# 第**12**章 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！

## 惡意程式的問題

dglxasset[6]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？為了保護自身的權益，我們應學會如何防範惡意程式的入侵。

### 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，都屬於惡意程式的一種，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。這類程式大多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x）：

表x 電腦病毒的種類

|  |  |  |
| --- | --- | --- |
| 類型 | 說明 | 舉例 |
| 開機型病毒 （系統型病毒） | 寄生在磁碟片的啟動磁區（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 |
| 檔案型病毒 | 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 | 十三號星期五病毒 |
| 混合型病毒 | 兼具開機型及檔案型病毒的特性，除了會感染啟動磁區之外，還會感染執行檔 | 大榔頭病毒 |
| 巨集型病毒 | 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病毒 |

⮚ 特洛伊木馬程式

【特洛伊木馬程式】（Trojan horse）是將惡意的程式暗藏在正常的檔案中，一旦使用者開啟檔案，電腦就會感染特洛伊木馬病毒。這種病毒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x 特洛伊木馬程式



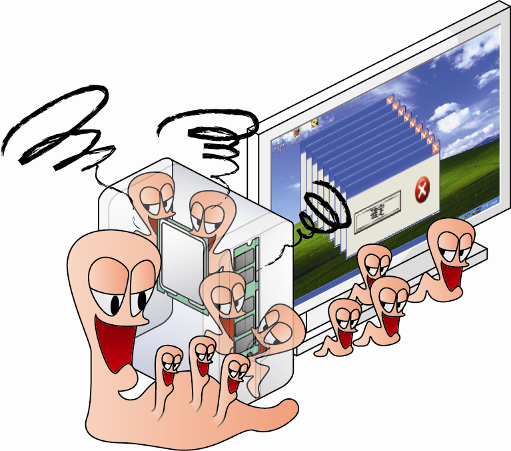
偽裝成遊戲，其實暗藏竊取檔案的惡意程式

⮚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，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12-31

圖x 電腦蠕蟲



會不斷大量自我複製，導致電腦因資源不足而癱瘓

表x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。

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 | 否 |
| 是否需寄生在別的檔案或程式 | 是 | 是 | 否 |
| 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 |

### 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X），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病毒感染。

!!!小辭典：【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。

圖x 防毒軟體 卡巴斯基（左）；Pc-cillin（右）

按此可更新病毒碼

-------案例：木馬入侵，女子遭側錄---------

有名女子某天連上自己的部落格，赫然發現自己的出浴照被人張貼在部落格中，嚇得她花容失色！經過瞭解，原來這名女子的電腦感染了「彩虹橋木馬程式」，駭客透過這種程式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。

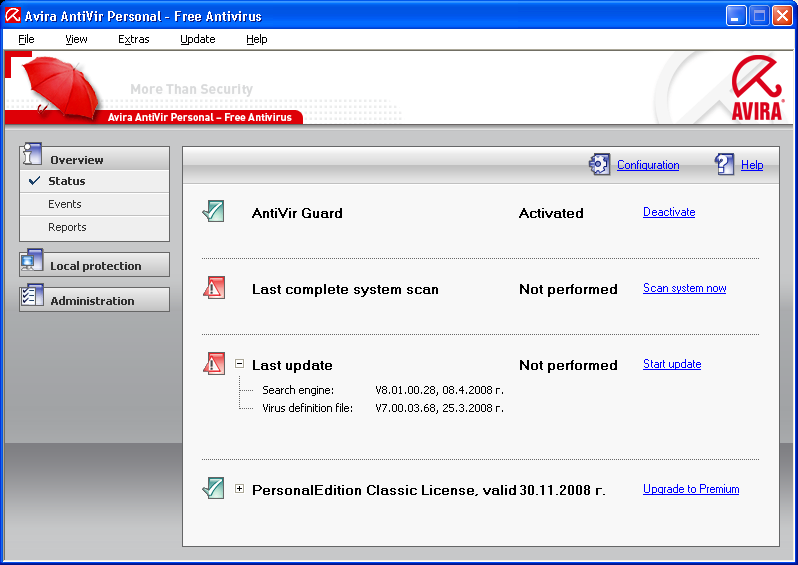
警方提醒，感染木馬程式時，電腦多半不會出現特殊徵狀，我們應養成定期掃毒的習慣，才能避免類似的情事發生。

----------------------------------------------------

---------------課外閱讀：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x 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，以下列出數款評價優良的軟體，同學可上網瀏覽或下載。

表x 免費防毒軟體網站

|  |  |  |
| --- | --- | --- |
| 軟體名稱 | 官方網站 | 語言 |
| AviraAntiVir | http://www.free-av.com/ | 英文 |
| avast! | http://www.avast.com/index\_cnt.html | 中文 |
| AVGAnti-Virus | http://free.avg.com/ | 英文 |

表x 免費木馬掃除程式

|  |  |  |
| --- | --- | --- |
| 軟體名稱 | 官方網站 | 語言 |
| SpywareDoctor（間諜醫生） | http://www.pctools.com/zh/ | 中文 |
| Ad-Aware | http://lavasoft.com/ | 英文 |

