CHAPTER 12

網路安全與保護

電腦中毒很麻煩，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」，大家都要關心哦！

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（**mal**icious **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：LINE）、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。

早期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：每逢米開朗基羅生日（03/06）發作，會使硬碟資料無法讀取
檔案型	多半是寄生在副檔名爲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：每逢13號星期五發作，會刪除硬碟中的執行檔
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：播放影集「大榔頭」的歌曲後發作，會使硬碟資料無法讀取
巨集型	通常寄生在含有VBA巨集的文件檔案（如.doc、.xls）上；當使用者開啓被感染的檔案後，此類病毒便會開始進行破壞電腦系統的運作	台灣NO.1：每逢13號發作，會大量開啓新Word文件，耗用電腦資源

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）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）。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。

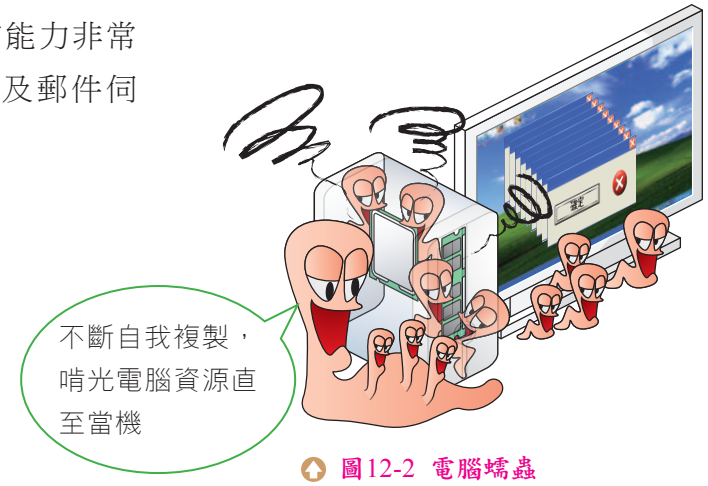


圖12-2 電腦蠕蟲

有很多惡意程式會刻意設計在特定時間或條件下才會發作，這類惡意程式俗稱為**邏輯炸彈**（logic bomb）。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

惡意程式 / 特性比較	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

參考案例

USB病毒大流行，專門感染蘋果作業系統

蘋果公司的作業系統一向給人安全性較高的印象，但近期出現一種針對蘋果作業系統的「超級病毒」，只要設備下載了非官方版的App程式，即可能感染病毒，且會將病毒傳染給以USB相連接的設備，造成一傳十、十傳百的效果。目前已有數十萬台蘋果設備染毒，官方呼籲民眾切勿使用未通過審核的程式。

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，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。

小辭典－病毒碼

病毒碼是從惡意程式中所擷取出來的一段程式碼。

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。表12-3為常見的防毒軟體。

表12-3　常見的防毒軟體

防毒軟體	免費中文版	下載網址
Avira AntiVir（小紅傘）	✓	http://www.free-av.com/zh-tw/
avast!	✓	http://www.avast.com/
AVG Anti-Virus	✓	http://www.avgtaiwan.com/
Norton（諾頓）	30天試用	http://tw.norton.com/
PC-cillin	30天試用	http://www.pccillin.com.tw/
Kaspersky（卡巴斯基）	30天試用	http://www.kaspersky.com.tw/

參考案例

付費防毒軟體App也有造假！民眾下載應小心

有一款防毒軟體「Virus Shield」號稱有最完善的防毒功能，要價3.99美元，上架一週即衝上App付費下載排行榜第一名。沒想到的是，這款防毒軟體竟無防毒功能，唯一的功能是將界面上的 ✗ 變成 ✓ 。經消費者檢舉後，Google Play商店已將這款App下架，並保證未來會加強上架App軟體的檢查。

資安專家提醒，民眾應使用信譽良好的防毒軟體，否則這種來路不明的軟體，可能不僅不防毒，還會害你的個資外洩。

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。
- **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，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。

