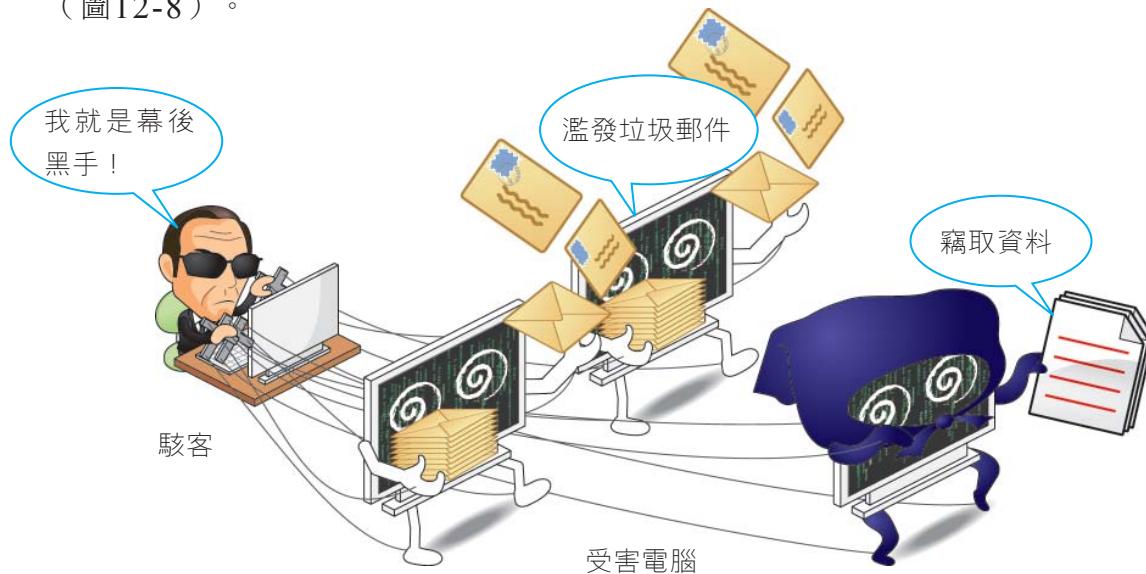
● **散布惡意程式**：製作並散布惡意程式，以炫耀自己的電腦能力，或竊取他人的私密資料，以獲取不法的利益。

● **阻斷服務攻擊（Denial of Service, DoS）**：藉由不斷地發送大量訊息，使被攻擊的網站癱瘓，而無法提供服務（圖12-7）。



▲ 圖12-7 阻斷服務攻擊

● **BotNet攻擊**：駭客透過網路散布具有遠端遙控功能的惡意程式，電腦一旦感染這種惡意程式，就會成為駭客手下的**殭屍電腦**。駭客常集結大量的殭屍電腦，來構成**殭屍網路**（BotNet），以進行濫發垃圾郵件、竊取他人個人資料等不法行爲（圖12-8）。



▲ 圖12-8 BotNet攻擊

● **零時差攻擊**：利用軟體本身的安全漏洞進行竊取資料、植入病毒等不法行爲。因為這種手法通常是駭客在發現軟體的安全漏洞後，立即發動攻擊，所以又被稱為「零時差攻擊」（Zero-day Attack）。



## 間諜軟體

間諜軟體 (spyware) 通常被設計成一個有用的小程式 (如密碼產生程式)，但卻會在暗地裡竊取使用者的個人資料 (如帳號、密碼)，或是做出騷擾的動作，例如不斷彈出廣告視窗、更換瀏覽器首頁、強制安裝工具列……等。

為了保護個人的隱私資料，我們應養成不安裝來路不明軟體的習慣。此外，我們也可安裝專業的反間諜軟體程式，如 Spyware Doctor (圖12-9)，來避免電腦遭到間諜軟體的入侵。