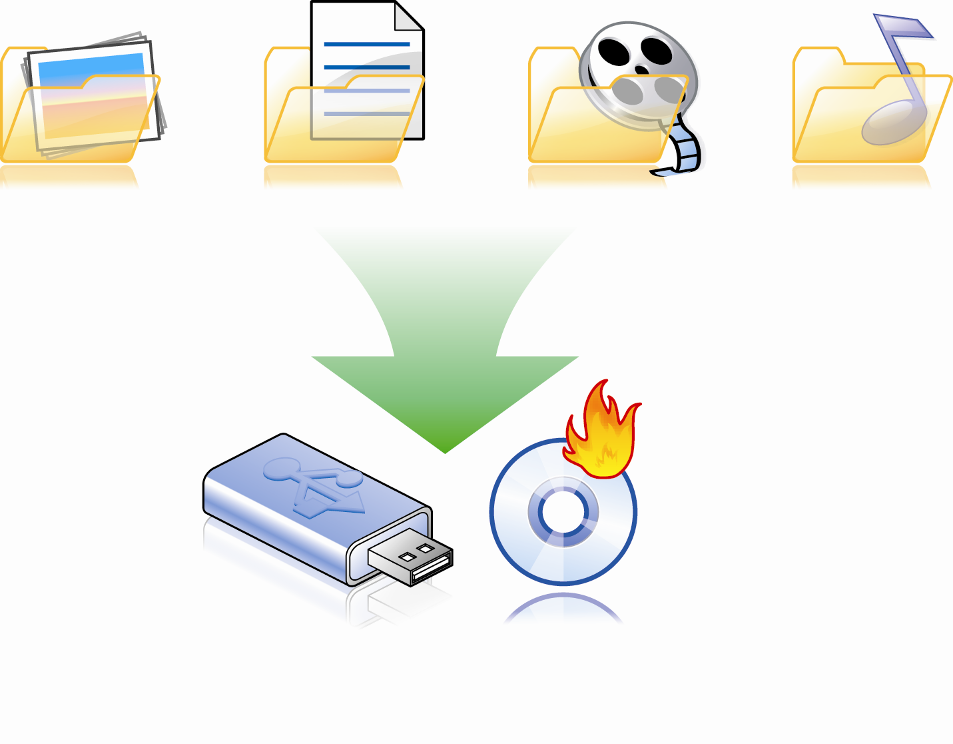
--------------------------------

[養成良好的電腦使用習慣]

要防範電腦病毒的入侵，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，才能減少電腦感染病毒的機會。

* 【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）經常含有惡意程式，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x），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。

圖x 定期備份資料 將資料備份在DVD、隨身碟等儲存媒體中



備份

我的照片

我的文件

我的影片

我的音樂

備份至隨身碟

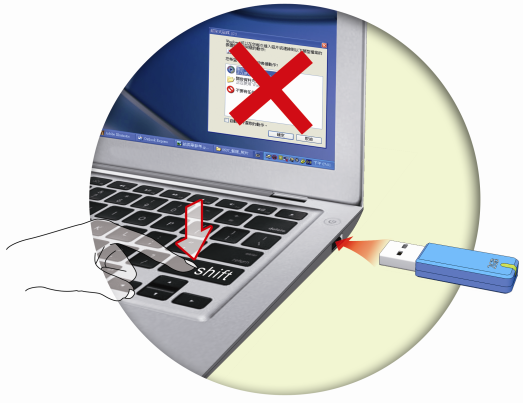
燒錄成光碟

----課外閱讀：如何防範USB病毒-----

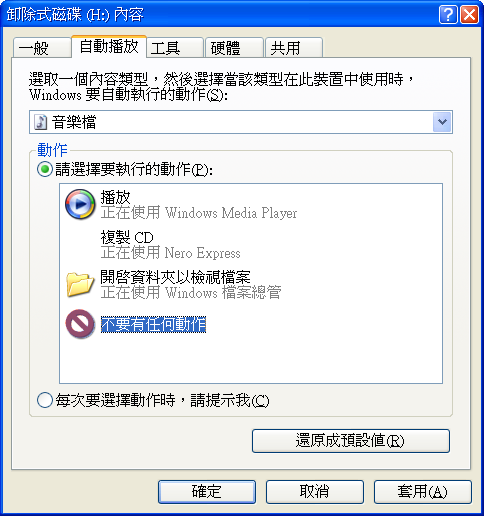
我們常用的隨身碟、行動硬碟等外接式設備，通常使用USB port來與電腦連接，這類設備雖然方便使用與攜帶，但要小心，它們是散播USB病毒的常見管道。

USB病毒會在外接式設備中建立自動播放檔（autorun.inf），當我們將感染有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，或是出現「程式發生錯誤」的訊息。

USB病毒是透過autorun檔案來進行散播，我們可以藉由關閉Windows作業系統的自動播放功能（圖x），來防範USB病毒的入侵。



按住shift鍵



STEP1：按住 <shift> 鍵不放，再插入外接式設備

STEP2：在新增的磁碟機按右鍵，選『【內容】』

STEP3：按【自動播放】

STEP4：將每一種資料類型，皆設定成不要執行任何動作

按此下拉式方塊，可選擇不同的資料類型

圖x 停止自動播放功能的方法

---------------

[感染惡意程式的補救措施]

如果電腦不幸感染到惡意程式，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，可利用未受到感染的電腦，上網查詢惡意程式的相關資訊，並下載解毒程式
3. 立刻關閉電腦，避免惡意程式感染其它檔案或造成更大的損害；若感染的惡意程式是透過網路傳播，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。