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

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。

課外閱讀

檢查App應用程式權限

你知道有些App軟體，可能會暗藏病毒，或是偷偷地蒐集你的個資嗎？若在安裝App時不留意，有可能「引狼入室」。以Google Play為例，下載App時，會顯示該App可存取的權限，如果發現有不合理的權限要求，就應避免下載此軟體。圖12-3為應用程式權限的範例。

例如照明用的「手電筒」App，若要求儲存檔案、撥打電話，就可能「不懷好意」

圖12-3 應用程式權限的範例

節練習

____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。請問這是因爲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。

3. 請連上http://www.youtube.com/icstwebmaster網站，開啓「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。

參考案例　駭客入侵智慧汽車，遠端操控油門、方向盤

近年來智慧型汽車越來越多，這些汽車通常具備有自動控速、倒車、網路連線等智慧功能，但是要小心！已證實駭客能入侵美國知名汽車公司出產的智慧汽車，並遠端控制汽車加速、減速、轉向、關閉引擎，可蓄意製造車禍。目前車廠已緊急召回140萬輛智慧型汽車，並更新系統以加強系統安全。

- **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。

參考案例　網頁掛馬威脅高，知名網站成箭靶

據報導，屈臣氏、會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。

同學請注意，電腦應安裝防毒軟體並定期更新病毒碼，以免因誤上「中毒」的網站而受害。

- **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（Denial of Service, DoS）攻擊**：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12-4）。

圖12-4 阻斷服務攻擊

- **殭屍網路（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**，以進行濫發垃圾郵件、竊取他人個人資料等不法行為（圖12-5）。

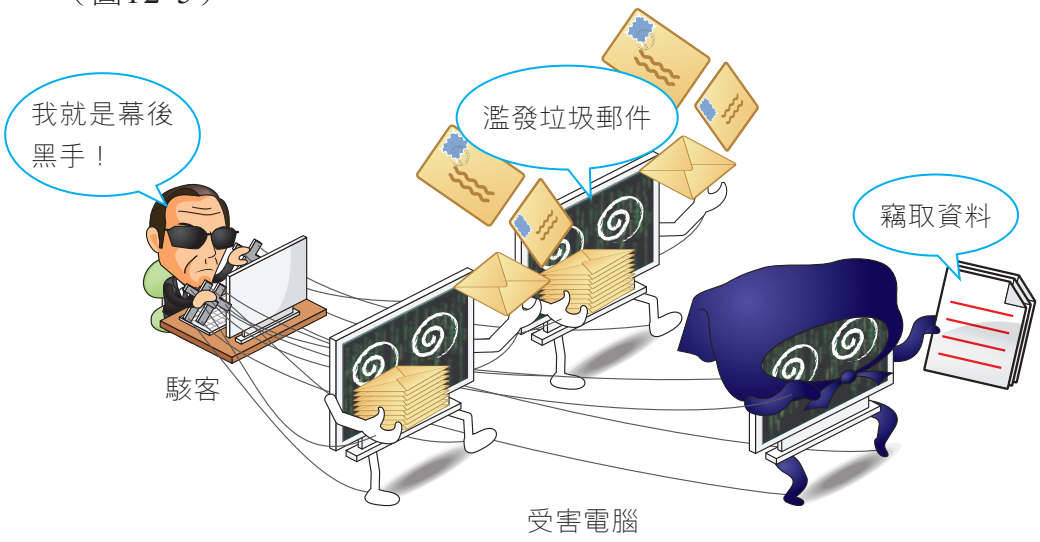


圖12-5 BotNet攻擊

參考案例　駭客遠端操控監視攝影機系統，癱瘓雲端服務

駭客不僅會入侵他人電腦、手機，當作DoS攻擊的犯案媒介，就連監視攝影機也遭殃。資安業者發現有駭客遠端操控由900台監視攝影機所組成的殭屍網路，來攻擊雲端服務，影響全球數百萬名用戶的權益。

