

個人資通安全保健手冊



Cyber-pa 提醒您：

平日做好資安保健

常保個人資安健康!

類別一：保護電腦資訊安全

1. 防火牆	<p>網路防火牆主要功能為阻擋試圖透過網際網路進入你電腦的駭客。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。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none">● 設定良好密碼、安裝防毒軟體、安裝防火牆。
2. 密碼	<p>使用一個容易猜的密碼，就好像打開大門邀請小偷進來般危險，即使小偷闖入後沒有取走任何東西，你的個人私密資訊也早被看盡。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none">● 密碼是保護電腦的第一防線，密碼安全的四大守則~<ol style="list-style-type: none">1. 不告訴任何人密碼（包括親人、職務代理人、上司等）2. 不寫下密碼3. 設定不容易被猜到的密碼4. 一旦懷疑有人可能知道你的密碼，即刻更改。
3. 軟體更新	<p>軟體使用一段時間後通常會出現一些安全漏洞，這些漏洞也是駭客容易利用的弱點，因此軟體製造商（尤其是具有商譽者）會設計更新或修補程式來修正這些問題。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none">● 隨時留意微軟作業系統更新功能與提醒。● 不使用盜版軟體。
4. 病毒	<p>從技術觀點而言，電腦病毒是一種會自我複製的可執行程式，其傳染途徑包括電子郵件、傳輸檔案、電腦遊戲，及任何從網路上面下載的檔案。病毒造成電腦的傷害可能方式有破壞硬碟檔案、重新格式化電腦硬碟、使效能變慢、上網時瀏覽器新視窗不斷被打開，直到電腦系統資源被耗盡為止等。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none">● 防止電腦病毒的第一法則：安裝防毒軟體，並且定期更新病毒碼。

<p>5. 安全的電腦操作環境</p>	<p>電腦雖然是機器，一個良好舒適的操作環境，將能夠延長其使用壽命，降低電腦損壞機會。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none"> ● 電腦操作環境應保持乾燥。 ● 確保電腦主機和其他周邊設備（如印表機）相連的數條纜線、電線不雜亂交錯，尤其注意插座的負荷量。 ● 避免在電腦桌上放置飲料、裝水的容器，以及飲食，都是寶貝電腦的方法。
<p>6. 資料備份</p>	<p>電腦硬碟容量越大，所儲存資料量也越多，若突然遇上硬碟陣亡、系統損壞等情形，即有資料付之一炬的風險，所以定期備份是件很重要的事。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none"> ● 將重要檔案複製到電腦硬碟以外的儲存媒體，例如光碟片、網路硬碟等。 ● 備份重要的軟體，以防原版軟體受到損傷。 ● 定期測試備份資料是否有效。

類別二：保護個人資料和隱私

<p>7. Cookie 記錄</p>	<p>Cookie 是網站伺服器儲存使用者瀏覽網頁時所留下的一些個人資料，以便網站伺服器在未來你再次到訪其網站時，可用以辨識你的身分，這也是為什麼你有時到訪雅虎或其他網站首頁時，網頁總是能夠顯示出你的名字。雖然這對於電腦系統不會產生直接的損害，但對於重視隱私權使用者者來說，可謂為一種侵犯。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none"> ● 透過設定瀏覽器的安全設定值來限制 Cookie 功能。路徑為瀏覽器的「工具」→「網際網路選項」→「隱私權設定」
<p>8. 隱私權</p>	<p>許多人會不小心在網路上將個人資料洩漏出去，例如填寫問卷調查、參加抽獎、加入會員等。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none"> ● 在網路上留下個人資料前，先閱讀該網站的「隱私權保護政策」內容。 ● 不任意在從來沒有聽過、或第一次造訪的網站中填寫重要的個人資料或留下信用卡資料。

<p>9. 公用存取</p>	<p>使用圖書館、公司、網咖、機場等地點的公用電腦上網，或甚至使用室友、朋友電腦上網時，必須要注意使用時所輸入的各種資料是否在這些公用電腦內「留底」，而有資料外洩遭有心人士利用的風險。</p> <p>提升資安抵抗力的秘訣：</p> <p>使用公共電腦的守則~</p> <ul style="list-style-type: none"> ● 使用公共電腦時，特別留意坐或站在旁邊的人，因為他們可以輕易地看到你所輸入電腦螢幕上的帳號、密碼或其他資料。 ● 絕對不勾選瀏覽器的「記住密碼」選項。 ● 使用公共電腦完畢離開前，應關閉網頁瀏覽器，若有登入網路服務（如電子郵件），應完成「登出帳號」動作後，再關閉瀏覽器。 ● 盡量不在公共電腦中輸入敏感性高的資訊。 ● 若經常使用公共電腦，更換密碼的頻率要更高。
<p>10. 垃圾電子郵件</p>	<p>Spam 專指未經收信者同意，以電子郵件的形式大量寄發的垃圾廣告信函。</p> <p>提升資安抵抗力的秘訣：</p> <p>雖然目前我們仍無法完全阻止垃圾電子郵件入侵，但是可透過幾個簡單方法減低可能造成的困擾：</p> <ul style="list-style-type: none"> ● 絕不回覆垃圾電子郵件，因為這樣會讓垃圾郵件散佈者知道你的信箱是有效的。 ● 不回應購買垃圾電子郵件的廣告商品。 ● 使用垃圾電子郵件過濾軟體。
<p>11. 間諜軟體</p>	<p>間諜軟體是一種和病毒相似，會毫無預警地溜進你的電腦系統，並隱匿行蹤，在未經你許可情形下，不知不覺地將你的資訊透過網路傳送到特定對象。間諜軟體常伴隨網路免費下載的程式軟體、或點對點音樂檔案交換等管道，進入到使用者電腦硬碟內。這是一種侵犯個人隱私權的行為。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none"> ● 下載免費或共享軟體前，需仔細閱讀和軟體有關的所有訊息。 ● 避免透過 P2P 程式或其他管道下載來路不明軟體。