↑ 圖12-9 Spyware Doctor

## 12-2-2 駭客入侵的防範措施

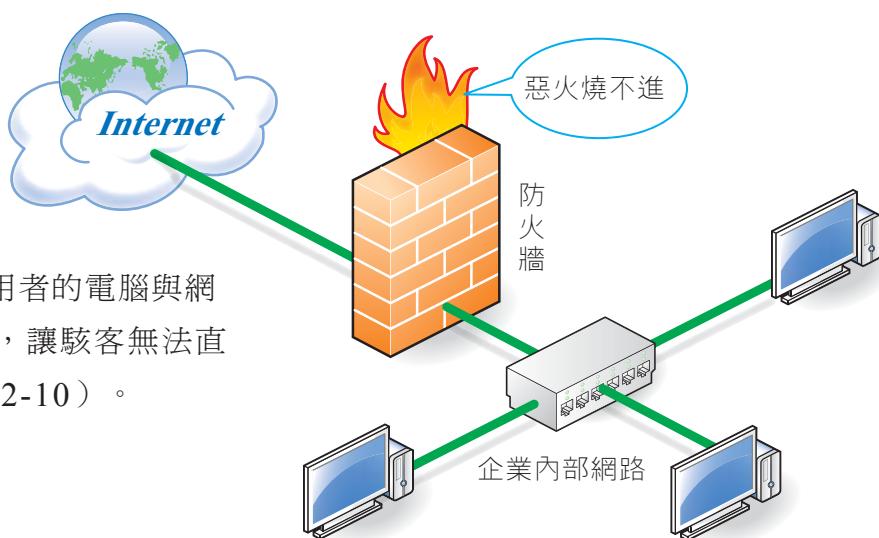
你知道一台沒有防護的電腦，在駭客眼中就像一頭肥羊嗎？如果同學以為自己的電腦不會被駭客「看上」，那可就太過樂觀了。要防範駭客的入侵，我們可以從安裝防火牆及養成良好的電腦使用習慣等方面來著手。

### 安裝防火牆

**防火牆** (firewall) 是一種可以用來過濾資料來源，以維護內部網路安全的軟體或硬體設備；它的運作原理類似於在使用者的電腦與網際網路之間建立一道防衛的城牆，讓駭客無法直接存取使用者電腦中的資料（圖12-10）。

#### TIP

Windows作業系統即內建有防火牆軟體，我們只要在控制台中點選Windows防火牆，即可進行防火牆的安全設定。



↑ 圖12-10 防火牆的運作示意圖



## 養成良好的電腦使用習慣

為避免駭客入侵，除了安裝防火牆之外，還須養成下列良好的電腦使用習慣：

- 配合軟體公司所發佈的更新訊息，下載並安裝修補程式。
- 妥善管理自己的帳號密碼，並定期更換密碼。
- 為避免駭客入侵竊取硬碟中的資料，機密資料最好儲存在隨身碟或光碟中。



### 參考案例

#### 網頁掛馬威脅高，知名網站成箭靶

據報導，屈臣氏、曾記麻糬等公司的網站都曾遭到「網頁掛馬」攻擊，使用者只要連上這些網站，電腦就可能感染惡意程式。

『資安之眼』、『大炮開講』等網站提供有最新遭惡意程式感染的網站名單，我們可以連上這些網站來查閱，以避免誤上「中毒」的網站而受害。



1. 所謂的「駭客」是指？ (A)奇裝異服的電腦從業人員 (B)電腦犯罪者 (C)網拍賣家 (D)線上遊戲玩家。
2. 下列哪些是常見的駭客攻擊手法？①入侵他人網站，②散布惡意程式，③阻斷服務攻擊 (A)①② (B)①③ (C)②③ (D)①②③。
3. \_\_\_\_\_ 可用來防範駭客入侵，以維護內部網路的安全。

## 12-3 網路釣魚

根據統計<sup>註</sup>在2008年間，全球每月約有3萬人遭「網路釣魚」的手法所騙，且有逐漸增加的趨勢。為了避免同學不慎落入網路釣魚的陷阱，造成財產或權益的損失，以下將介紹何謂網路釣魚，及其防範的措施。