專家提醒，只要是有連網的3C產品，都應設定密碼，以免淪為駭客為惡的工具。

- **零時差攻擊**：利用軟體本身的安全漏洞進行竊取資料、植入病毒等不法行為。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）。

參考案例　駭客藉由Java漏洞，攻擊政府及企業電腦系統

網頁中許多遊戲、動畫都需要Java程式才可正常執行。在2015年，Java又出現系統漏洞，駭客可藉由此漏洞，遠端遙控受害者的電腦。至今已有政府單位、微軟、蘋果、Facebook等公司都因Java漏洞，遭駭客零時差攻擊，許多客戶資料因此流失，造成嚴重的損失。

資安專家提醒，零時差攻擊發生後，軟體公司通常會立即發布修補程式，使用者應配合軟體公司的提醒進行程式更新，以免成為「受害者」。

- **字典攻擊法**：駭客蒐集常用來作為密碼的字串，做成「字典」檔，再利用程式依序從「字典」檔中讀取這些字串，並透過一一嘗試的破解方式，來找出正確的密碼。取得密碼後，駭客會進行不法行為，例如竊取個人資料、冒用身分等。許多網站要求登入帳號密碼時，還需輸入「圖形驗證碼」（圖12-6），即是為了防範字典攻擊法。

（http://www.momoshop.com.tw）

圖12-6 圖形驗證碼

- **網路釣魚（Phishing）**：駭客建立與合法網站極為相似的網頁畫面，誘騙使用者在網站中輸入自己的帳號、密碼、信用卡卡號，以取得使用者的私密資料。

小辭典－社交工程

是指利用社交手段（如套關係、冒充身分）來降低他人戒心、博取他人信任，再趁機騙取機密資料的犯罪手法，例如網路釣魚即是社交工程的一種。

參考案例　網購搶便宜，小心落入「網路釣魚」陷阱

一名老先生想透過網拍買相機，他瀏覽一間出價特別低的賣場網站後，便有偽裝成線上客服的騙子要求老先生連至一個看似正常，其實是釣魚網站的網頁，老先生不疑有他輸入銀行帳號密碼，幾天後，才發現存款已被掏空。

民眾勿存貪便宜的心態，以免被騙，也務必要在正規的電子商務網站內進行交易，消費權益才能受到保障。

- **勒索軟體（Ransomware）**：駭客入侵他人電腦，將受害者電腦中的所有檔案加密，並威脅受害者於期限內交付贖金才解密，否則電腦中的所有檔案將無法解密。

