# Home Network Security (家用網路安全)

這份文件提供一份觀念性的家用者關於網路連線的安全風險與對策，特別是專線使用者或寬頻用戶（例，如 cable modems 及 DSL），然而，這份文件同樣適用於傳統的撥接上網用戶（也就是利用 modem 連線上網的使用者）。

## 1. 電腦安全（Computer security）

### A. 什麼是電腦安全？

電腦安全就是一種防止與偵測未經授權而使用你的電腦的程序，事前的檢測動作幫助你發現及停止未經授權使用者（入侵者）對電腦系統的使用：幫助你瞭解是否有人企圖入侵你的電腦，及他們對你做了什麼。

### B. 為何我需要關心電腦安全

我們將電腦運用在很多地方，例如：銀行業務、投資、購物與透過 E-mail 與人聯絡，雖然你並不習慣將聯絡方式在網際網路溝通環境上加密，但可能因此陌生人可以閱讀你的私人信件，或用你的電腦去攻擊其他人的系統，或是檢視你的個人金融資訊等不可預期的後果。

### C. 有誰會想要入侵我的家用電腦

入侵者(也就是所謂 hackers,attackers,或是 crackers)通常採取的入侵攻擊方式是把對方當作跳板，他們所想要的是獲得你電腦的控制權，並用之以攻擊入侵其他人的系統。

取得控制權之後他們將有能力隱藏他們真實的位址，當展開攻擊時，尤其是在對付高階、大型的電腦系統，例如：政府當局的網路系統或是金融、商業等規模較大的知名網站。甚至是透過撥接網路連接上 Internet，玩個駭客攻擊程式或是發一封偽造 e-mail 給你的朋友或是親人，你的電腦都有可能會成為目標。

入侵者能夠任意地監控你的電腦，或是格式化你的硬碟、入侵網路周邊設備及竄改電腦中的資料而造成損失。

### D. 入侵家用電腦是多麼容易的

很不幸的，入侵者總是可以從電腦軟體中發覺新的漏洞（通常稱為 holes），而日益複雜的軟體也使得徹底測試電腦系統安全愈來愈困難。

當漏洞被發掘，電腦軟體廠商通常會發展出相對的修補程式並指出問題所在，但去下載並安裝、或是正確地設定讓作業系統更安全的運作通常是我們使用者的責任，在 CERT\CC（電腦網路危機處理中心）會接到大部分的電腦入侵事件回報，若系統管理員有時時更新、安裝修補程式，並正確的設定電腦軟體，這些入侵事件將得以被預防。通常，應用軟體會有一些設定去讓外部使用者能夠使用你的電腦（遠端遙控的功能－remote control），除非有再作另外的安全設定，例如：聊天軟體能夠允許外部使用者執行特殊的命令；或

是利用瀏覽器，當你按執行按鈕時都有可能讓外部使用者去執行、置換一些有害的程式進入你的電腦。

## 2. 技術（Technology）

下面這個章節對 Internet 上的運用的連線技術作一些基礎的介紹，這是一些初學的終端使用者所應牢記在心的，但並不包含所有的基礎研究技術，而每一個小節對不同的題目有簡單的介紹，此章節有一份確切的技術介紹，下面包含了較多資訊的連結，能提供給有興趣深入瞭解的人。

### A. “寬頻”(broadband)是什麼意思？

“寬頻（Broadband）是一般高速網路的通稱。在這篇文件當中，提到所使用的纜線數據機（cable modem）或是 DSL（Digital Subscriber Line ）連接上 Internet 即被稱為寬頻網路連接，例如一般利用撥接數據機所提供的每秒 56k 頻寬便不能稱為寬頻，至少是超過每秒 1MB 的連接速度才被用以寬頻稱呼。