### 12-3-1 何謂網路釣魚

**網路釣魚** (phishing) 是一種網路詐騙手法，駭客通常是建立一個與合法網站（如：知名銀行）幾乎一模一樣的網頁畫面，再發送電子郵件通知使用者登入假的網站進行身分驗証，以騙取使用者的帳號、密碼、信用卡卡號等私密資料，再利用這些資料，來從事不法的行為，例如竊取使用者的銀行存款。



## 12-3.2 網路釣魚的防範措施

為了避免落入電腦駭客所設下的「網路釣魚」陷阱，我們應養成以下良好的電腦使用習慣：

- **檢查網站是否合法**：合法的網站多半會向**認證中心（CA）**申請「憑證」，以證明自己是合法經營。我們要登入網站前，應先確認網站是否持有憑證（圖12-11）。



↑ 圖12-11 網站的登入畫面

- **使用具有反網路釣魚功能的瀏覽器**：目前IE、Firefox、Chrome……等新版本的瀏覽器都內建有反網路釣魚的功能（圖12-12），一旦使用者連上被歸類為黑名單的網站，就會出現警示訊息。



↑ 圖12-12 具有反網路釣魚功能的瀏覽器



- **檢查網址是否正確**：可先檢查網址類別，例如政府網站的網址類別應為gov，公司行號則為com，再檢查網址的機構名稱，例如YouTube網站的網址是 "youtube" 而非 "yuotube"。
- **不回覆索取個人資料的郵件**：收到索取個人資料的電子郵件時，應先求證，不要使用郵件中的電話與對方聯絡或直接回覆郵件。
- **不利用郵件中的連結登入網站**：如果要造訪網站，應該自己輸入網址，或使用值得信賴的搜尋引擎（如Yahoo!奇摩、Google等）來搜尋網站網址，再進行登入。



### 參考案例

#### 關鍵字搜尋藏「釣魚」，網路銀行受害！

網路釣魚詐騙的手法又翻新，民衆透過搜尋引擎找到的連結，可能是網址類似的釣魚網站，例如會有釣魚網站使用 "1andbank"（第1個字母為阿拉伯數字1）來偽裝為 "landbank"（台灣土地銀行）。

駭客常偽造銀行網站來進行詐騙，我們要登入網路銀行前，應該仔細檢查網址是否正確，或是連上行政院金管會網站 (<http://www.fscey.gov.tw/>)，再透過其提供的連結來造訪銀行網站。



- 1. 近年來經常有駭客假冒知名銀行或網站的名義，寄發電子郵件要求使用者回報自己的帳號與密碼，再利用這些資料來盜取使用者的銀行存款或個人資料。請問這種手法是屬於下列哪一種電腦犯罪行為？ (A)資料攔截 (B)電腦蠕蟲 (C)網路釣魚 (D)特洛伊木馬。
- 2. 請問下列哪一種做法，最有助於防範網路釣魚詐騙案件的發生？ (A)安裝防毒軟體 (B)時常備份檔案 (C)用電子郵件中的連結造訪銀行網站 (D)不回覆索取個人資料的郵件。
- 3. 連上微軟網站 (<http://www.microsoft.com/taiwan/protect/videos/default.mspx>)，觀看防範網路釣魚的宣導影片，以了解防範網路釣魚的方法。
  - (1) 按「保護您的家人免受線上詐騙干擾」主題的影片連結
  - (2) 觀看影片並記錄防範網路釣魚的方法



## 12-4 線上交易安全的問題

線上交易是另一種購物管道，具有便利、快速，不出門也能享受購物樂趣的好處，但卻也隱藏著個人資料外洩、身分遭盜用的風險。為了讓同學了解如何在網路上「買得安心」，以下將介紹線上交易的安全問題，以及保護線上交易安全的措施。