參考案例　電腦遭綁架，3天內須交付「贖金」

勒索軟體入侵台灣，許多企業紛紛受害。某公司的一名會計，因誤點駭客發送的郵件，導致會計部伺服器被勒索軟體加密無法使用，必須付錢才能解開，綁架期間造成公司嚴重損失。

資安專家提醒，在台灣被勒索的裝置，半年內就超過13萬個，民眾應提高警覺，不要任意開啓來路不明的郵件或附加檔案，以免成為綁架對象。

課外閱讀

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。

爲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12-7），來避免電腦遭到間諜軟體的入侵。

圖12-7 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12-8）。

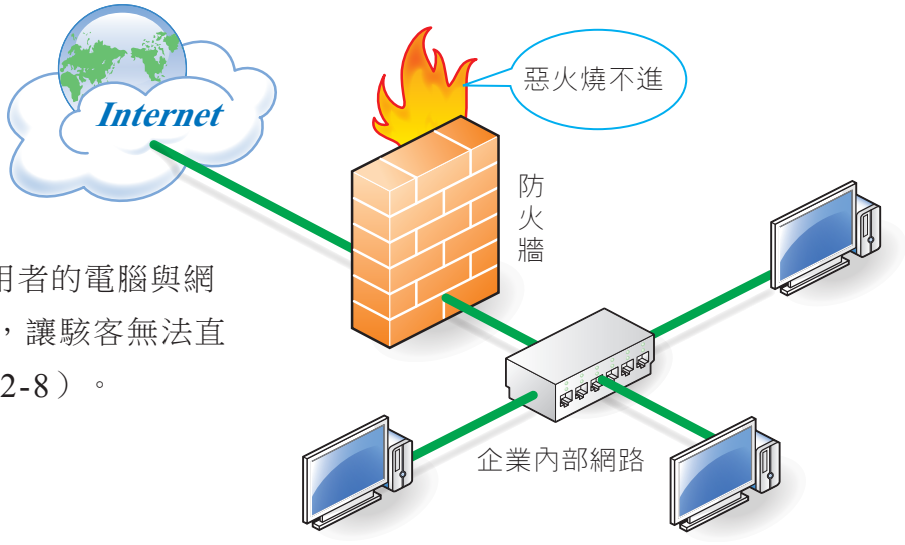


圖12-8 防火牆的運作示意圖

Tip

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

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：

- 配合軟體公司所發布的更新訊息，下載並安裝修補程式。
- 遵照以下原則，設定及管理密碼。
  - 密碼至少8個字元以上。
  - 密碼宜使用英文大小寫、數字、符號混合。
  - 避免使用個人相關的資料（如生日）作為密碼。
  - 不定期更換密碼，且勿隨意透露自己的密碼。

小辭典－懶人密碼

指簡單好記的密碼，例如"1111"、"1234"、"password"、"abc123"……等。這類密碼最容易被駭客以「字典攻擊法」破解，請同學一定要避免使用這類密碼。

- 公用電腦容易遭受電腦病毒感染，因此應避免使用公用電腦進行線上交易，以免私密資料外洩。
- 若需要在網站中登入帳號、密碼等私密資料，應確認網址是否正確，例如政府網站的網址類別應為gov，公司行號應為com，再檢查網址的機構名稱，例如YouTube網站的網址是"youtube"，而非"yuotube"。
- 若有郵件、簡訊、即時訊息（如LINE訊息）要求你登入某個網站，可能是網路釣魚的手法，請勿直接點按郵件或訊息中的連結來登入網站，建議同學自己輸入正確網址，或利用值得信賴的搜尋引擎（如Google）來連結至該網站。
- 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。

節練習

____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. 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。

4. _____可用來防範駭客入侵，以維護內部網路的安全。

課外閱讀

防火牆的運作原理

在網際網路傳輸的資料，是被分割成許多特定大小的封包（packet），每一個封包中除了資料本身之外，還會包含來源位址、目的位址、來源埠位址、目的埠位址、……等附加內容，防火牆可以透過檢查封包中的附加內容，來過濾與控管封包的進出（圖12-9）。表12-4所列為防火牆過濾規則設定的範例[註]。

表12-4　防火牆過濾規則設定的範例

規則	來源端		目的端		允許/拒絕
	位址	埠位址	位址	埠位址	
1	內部（如192.168.1.0）	任何	某一含毒網站（如66.249.6.3）	網站伺服器（80 port）	拒絕
2	內部（如192.168.1.0）	任何	任何	任何	允許
3	任何	任何	內部（如192.168.1.3）	網站伺服器（80 port）	允許
4	任何	任何	內部（如192.168.1.2）	郵件伺服器（25 port）	允許
5	任何	任何	任何	任何	拒絕