### B. Cable modem 如何運作？

纜線數據機（Cable modems）允許讓單一或是一整個網絡上的電腦利用電視的訊號纜線設備連接上網，通常 cable modem 利用一張乙太網路卡連接上電腦，並且提供超過每秒 5MB 的傳輸速度。
因為纜線的業者將一整個鄰近的區域都納入同一個區域網路，使 cable modem 傳輸速度通常低於他所能提供的最大值，尤其在尖峰時刻，又特別能夠體會得到他速度的緩慢，且較其他的連接網路方法使用者，更有受到封包監聽及未受保護的資源分享的危險！

### C. DSL 如何運作？

DSL（Digital Subscriber Line）不像 cable modem，而是提供給使用者專用的頻寬，因為使用的連接網路方法不同，使得 DSL 的最大頻寬小於 cable modem 最大頻寬，且專用的頻寬僅在使用者家中到 DSL 系統提供業者的中央機房這一段，而並不保證整個所運用到的網路。
使用 DSL 並不像 cable modem 容易受到封包監聽，但仍是有許多安全問題存在於 DSL 與 cable modem 的連接段。

### D. 寬頻服務與撥接上網服務之不同？

傳統的撥接上網，是只有用到時才撥號連接上網，也就是說，當有需要用到網路時才連接上網，例如要傳送一封 e-mail 或是下載一個網頁，只要沒有資料需要被傳送，或是經過一段閒置的時間，連接即會被切斷，在大多數的撥接中，撥接上網通常連接到 ISP 的數據機，去獲得一個被分配的動態 IP 位址，且每一個撥接的 IP 位址並不會重複，所以，入侵者便較難（並非不可能，只是較困難）利用系統服務中的漏洞去取得電腦控制權。
寬頻的服務則是一直保持連接的，因為當有資料需要傳遞的時候它並不需經過撥接設定，家中使用的電腦透過網路卡（NIC）一直保

持連線，等待傳輸資料或接收資料，所以 IP 位址也就很少改變，容易成為有心人的攻擊目標。
此外，寬頻服務的提供業者通常提供固定範圍的 IP 位址給家庭使用者，所以或許入侵者並不清楚哪一個特定的 IP 位址是屬於你，但至少，他們能夠知道某一 ISP 業者的固定 IP 範圍，這也使得家中使用者的電腦容易成為目標。

**以下表格提供一份撥接與寬頻服務的比較：**

| | 撥接 | 寬頻 |
|---|---|---|
| 連線型態 | 撥接上網 | 永遠連線 |
| IP 位址 | 每次撥接皆改變 | 靜態或極少改變 |
| 連線速度的比較 | 慢 | 快 |
| 遠端控制的功能 | 電腦必須連上網才有機會 | 電腦總是開啟，所以在任何時間都能控制 |
| ISP-提供的安全機制 | 極少甚至沒有 | 極少甚至沒有 |

*撥接與寬頻的比較*

**E. 寬頻和我平常上網的運作有何不同？**

公司組織及政府通常運用多種安全的層級去保護網路，從防火牆到資料的保密性，此外他們也有許多成員幫忙維護網路及保持網路的暢通。
雖然 ISP 業者有責任去維護他們所提供給你的網路服務，在你身旁也可能有專門的人員在維護你的家用電腦系統，但最終的維護人員仍舊是自己，所以事實上自己仍是要為所用的電腦負最大的責任去更新、保全系統以防止意外的或是惡意的入侵行為。

**F. 什麼是通訊協定？**

通訊協定（protocol）即是一種定義良好的敘述，讓電腦能夠透過網路彼此溝通，簡言之，通訊協定定義電腦間講話的共通語言文法。

**G. 什麼是 IP？**

IP 代表的是” Internet Protocol”他能被想像成一種電腦在網路上使用共通的語言，已有很多詳盡的探討文件說明 IP，所以在此文件並不詳述，但為了去了解如何保護你的電腦安全去瞭解 IP 仍舊是非常重要的，提供以下連結包括 IP addresses, 靜態 VS 動態位址 static vs. dynamic addressing,NAT、TCP 和 UDP Ports、TCP/IP 概觀……..