### 12-4-1 侵害線上交易安全的行為

線上交易是透過網際網路來傳送交易資料，在交易過程中，可能因為**交易者身分遭冒用**、**交易資料遭竊取**及**交易資料遭篡改**等侵害行為（圖12-13），而影響線上交易的安全。

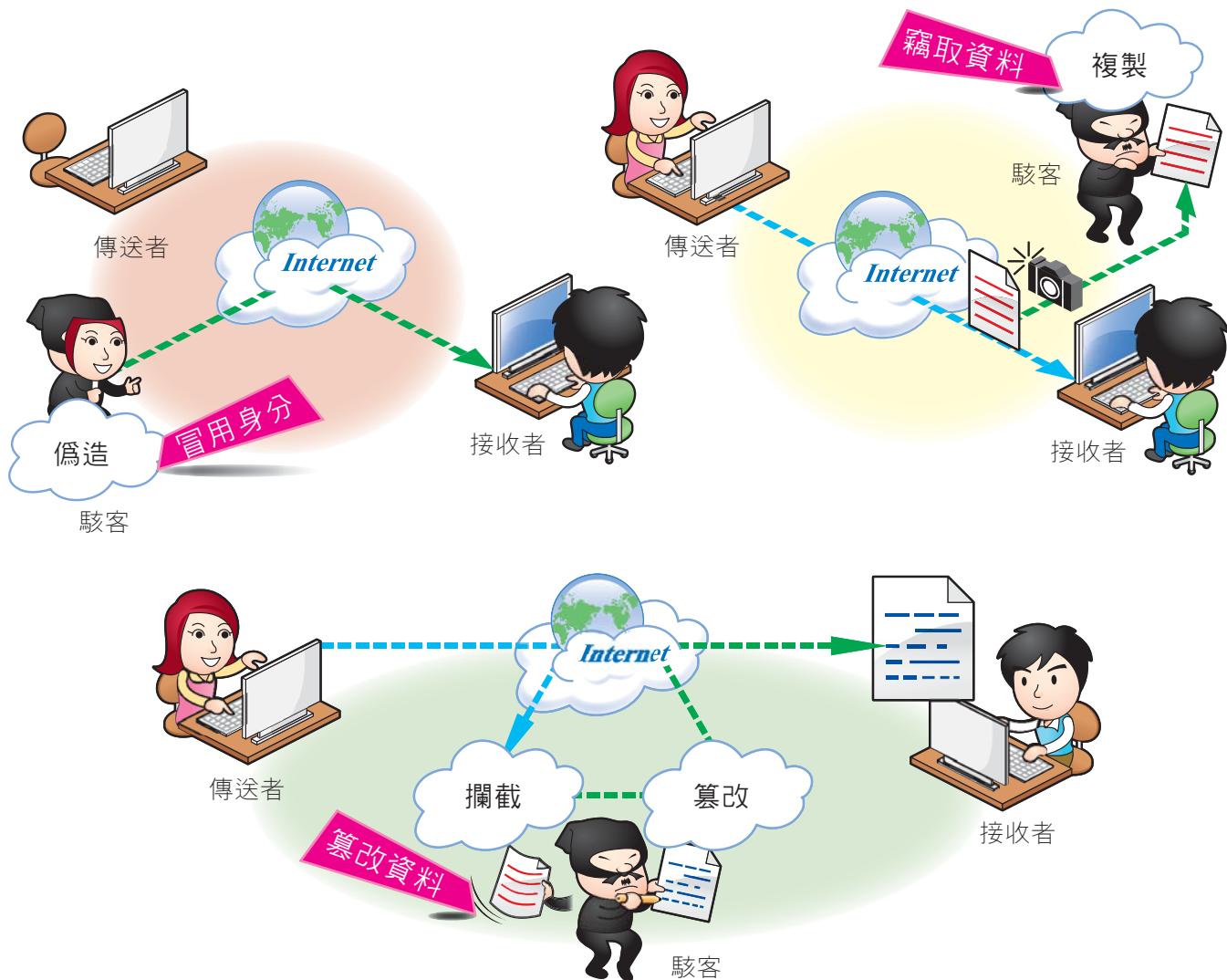


圖12-13 侵害線上交易安全的行為



## 12-4.2 線上交易安全的維護措施

要確保線上交易系統的安全，通常必須符合下列的安全要求：

- **身分驗證** (authentication)：確認交易者（消費者、商家、銀行）的身分，避免冒名頂替的情形發生。
- **資料隱密** (confidentiality)：確保交易資料在傳輸過程中不被他人窺知。
- **資料完整** (integrity)：確保接受方接收到的資料正確且未被篡改。
- **不可否認** (non-repudiation)：交易雙方不可事後否認其交易的事實。

**安全資料傳輸層** (Secure Socket Layer, SSL) 是Netscape公司為了保護網路上資料傳輸安全，而制定的一種安全規範。這種規範符合**資料隱密**、**資料完整**及可確認商家身分等線上交易安全的要求，同學在購物網站中購物，最好選擇有使用SSL規範的購物網站（如Yahoo!奇摩購物中心、露天拍賣、PayEasy），以確保交易資料傳輸的安全（圖12-14）。



↑ 圖12-14 『Yahoo!奇摩購物中心』網站



### 參考案例

#### 駭客盜取帳號，網拍賣家被「駭」

一名長期從事網拍事業的張小姐，某天瀏覽自己所經營的賣場時，驚見有人盜用她的帳號拍賣物品，且已有多名買家上當匯款，害得她長期經營的商譽毀於一旦，還差點背上詐欺的罪名。

為了防範類似案件的發生，提供拍賣服務的網站呼籲買賣家要特別小心保管自己的帳號資料，並善用網站所提供的安全措施（如Yahoo!奇摩安全憑證），以保護自己的權益。



## 數位憑證

由於SSL安全規範無法確認交易者的身分，易有冒名頂替的情形發生，因此許多提供重要金融交易服務（如網路股票下單、網路報稅）的網站，特別採用了可同時符合上述**身分驗證**、**資料隱密**、**資料完整**、**不可否認**等4項要求的**數位憑證**（Digital Certificate）機制，來確保交易的安全。