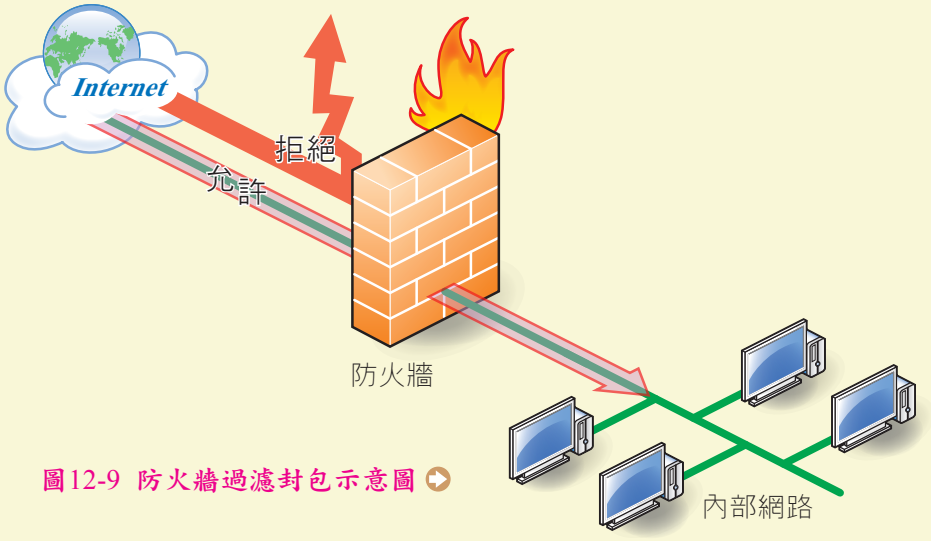


圖12-9　防火牆過濾封包示意圖

以下說明表12-4中各項規則可達成的效果：

- 規則1：拒絕內部網路連線至已知含有病毒的網站。
- 規則2：允許內部網路連至所有前項規則未拒絕的連線。
- 規則3：允許任何來源端存取內部網路的網站伺服器。
- 規則4：允許任何來源端存取內部網路的郵件伺服器。
- 規則5：拒絕所有前項規則未允許的連線。