http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part1/

http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part2/

**H. 什麼是 IP 位址？**

IP 位址能夠想像成電話號碼一般，當你想要撥電話給某人，第一件事即需要知道他的電話號碼，同樣的當一台在網路上的電腦要傳送資料給其他電腦，也就需要知道目的端電腦的 IP 位址，IP 位址通常是 4 位數的十進位號碼，例如, 10.24.254.3 及 192.168.62.231。

**I. 什麼是靜態與動態位址？**

靜態 IP 通常為 ISP 業者永久不變地指派一個或多個 IP 位址給每一位使用者，這個位址不會隨著時間而改變，然而若是一個已被分配的 IP 無人使用，則便造成了浪費，既然 ISP 所擁有的 IP 位址有限，則 ISP 業者就得好好利用所擁有的 IP 位址。

動態 IP 位址能夠讓 ISP 業者更有效率地使用 IP 位址，使用動態 IP，每一個 IP 位址將會隨著時間而改變，當一個 IP 位址無人使用，則系統會將之自動地分配給下一個需要的人，以提高 IP 位址的使用效率。

**J. 什麼是 NAT？**

網路位址轉換（Network Address Translation NAT）提供一個將網路上私有 IP 位址隱藏但仍允許電腦使用網路資源的方法，NAT 能夠用在很多方面，但使用頻率最高的是將之應用在虛擬 IP（masquerading）上。

使用 NAT masquerading 可以讓許多在同一區網的設備共同使用一個相同的 IP 連接上網路，也就是說家庭使用者能夠讓多台電腦共用一個 cable modem 或是 DSL 所提供的 IP 位址，而不用要求 ISP 業者分配多餘的 IP 位址，使用這種方法，ISP 所分配的 IP 能夠是靜態的亦能夠是動態的，且大多數的防火牆支援此 masquerading 技術。

**K. 什麼是 TCP 與 UDP 連接埠？**

TCP (Transmission Control Protocol) 和 UDP (User Datagram Protocol)兩者都是 Internet Protocol（IP），當網路上兩部電腦使用 IP 去做溝通，則 TCP 和 UDP 允許兩部電腦的應用程式（例如 services）做溝通。

就像是電話號碼及信箱地址可能由多人共用，公司中的應用程式（例如：e-mail，檔案伺服器、網頁伺服器等）在同一個 IP 位址上執行，連接埠號（ports）用來辨別是 e-mail 或是網頁的資料，每一項服務的連接埠號在每台電腦上所使用的是唯一的號碼，TCP 和 UDP 都使用連接埠號的機制，一些常用的埠號例如：80 是作 Web 服務;25 是作 e-mail 服務;53 則是 DNS 服務。

**L. 什麼是防火牆？**

防火牆的 FAQ (http://www.faqs.org/faqs/firewalls-faq/) 定義其為單一或是一個群組系統，用於設定網路之間的控制規則，在這份文件中，防火牆被區分為兩種形式：

*Software Firewall*—個人電腦使用的特殊軟體

*Network Firewall*---專用的設備用來保護單一台或多台的電腦
兩種型態的防火牆皆允許使用者去設定在他們所保護的系統內部連接的執行規則，許多的防火牆亦提供設定某些在所保護的電腦上的服務允許通過與否，且大部分的防火牆能夠讓使用者依照個人需求去客製化自己所需的規則。

**M. 防毒軟體為我們做什麼？**

有許多的防毒軟體以不同的運作方式執行，端看製作的廠商如何去實作他們的軟體，通常的作法是去檢視檔案及記憶體中可能的已知病毒，防毒軟體由廠商所提供的病毒碼去比對，以知道是怎樣的病毒。
每天都會有新的病毒被發現，而最有效的防毒方法則是更新至最新的病毒碼，將它安裝在你的電腦中，所以更新病毒碼是相當重要的。
還有很多病毒相關的資訊，請參考以下連結網頁：

http://www.cert.org/other_sources/viruses.html

## 3. 家用者的電腦安全風險

**A. 有怎樣的風險？**

資訊的安全與三個部分有關：
***機密性（Confidentiality）***--資訊能夠被有所有權限的人取用並執行。
***直接使用（Integrity）***--資訊的取得通常被並授權給授權者使用。
***可取用的（Availability）***--資訊通常提供給那些需要他們的人。