當我們向金融機構或政府單位申請取得數位憑證後，必須將數位憑證的檔案匯入至瀏覽器中（圖12-15），才能在進行線上交易時，發揮數位憑證的功能。

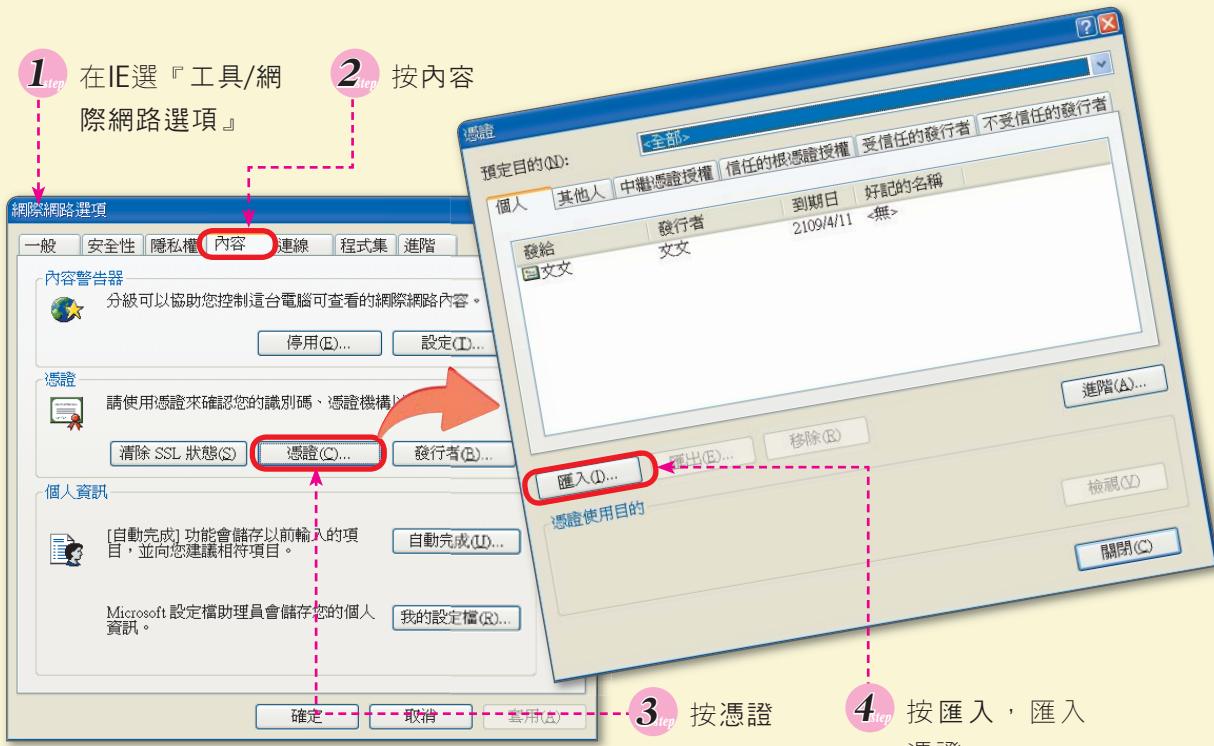


圖12-15 匯入數位憑證的方法



1. 下列何者是用來保護線上交易安全的規範？ (A)SSL (B)http (C)ftp (D)bbs。
2. 下列何者不是維護線上交易安全的要件？ (A)身分驗證 (B)資料隱密 (C)資料完整 (D)資料分類。
3. 網址開頭為 \_\_\_\_\_，表示該網站使用SSL安全規範。



# 本章習題

## ● 選擇題 ●

- \_\_\_ 1. 鴻廷的電腦最近只要一開機，就會出現關機倒數計時的畫面，請問會發生這種現象，最可能的原因是？ (A)電源供應不穩定 (B)感染惡意程式 (C)顯示器故障 (D)網路頻寬不足。
- \_\_\_ 2. 「I Love You」惡意程式會不斷自我複製，並藉由電子郵件來散播，會造成全球約150億美元的損失。請問它是屬於下列哪一種類型的惡意程式？ (A)特洛伊木馬程式 (B)DoS攻擊 (C)開機型病毒 (D)電腦蠕蟲。
- \_\_\_ 3. 「網頁掛馬」是一種駭客的攻擊手法，駭客在正常的網頁中植入惡意程式，使用者只要瀏覽網頁，電腦即可能感染病毒。請問我們可以透過下列哪種方法來防範這類攻擊？ (A)安裝防毒軟體 (B)使用外接式硬碟 (C)時常進行磁碟重組 (D)設定帳戶密碼。