註　本範例係為了方便教學，刻意簡化防火牆的過濾規則，實務上的防火牆過濾規則會比本範例複雜許多。

12-3 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。

12-3.1 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12-10），而影響線上交易的安全。

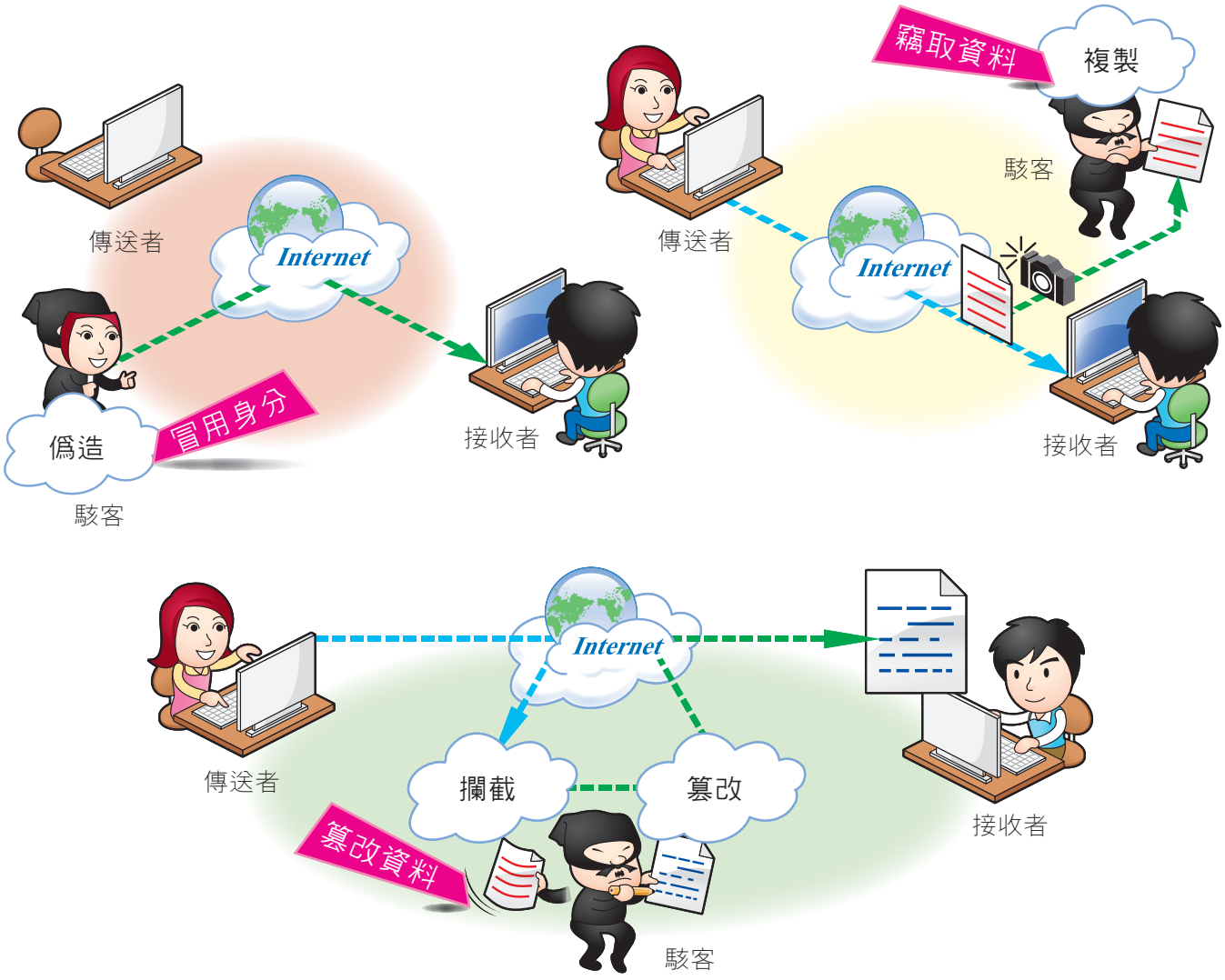


圖12-10 侵害線上交易安全的行為

12-3.2 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12-11）。

圖12-11 『Yahoo!奇摩購物中心』網站

參考案例

警察也被騙，網購要當心

2015年，一名女警在網路上購買化妝品，嫌犯假冒客服，通知她匯款時誤選了分期付款，須聽從他的指示操作ATM來解除分期，女警便聽從指示將帳戶款項都轉帳給嫌犯，結果存款被騙光。

警方提醒，詐騙手法層出不窮，只要被要求額外的匯款，都應撥打警政署165專線或向賣家確認，以免落入不肖人士所設計的陷阱裡。

註 不同的瀏覽器（如Firefox、Chrome）或版本，鎖狀的圖示位置可能會有差異。

課外閱讀

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12-12），才能在進行線上交易時，發揮數位憑證的功能。