這一些觀念如同法人組織與政府一般同樣適用於家庭的網路使用者，就像是你不會讓陌生人任意的去閱讀你的文件一樣，你可能也會希望將你在電腦上的工作保持隱密，例如在確認你的投資、發 e-mail 給你的親人及朋友時，並且保證你所輸入電腦的資訊完整無誤當下一次你又需要它時。

有一些的危險是來自於入侵者經由網路的惡意攻擊及濫用你的電腦，而有一些則不是（例如：硬碟損毀、被偷竊等），壞消息是你可能無法去為每一個可能的危險做防備計畫；而好消息是你可以透過一些簡單的步驟，降低你所可能遭遇的威脅，不管是來自於惡意或是偶發的事件。
在進入教導你如何保護自己電腦之前，以下先做一些風險的介紹：

**B. 對你電腦的惡意濫用**

下面列出一些常見的方法，是入侵者常用來獲取家用者電腦控制權的方法：

1. **特洛依木馬程式**
   特洛依木馬程式是一種常用的方法去設法讓你的電腦安裝"後門程式"，它能讓入侵者在你所毫無知覺的情況下，或是更改電腦的設定，或是感染電腦病毒，下列的連結文件提供更多的資訊：
   http://www.cert.org/advisories/CA-99-02-Trojan-Horses.html

2. **後門程式與遠端管理者程式**
   在視窗的電腦環境下有三個入侵者常用來取得遠端控制的程式：BackOrifice, Netbus, 以及 SubSeven，這些後門程式或是遠端管理執行的程式一旦安裝即可讓遠端的使用者操控你的電腦，我們建議參考 cert 的漏洞回報，對於 BackOrifice 如何運作、如何防止及偵測皆有詳細的說明：
   http://www.cert.org/vul_notes/VN-98.07.backorifice.html

3. **DOS（Denial of Service）**
   另一種型態的攻擊稱之為 Denial of Service (DoS)攻擊，這種型態的攻擊造成你的電腦當機或是忙於處理資料，讓你無法正常操控你的系統，然而最新的修補更新程式已能避免此問題，以下連結將對 DOS 有更詳細的介紹：
   http://www.cert.org/advisories/CA-2000-01.html

   除了注意到不要成為 DoS 的目標之外，也注意不要讓你的電腦被利用成為攻擊別人的跳板。

4. **成為另一個入侵的跳板媒介**
   入侵者通常使用被入侵的電腦當作發動攻擊的基地，例如使用 DDoS 的工具就是一個例子，入侵者使用代理人程式（通常由木馬程式夾帶）植入被入侵的電腦，以等待指揮，當一定數量的代理程式被分散植入分佈在各地區的電腦後，即會對任何的電腦發動 DoS 攻擊，如此一來被入侵的電腦變成為入侵者的跳板。

5. **未保護的 windows 分享**
   未保護的 windows 分享，會被入侵者利用來入侵許多連接上網路的電腦，因為在網路上電腦安全是相互依賴的，所以一台電腦被入侵將不只是使用者的問題，更將造成其他電腦的威脅，很嚴重的問題便出現在一群未受保護的 window 分享的電腦，如下連結所列：
   http://www.cert.org/incident_notes/IN-2000-01.html
   另外一種造成惡意的及破壞性的程式碼，例如病毒、網蟲，利用視窗分享的環境加以繁殖，例如下列連結所描述的 911 網蟲：http://www.cert.org/incident_notes/IN-2000-03.html

6. **動態程式碼（JAVA，JavaScript，ActiveX）**

動態程式碼例如（JAVA，JavaScript，ActiveX）是讓網頁撰寫者利用來編寫網頁的程式語言，他們能夠以瀏覽器執行，另一方面也被入侵者拿來用以收集資訊，例如你所瀏覽的網站或是在你的電腦上執行一些惡意的程式碼，若是有可能的話，在瀏覽一些不熟悉或是你所不信任的網站，最好將 JAVA，JavaScript，ActiveX 的功能關閉。