- \_\_\_ 4. 下列觀念敘述，何者不正確？ (A)使用防毒軟體，仍需經常更新病毒碼 (B)不可隨意開啟不明來源電子郵件附加檔案 (C)重要資料燒錄於光碟儲存，可避免受病毒感染及破壞 (D)將資料備份於硬碟中不同的資料夾內，可確保資料安全。
- \_\_\_ 5. 下列何者不是預防電腦病毒的基本做法？ (A)將重要的資料隨時備份 (B)不開啟任何來路不明的電子郵件 (C)登入系統之密碼應不定期更換 (D)使用具有合法版權之軟體。
- \_\_\_ 6. 下列哪一種做法與電腦病毒的防治最沒有關係？ (A)使用合法軟體 (B)定期備份資料 (C)定期執行磁碟重組 (D)安裝防毒軟體。
- \_\_\_ 7. 下列哪一項做法，最不可能防範駭客的入侵？ (A)定期備份 (B)定期修補程式漏洞 (C)定期更改密碼 (D)安裝防火牆軟體。
- \_\_\_ 8. 下列何種電腦犯罪模式，是針對特定主機不斷且持續發出大量封包，藉以癱瘓系統？ (A)木馬攻擊 (B)網路蠕蟲攻擊 (C)阻絕攻擊 (Dos) (D)隱私竊取。
- \_\_\_ 9. 透過網路報稅快速又方便，但也隱含報稅資料被駭客竊取的危險。請問下列哪一項動作對於網路報稅的安全防護沒有助益？ (A)安裝防火牆 (B)更換最新型的CPU (C)掃瞄電腦是否感染病毒 (D)更新防毒軟體的病毒碼。
- \_\_\_ 10. SSL是許多線上交易網站所採用的安全規範，請問下列何者不屬於SSL的保護範圍？ (A)防止資料在傳送過程中遭窺視 (B)防止資料在傳送過程中遭篡改 (C)確認商家身分 (D)確認買家身分。