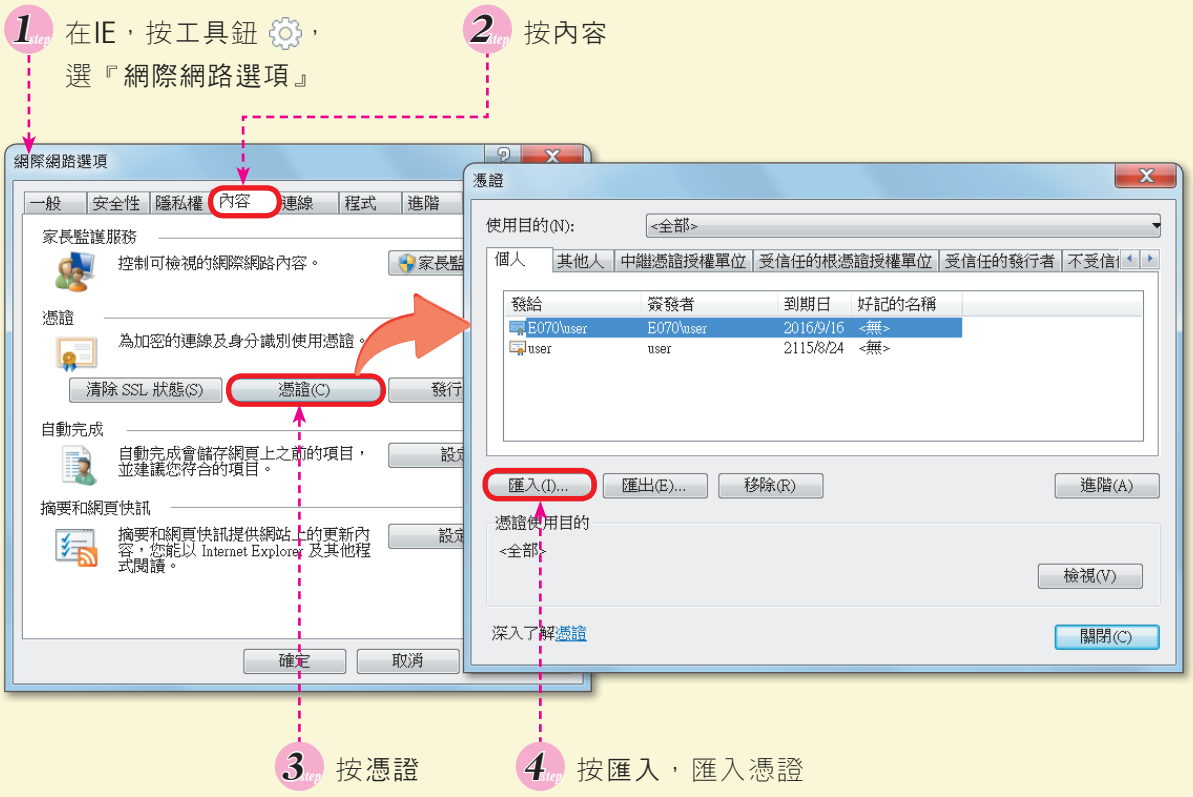


圖12-12 匯入數位憑證的方法

節練習

____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，曾造成全球約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)不可隨意開啓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)不開啓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)阻斷服務（DoS）攻擊 (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. 請同學在搜尋引擎輸入關鍵字 "AOEMA線上安全網"，連上『線上安全網』網站，並點選「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2招

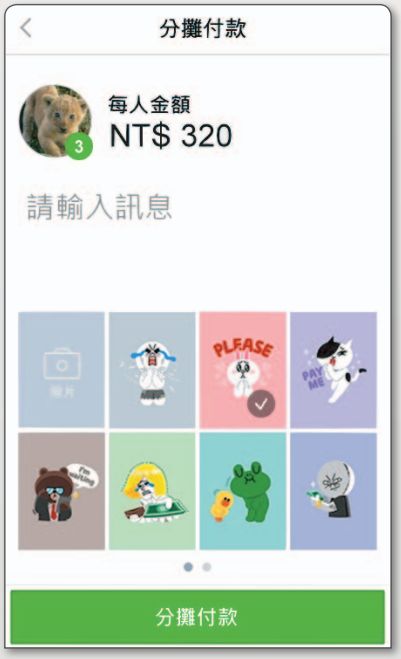
第1招 LINE的應用，真不賴！

（可配合11-1.1節介紹）

想必同學對LINE一點都不陌生，不過你知道除了可以用來聊天之外，還可以用LINE做什麼嗎？它提供有筆記本、相簿、訊息自動重傳、桌面建立好友聊天捷徑、LINE PLAY虛擬人偶遊戲等功能，以下再介紹幾個特別的功能與服務：

- 限時聊天：可設定訊息在對方已讀後2秒、5秒或至多1週即刪除，講秘密不怕留下痕跡。
- LINE極短片：提供濾鏡、動態標題、背景音樂等功能，輕鬆製作30秒以內的影片，立即與LINE好友分享。
- LINE Pay行動支付：LINE與多家銀行合作，推出儲值支付帳戶，使用者只要綁定信用卡資料或儲值現金，即可在LINE Pay合作的線上商店購物，或透過LINE通訊錄好友名單轉帳。
- LINE MART買賣市集：只要有LINE帳戶就可以在MART市集買東西、賣東西，是一個簡潔、容易上手的購物平台。
- LINE Manga電子漫畫：提供多部日本人氣漫畫電子書，可讓LINE使用者線上免費閱讀，還會附贈漫畫貼圖哦！
- LINE Webtoon「素人」漫畫：不僅可免費閱讀漫畫，還可將自己繪製的漫畫上傳至該平台與他人分享，人人都可以是漫畫家。
- LINE HERE位置分享：一個向左走、一個向右走，遲遲找不到相約的好友嗎？只要透過該軟體，就可以動態顯示好友目前的所在位置，不怕迷路。