而被人所熟知的 e-mail 軟體也是利用讀信軟體開啟 HTML 語法的程式碼，所以，在 JAVA，JavaScript，ActiveX 上的漏洞同樣出現在閱讀 e-mail 時。

在 http://www.cert.org/tech_tips/malicious_code_FAQ.html 有更多惡意程式碼的資訊。

而在 http://www.cert.org/archive/pdf/activeX_report.pdf 有 ActiveX 安全的資訊。

7. **交叉網站描述語言**

惡意的網站開發者會夾帶一些 script 傳送給網站，例如 URL 一些表單的程式碼或是資料庫的查詢，而當你發出需求時，惡意的 script 即會回應給你的瀏覽器。

你可能透過瀏覽器所接觸到的惡意 script 有：

- 按下網頁、e-mail 或是新聞群組的連結，而不知其將連往何處。
- 使用交談式網頁去瀏覽未受信任的網站。
- 瀏覽一個使用者會以 HTML 標籤格式發表言論的新聞群組。

在下列的連結能取得更詳細的惡意程式碼資訊：

CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests.

8. **E-mail spoofing**

E-mail spoofing 發生在當收到 e-mail 而真實的來源卻是從另外一部來源伺服器所發出，通常企圖造成使用者的危險，或是為取得一些敏感性的資訊（例如：password）

欺騙性的 e-mail 範圍從無害的惡作劇，到社交學程的活動都可能發生，以下是一些例子：

***系統管理者發 e-mail 要求使用者使用特定的字串當成他的密碼，或是核對帳號加以欺騙。***

***有權利發 e-mail 的人發信給使用者要求他們拷貝一份敏感性資訊或是密碼檔***

值得注意的是，當系統提供者偶然的要求你更改密碼，但大多數的合法系統業者絕不會去要求你利用 e-mail 去傳送密碼或是敏感資訊，若是你有察覺到有人散發有惡意企圖的 e-mail，你就該趕緊聯絡系統提供業者。

9. **E-mail 骨幹病毒延伸式的隱藏檔**

病毒及其他一些惡意性的程式碼容易利用 e-mail 的附加檔傳播，在打開附加檔之前應該知道他確實的內容是什麼，而僅能

辨識出他的來源位址事實上是不夠的。例如梅莉莎病毒即是從一個認識熟悉的位址所夾帶，所以，惡意的病毒可能會夾在一些好玩或是誘人的程式之後。
絕對不要任意地執行一個你所不知道的程式，不論它的作者是你所信任某人或是電腦，當然更不要因為程式的好玩或是誘人而夾檔寄給你的朋友、親人或同事，因為他通常都可能會有特洛伊木馬病毒。

**10. 隱藏的延伸檔案**

Windows 作業系統對於已知的檔案型態，會加以隱藏，這是作業系統一般的預設值，而 e-mail 病毒及利用這個弱點加以感染，第一支巨集型的病毒"我愛妳"( VBS/LoveLetter)病毒即利用此方式感染，而經由附加檔夾帶一封" LOVE-LETTER-FOR-YOU.TXT.vbs"的檔案。下面所列的是一些已知的惡意程式：

- ***Downloader (MySis.avi.exe or QuickFlick.mpg.exe)***
- ***VBS/Timofonica (TIMOFONICA.TXT.vbs)***
- ***VBS/CoolNote (COOL_NOTEPAD_DEMO.TXT.vbs)***
- ***VBS/OnTheFly (AnnaKournikova.jpg.vbs)***

**11. Chat client**

網際網路上的聊天軟體，例如即時傳訊軟體或是網路(IRC)等，提供一個雙向的網路資訊轉換、傳播機制，聊天軟體，提供群組性的對話、網站或 URL 的平台，以交換任意型態的檔案。
因為聊天軟體，提供交換、傳送一些可執行的程式碼，所以它的風險性也就跟 e-mail 軟體一樣，當然也就該更去留意及限制聊天軟體所下載下來的檔案，尤其對於未知的檔案更該謹慎！