## ● 多元練習題 ●

1. 請連上『線上安全網』網站 ([http://www.icst.org.tw/online\\_security/home.htm](http://www.icst.org.tw/online_security/home.htm))，點選「二分鐘測驗」超連結，來進行電腦安全等級測驗，以了解自己的電腦是否有足夠的安全防範措施（防止駭客的入侵及電腦病毒的感染）。

# 電腦達人 3 招

## 第 1 招

### 如何選擇合適的ADSL寬頻上網方案？

(可配合11-1節介紹)

想要找到「俗擶大碗」的寬頻上網方案，來享受飆網的樂趣嗎？首先要先評估自己的網路使用需求，再比較幾家ISP業者推出的方案，才能「貨比三家不吃虧！」。以下以台灣固網的ADSL寬頻上網方案（如下圖）為例，說明在選擇ADSL上網方案時，應評估的3個主要項目。

The screenshot shows a web browser window for Taiwan Telecom's broadband service. The URL is [https://service.tfn.net.tw/TFN\\_TFN\\_OK\\_SOLUTION/TFN\\_OK/data/adsl\\_product/97q3\\_01.aspx](https://service.tfn.net.tw/TFN_TFN_OK_SOLUTION/TFN_OK/data/adsl_product/97q3_01.aspx). The page title is "台灣固網 [ADSL寬頻上網] - Mozilla Firefox". A cartoon character is on the right.

**A 頻寬**: Points to the "頻寬" column in the table, which lists download/upload speeds: 256K/64K, 1M/64K, 2M/256K, 4M/1M, and 8M/640K. The 8M/640K option is highlighted with a red box.

**B 月租費**: Points to the "月繳" (Monthly Payment) column in the table, which lists monthly fees: 無 (None), 219元/月, 259元/月, 559元/月, and 419元/月. The 419元/月 option is highlighted with a red box.

**C 接線費**: Points to the "年繳" (Annual Payment) column in the table, which lists annual fees: 1,080元/年 (平均月繳90元), 2,388元/年 (平均月繳199元), 2,868元/年 (平均月繳239元), 6,420元/年 (平均月繳535元), and 4,788元/年 (平均月繳399元). The 4,788元/年 option is highlighted with a red box.

超值方案一年期方案(新申裝)		
新申裝	轉換 ISP	
<b>頻寬</b>	<b>月繳</b>	<b>年繳</b>
256K/64K	無	1,080元/年(平均月繳90元)
1M/64K	219元/月	2,388元/年(平均月繳199元)
2M/256K	259元/月	2,868元/年(平均月繳239元)
4M/1M	559元/月	6,420元/年(平均月繳535元)
<b>8M/640K</b>	<b>419元/月</b>	<b>4,788元/年(平均月繳399元)</b>