限時聊天



LINE Pay行動支付

LINE Manga電子漫畫

第2招　免費擴增手機的儲存空間

（可配合11-2.6節介紹）

擔心手機中的資料太多，儲存空間不足嗎？透過雲端硬碟Dropbox，可讓我們將手機內的資料儲存於該雲端硬碟，待需要使用時再下載至手機。另外，Dropbox還提供如下圖所示的「照片即時備份」功能，可將手機中的相片自動上傳備份至網路上。

1 啓動手機中的Dropbox App

2 按登入鈕，登入帳號、密碼

3 按此鈕，切換至相機上傳頁面

4 按開啓鈕，即會執行「照片即時備份」功能

5 按此鈕，以管理雲端硬碟中的照片（如刪除照片、分享照片至臉書等）

Dropbox「照片即時備份」功能的操作畫面

分組練習棧

環遊世界8分鐘

活動目標

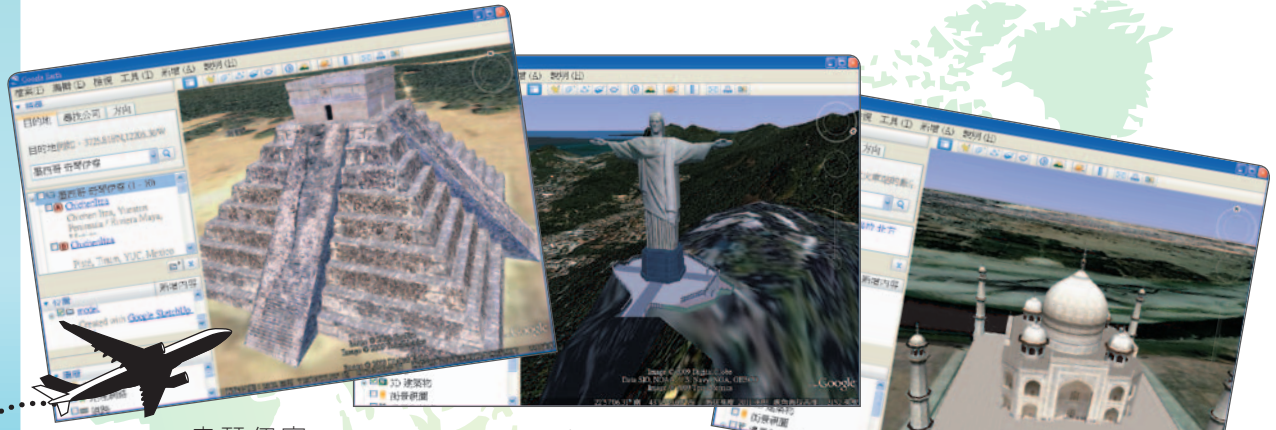
1. 藉由此項活動，讓同學認識世界新七大奇蹟。
2. 綜合練習網際網路應用服務的操作，包含資料搜尋、知識搜尋、檔案下載、部落格、電子郵件等。

活動進行

1. 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。
2. 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
3. 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（格式爲『國家 奇蹟名稱』，如『中國 長城』），再按 Enter 鍵。
4. 按 Alt + PrtSc SysRq 鍵擷取螢幕的畫面，並在小畫家中按 Ctrl + V，最後存檔（*.jpg）。



奇琴伊察　救世基督像　泰姬瑪哈陵

5. 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。

Note...