**12. 封包監聽（Packet sniffing）**

封包監聽是一種能夠從網路上傳遞資訊時擷取網路封包的程式，這些資訊包含使用者帳號、密碼等資訊，它們在網路上以明碼方式傳遞，入侵者能夠利用到這些被擷取到的成千成百的密碼或資訊展開攻擊，且安裝監聽程式並不一定需要系統管理員的權限。
相較於 DSL 與撥接上網，cable modem 的使用者有較高的風險，受到監聽程式的影響，因為它們全都是暴露在同一個區域網路之下，只要將封包監聽工具安裝在任何一台 cable modem 使用者的電腦，就能監聽鄰近的所有電腦。

## C. 意外事故與其他風險

除了連接網路的風險以外，還有許多風險是跟網路完全沒有關係的。這些大部分是眾所周知的，所以接下來的文件就為您詳細說明

這些風險。請注意，實踐以下降低風險的工作也可能幫助減少本文之前所提到與網路相關的風險性。

1. **磁碟錯誤**
   回憶一下之前所提到，可取用性為資訊安全的三要件之一。然而儲存在硬碟的資料卻因為機械的物理原因而存在較高的風險，可能使資料因為實體儲存媒介被破壞、摧毀、或遺失而變的不可取得。硬碟壞軌是個人電腦常遇到的資料遺失原因。定期的備份是唯一有效的補救方法。

2. **電源故障和突然高壓**
   電源問題（例如突然高壓，熄燈，以及部分停電）可以造成電腦的實體損毀，包括硬碟壞軌以及其他電子部分的傷害。常見的緩和方式包括使用瞬間高壓抑制器以及 UPS（不斷電系統）。

3. **實體偷竊（Physical Theft）**
   當然，電腦之實體偷竊造成機密和可取得性的資料遺失，且即使尋回，也會令人懷疑資料的正確及完整性。有規律地將系統備份並且存放在或分散在離該電腦有些許距離的地方可讓資料分散集中存放的危險，單一的備份資料並不能確保機密性。 使用加密的工具將硬碟內的資料加密。 建議應用這些工具在含有機密性資料或是容易遺失（如手提電腦或是其他可攜帶式的電腦）的電腦。

## 4 家用者所能夠採取的電腦保護措施

1. **若是你從家中使用，聯絡你的系統維護者**
   如果您是使用寬頻網路經由 VPN 或是其他方式連接您公司的網路，您的公司應有規則或制訂程序是和網路安全有關的，所以在按照著這份文件步驟執行的同時你就該先確定與你的網路系統管理者取得聯繫。

2. **使用防毒軟體**
   在這份文件中，建議在任意一台連接上網的電腦上都應該安裝防毒軟體，且要確定防毒軟體要隨時更新，許多的防毒軟體都有自動更新病毒檔的功能，我們建議應該執行自動更新病毒檔。
   以下連結有更多資訊：
   http://www.cert.org/other_sources/viruses.html#VI

3. **使用防火牆**
   強烈的建議應安裝防火牆軟體，例如網路應用軟體或是個人化防火牆，入侵者不停針對已知的漏洞展開掃瞄，網路防火牆（軟體或是硬體設施）可以提供一些防止這些攻擊的保護。然而，並沒有任何防火牆可以完全偵測或是停止所有攻擊，所以

如果僅安裝一套防火牆之後就忽視其他安全衡量是絕對不足夠的！

4. **不要任意開啟未知的 E-mail 夾檔**

在開啟任何電子郵件附件以前，一定要確知其來源。光知道郵件來源住址是不足夠的。Melisa 病毒可以精確的傳播正是因為它的來源信件地址都是令人熟稔的。可怕的病毒極有可能散佈在有趣的標題或是誘人的程式中。