類別三：安全地使用網路上的各項服務

12. 網路毀謗	<p>以言論傷害他人名譽或侮辱毀謗他人，是觸犯刑法公然侮辱罪或誹謗罪。網路因為具有快速、大量傳播、成本低、匿名性高等特性，透過網路的毀謗所造成傷害力更大；在網路上傳播言論若觸法，一樣要接受法律制裁。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none">● 在網路上發言前，三思而後發佈。● 不隨意轉寄未經證實的網路流言信件等。
13. 即時通訊軟體	<p>越來越多人和企業使用「即時通」軟體，例如進行多方會議、訊息與檔案交換等。雖然方便，若沒有針對你的電腦及個人資訊進行保護措施，即時通是會造成潛在資訊安全危機的。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none">● 不隨意接受透過即時通所傳遞來的檔案。● 不透過即時通傳遞個人資料，或重要的公司機密資料。● 安裝防毒軟體、防火牆。
14. 智慧財產權	<p>國內對於智慧財產權保護的認定標準上，採取的是「最低原創原則」，亦即著作必須有一定限度以上的原創性，才可以成為著作權法保護的標的。然而，網路使得數位創作智財權更容易受到侵犯。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none">● 不論是網路內容的使用者或提供者，皆須瞭解違反著作權的行為包括：未經授權的使用圖片、抄襲他人的成果、點對點分享音樂檔案等。● 當你的網站使用其他網站的文字、圖片、照片等內容時，必須取得對方的許可，以避免觸犯其他網站的商標或著作權。
15. 網路釣魚與網路詐騙	<p>網路釣魚犯罪方式，是由駭客仿冒知名公司網站神似網頁，並以該公司名義發出假 email，標題多半為「系統更新，請檢查帳號」、「請變更密碼」、「帳號被關閉，請上網重新啟動」等字眼，而 email 裡幾乎都會有該公司商標，取信於收信者，然後提供一個假的超連結，誘騙使用者登入假網站輸入個人資料。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none">● 不直接使用 email 所提供超連結，以自己輸入網址方式取代。● 凡事求證後才行動，可減少被騙機會。

16. 無線上網	<p>電腦駭客可以在你家屋外透過裝有無線網路卡的電腦，就可以進入你家的無線網路；加上一些設備與免費的惡意攻擊程式，駭客可輕易地進入你的電腦系統，甚至植入後門程式。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none"> ● 啟動防毒軟體與防火牆。 ● 不隨意連線到不明的無線 Access Point。 ● 關閉 DHCP 自動指派 IP 位址之設定。
----------	--

類別四：安全地在網路上購物與拍賣

17. 數位簽章	<p>我們可以將數位簽章想像是一個電子圖章，以晶片卡、隨身碟等方式存在，透過應用軟體在 email 訊息或文件上做「簽名」動作。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none"> ● 有法律保障的電子簽章，應是由經濟部公告核定的憑證機構所核發之電子憑證所產生的。 ● 只在電子憑證所定義的使用範圍內應用憑證。
18. 網路交易糾紛	<p>線上購物在台灣是同等於郵購的，消費者享有 7 天內可不須說明理由、不付任何費用，退回商品或解除買賣契約。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none"> ● 在網路購物前，應檢視電子商店網站是否提供充分的業者聯絡資訊，並詳細閱讀業者契約條款內容。 ● 發生消費爭議時，可撥打「1950」全國性消費者服務專線電話，或直接向各縣市政府消費者保護官請求協助。
19. 網路付款	<p>網路交易付款方式很多，最常見者為直接於網站上輸入信用卡號。</p> <p>提升資安抵抗力的秘訣：</p> <ul style="list-style-type: none"> ● 輸入信用卡等重要個人資料時，應確認網路商店的網站付款機制符合 SSL 等安全機制，以確保資料傳輸時的安全。簡單的檢查方法包括： <ul style="list-style-type: none"> - 網址最前方是否為 https（一般網址開頭為 http）。 - 網站是否有認證標章。 - 網頁右下方是否出現鎖匙圖案 ● 選擇有商譽的網路商店進行交易。

20. 安全認證網站

安全認證標章是由公正第三方之驗證機構，針對網路商店之交易安全進行檢驗；通過驗證之網路商店，驗證機構會提供「安全認證標章」張貼於該網站上，以便消費者辨識該網站之交易安全與可靠。

提升資安抵抗力的秘訣：

- 在網路上填寫個人資料或進行交易時，先檢查該網站是否有標示信賴標章。
- 特別注意網路商家是否提供完整的公司基本資料、聯絡方式、商品說明、退換貨條件方式、申訴處理機制等必要資訊。

策動單位：行政院國家資通安全會報

委託單位：資訊工業策進會

執行單位：NII 產業發展協進會

地址：台北市松江路 317 號 7 樓

電話：02-25082353 傳真：02-25073507

Email：i-security@nii.org.tw