※現在辦8M就送卡巴斯基兩年防毒防駭!!  立即申請

**注意事項**

- 轉換用戶係指轉換ISP用戶,由他家ISP業者所提供之ADSL或光纖上網服務,轉換至台灣大寬頻上網服務
- 以上費用為上網月租費，另需支付電路月租費256K/64K-170元/月、1M/64K-365元/月、2M/256K-393元/月、4M/1M-672元/月、8M/640K-500元/月，使用中華電信替代電路之用戶，電路資費依提供電路服務業者之規定繳交。
- 申辦超值方案用戶自第13月起，若未申請加入新方案或為不續約之意思表示者，視為立同意書人同意以本同意書所約定之費率依原指定頻寬繼續租用台灣固網上網服務；申辦以下方案（流行方案用戶自第13月起，哈燒方案第25個月起，轉換超值與轉換流行方案第15個月起，轉換哈燒方案第27個月起）若未申請加入新方案，視為立同意書人同意以台灣固網當時公告費率或促銷優惠費率繼續依原指定頻寬繼續租用台灣固網上網服務。
- 電路費相關規定：使用台灣固網電路：第一次電路接線費\$1500，簽約2年之客戶，減免優惠為\$500，若租用未達2年退租者，須補繳\$1000；使用中華電信替代電路：電路相關資費依中華電信之規定繳交。

(<https://service.tfn.net.tw/>)

#### 台灣固網ADSL方案

如果我們對網路使用的需求為瀏覽網頁、收發信件、玩線上遊戲等，建議申請ADSL上網方案中的2M/256K頻寬即可。

## 第2招 如何讓惡意網站無所遁形？

(可配合12-1節介紹)

網路上有許多含有惡意程式的網站，只要不小心連上這些網站，電腦就可能感染電腦病毒，或受到惡意程式的攻擊。例如視窗畫面經常跳出廣告訊息，令使用者不勝其擾；或是瀏覽器首頁被改成特定網頁，且無法重新設定（俗稱綁架首頁）。

你知道有什麼工具可提醒我們避開這類網站嗎？「雲端WTP掃毒引擎」是一款能偵測惡意程式的防毒工具，它會在我們要連上含有惡意程式的網站時，提出警訊，並阻斷連線，以避免我們誤入這類網站。我們可以從趨勢科技網站（<http://www.trendmicro.com.tw/wtp/micro/index.asp>）下載這套免費的工具來安裝使用。

雲端WTP掃毒引擎 ➔



## 第3招 如何保護「不能說的祕密」－檔案加密

(可配合12-2節介紹)

你的電腦中是否存放一些不想被他人窺視的資料（如心情日記）呢？我們可以利用檔案加密軟體（如檔案護照、AxCrypt），為這些私密的檔案加密，如此一來，就不怕「不能說的祕密」曝光了！

檔案加密後，檔案內容會被轉換成亂碼；如果要將檔案解密，必須輸入檔案加密時所設定的密碼，才能將檔案還原，如下圖所示。



檔案加密示意圖



## 分組練習機

# 環遊世界 8 分鐘



### ☆ 活動目標

- 藉由此項活動，讓同學認識世界新七大奇蹟。
- 綜合練習網際網路應用服務的操作，包含資料搜尋、知識搜尋、檔案下載、部落格、電子郵件等。

### ☆ 活動進行

- 請同學連上『Google地球』的網站 (<http://earth.google.com/>)，下載並安裝Google地球程式。
- 請將同學分成數組，並請各組同學利用維基百科找出以下世界新七大奇蹟中任3個景點的所在國家。
  - (1) 泰姬瑪哈陵      (2) 圓形競技場      (3) 奇琴伊察      (4) 馬丘比丘
  - (5) 救世基督像      (6) 佩特拉古城      (7) 長城
- 請各組同學開啓Google地球，並勾選**3D建築物**核取方塊；接著在**目的地**欄輸入奇蹟名稱（格式為『國家 奇蹟名稱』，如『中國 長城』），再按 **Enter** 鍵。
- 按 **Alt + PrintScreen** 鍵擷取螢幕的畫面，並在小畫家中按 **Ctrl + V**，最後存檔 (\*.jpg)。



- 要求同學至部落格發表一篇文章（如「世界奇蹟」），並在文章中插入擷取的圖檔，再利用電子郵件，將該篇文章的網址寄送給老師。