如果您必須開啟一封無法立即確認來源的附加檔案，我們建議您依以下的程序：

***1.確定您的病毒辨識軟體是更新到最新的。***（請見上文中的 "Use virus protection software"）

***2.將檔案存到硬碟。***

***3. 使用防毒軟體先行掃瞄該檔案***

***4.開啟檔案。***

額外的保護作法是在開啟該檔案前先行切斷網路連線。

依循上述步驟雖然不能完全杜絕隱藏在郵件附件中的惡意程式從您的電腦散播出去，但是起碼可以做些防護。

5. **不要執行未知來源的程式**

絕不執行非您所信任的人或公司所授權的程式。另外，不要因為某些來源不明的程式看起來十分誘人就寄給您的朋友或同事。它們可能含有特洛依木馬程式。

6. **關閉隱藏延伸檔案的功能**

視窗作業系統含有一選項可以"隱藏已知檔案類型的副檔名"。這項功能在預設值中被設定開啟，但是您可以自行關閉該選項以在視窗作業系統中看見檔案副檔名。在預設值中，即使在關閉該選項後仍然會有部分副檔名會保持隱藏。

在 windows 作業系統中有一個可以設定的註冊機碼，若是有註冊，除非是使用者自訂去修改選擇隱藏已知檔案類型的副檔名功能，否則就會在系統中秀出已知類型檔案的副檔名。"NeverShowExt"的機碼即是被用以隱藏 windows 作業系統的檔案，例如".LNK"這個用來表示捷徑的已知副檔名形式即會被隱藏起來，不管是否有選擇開啟隱藏檔案功能。

更詳細的隱藏已知檔案資訊在下列連結：

http://www.cert.org/incident_notes/IN-2000-07.html

7. **保持軟體更新修正檔**

廠商通常在軟體漏洞被發佈之後會提供更新檔，大部分的產品在出廠後也會在文件中告訴使用者哪裡能夠取得更新修正程式，使用者應從廠商的網站上取得廠商所提供的修正檔或是相關的資訊。

現在已有許多軟體當有更新程式被提供時，使用自動更新功能，有些廠商也會自動依據郵件清單上的 e-mail 自動、定時聯

絡使用者，到製造廠商的網站上去找尋自動更新的功能或是訂閱軟體更新資訊的 e-mail，若是無此功能，使用者最好還是定期的去取得修正檔。

8. **不用電腦或不連上網時關閉電腦**
   當不使用網路時，請將電腦關閉或是將連接網路的功能關閉，因為入侵者絕對無法對一台關機的電腦或是沒有連接上網的電腦展開攻擊。

9. **若可能，關閉 JAVA，JavaScript，ActiveX**
   對於動態的程式碼例如 JAVA，JavaScript，ActiveX 要加以留意，因為一個惡意的網站開發者可能用之以夾帶一些描述性的程式碼，將 URL、一些表單程式碼、或是資料庫的存取要求傳送給有心人，當使用者開了瀏覽器，而網站也有了回應，這些不懷好意的程式碼即能竊取你的資訊。
   最有效的防止方法也就是關閉讀取這些動態網頁的功能。將之關閉能保護使用者的系統不被這些惡意程式碼所侵犯，當然，如此一來對於使用者的網際網路功能也大受限制。
   有許多正當的網站使用這些動態的描述程式碼以增加自己的特色或功能，關閉此描述性語言則會大大降低與網站互動的功能。
   更仔細的瀏覽器描述語言控制能在以下連結取得更多資訊：
   http://www.cert.org/tech_tips/malicious_code_FAQ.html
   其他更多關於 ActiveX 安全的資訊及網站管理員資訊可由以下連結取得：
   http://www.cert.org/archive/pdf/activeX_report.pdf
   更多關於網頁動態程式碼的資訊可由以下連結取得：
   CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests

10. **關閉 E-mail 軟體的陳述性語言**
    因為許多電子郵件程式使用有如瀏覽器的程式來呈現 HTML 格式，所以會影響 Active X, JAVA,以及 Java Script 的一些弱點均可適用在網頁上般的影響電子郵件。因此，我們建議使用者除了在瀏覽器上關閉這些陳述性語言也要關閉在電子郵件程式中的陳述性語言。(請參考上文中的 "Disable Java, JavaScript, and ActiveX if possible" )

11. **對重要的資料進行備份**
    在如 ZIP 或是可讀寫光碟機般的可移除的裝置上保留一份重要資料的備份。如果可以取得的話，使用軟體工具做備份，並且將備份好的磁片存放在電腦以外的地方。

12. **製作一張開機片以防電腦出狀況**
    為了在電腦發生安全入侵或是硬碟壞軌的時候提供協助，請使用軟碟機製作一張可開機磁片。這將可以在復原電腦時提供幫

助。然而，請記住在您系統發生任何安全事件之前製作此可開機磁片。

# 附錄

## 其他相關資訊及附件：

### *相關資訊：*

- CERT Advisories
- CERT Incident Notes
- CERT Vulnerability Notes
- CERT Tech Tips
- Other CERT documents

**CERT 諮詢報告**

CA-1999-02: Trojan Horses
http://www.cert.org/advisories/CA-1999-02.html
CA-1999-04: Melissa Macro Virus
http://www.cert.org/advisories/CA-1999-04.html
CA-2000-01: Denial-of-Service Developments
http://www.cert.org/advisories/CA-2000-01.html
CA-2000-02: Malicious HTML Tags Embedded in Client Web Requests
http://www.cert.org/advisories/CA-2000-02.html

**CERT 事件記錄：**

IN-2000-01: Windows Based DDOS Agents
http://www.cert.org/incident_notes/IN-2000-01.html
IN-2000-02: Exploitation of Unprotected Windows Networking Shares
http://www.cert.org/incident_notes/IN-2000-02.html
IN-2000-03: 911 Worm
http://www.cert.org/incident_notes/IN-2000-03.html
IN-2000-07: Exploitation of Hidden File Extensions
http://www.cert.org/incident_notes/IN-2000-07.html
IN-2000-08: Chat Clients and Network Security
http://www.cert.org/incident_notes/IN-2000-08.html

**CERT 漏洞記錄：**

VN-98.07: Back Orifice
http://www.cert.org/vul_notes/VN-98.07.backorifice.html

**CERT 技術網頁：**

Frequently Asked Questions About Malicious Web Scripts Redirected by Web Sites
http://www.cert.org/tech_tips/malicious_code_FAQ.html
Protecting Yourself from Email-borne Viruses and Other Malicious Code During Y2K and Beyond
http://www.cert.org/tech_tips/virusprotection.html
Spoofed/Forged Email
http://www.cert.org/tech_tips/email_spoofing.html
Windows 95/98 Computer Security Information
http://www.cert.org/tech_tips/win-95-info.html

**其他 CERT 文件**

Other Computer Virus Resources
http://www.cert.org/other_sources/viruses.html
Securing Desktop Workstations
http://www.cert.org/security-improvement/modules/m04.html
Results of the Security in ActiveX Workshop
http://www.cert.org/archive/pdf/activeX_report.pdf
Security of the Internet
http://www.cert.org/encyc_article/tocencyc.html#PackSnif

## *附件資源：*

TCP/IP Frequently Asked Questions
http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part1/
http://www.faqs.org/faqs/internet/tcp-ip/tcp-ip-faq/part2/
Computer Virus Frequently Asked Questions for New Users
http://www.faqs.org/faqs/computer-virus/new-users/
alt.comp.virus Frequently Asked Questions
http://www.faqs.org/faqs/computer-virus/alt-faq/part1/index.html
http://www.faqs.org/faqs/computer-virus/alt-faq/part1/index.html
http://www.faqs.org/faqs/computer-virus/alt-faq/part1/index.html
http://www.faqs.org/faqs/computer-virus/alt-faq/part1/index.html
VIRUS-L/comp.virus Frequently Asked Questions
http://www.faqs.org/faqs/computer-virus/faq/
Firewalls Frequently Asked Questions
http://www.faqs.org/faqs/firewalls-faq/

---

**這份文件的英文版本**: http://www.cert.org/tech_tips/home_networks.html