防詐停看聽
網路購物安全指南

經濟部廣告

防詐停看聽
網路購物安全指南

電子商務連年蓬勃發展，根據資策會產業情報研究所(MIC)統計，2012年電子商務市場規模成長至6605億，預估2013年將繼續成長至7400億，「電子商務」已然成為新世代創業模式及數位時代中最受矚目的經濟焦點。

然而，才剛在網拍下單或線上購物，就馬上接到詐騙電話，這是許多人都曾有過的不愉快經驗。根據警政署統計估算，2012年的網路詐騙多達2245件，包含網路帳號盜用、交友網站詐騙等；賽門鐵克2011年全球網路安全威脅研究報告指出，台灣在亞太區的惡意程式活動來源國和釣魚網站發起地等排名均高居前三大，駭客善於引誘消費者上當，如利用email主旨吸引消費者開啟具有惡意程式之附件、假冒節慶活動或折扣促銷，引誘網友點擊惡意連結等，連結至釣魚網站以竊取個人資料，民眾不可不防！

透過這本《防詐停看聽 網路購物安全指南》，你可以了解各種網路常見的攻擊手法與如何因應；購物平台百百種，選擇購物網站，除了比價之外，你更應該知道具備哪些基本要素的網站才安全；在網路世界，要加入購物網站會員填寫個人資料時，該注意哪些原則，避免過多的個人隱私曝光，讓駭客進行資料拼圖，使自己更容易被騙；最後，養成手機行動上網安全的基本觀念，就像在海邊看到禁止游泳的告示牌就知道要避開危險區域一樣。練好上網安全基本功，才能暢遊網路世界，減少被詐騙所造成的財產損失。

目錄 CONTENTS

計畫簡介

電子商務網站身分識別機制推廣計畫

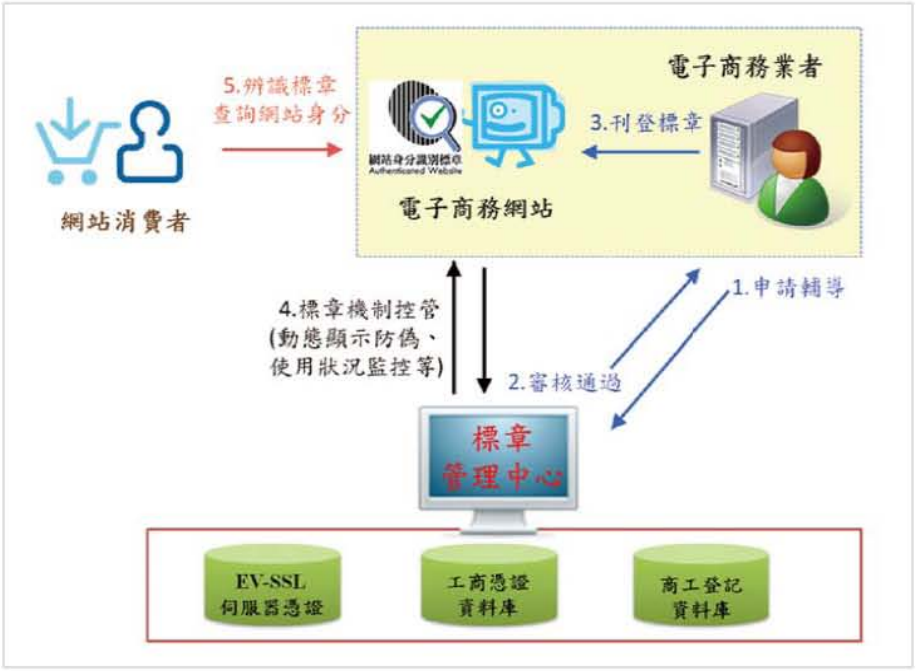
計畫緣起

本計畫係依98年12月行政院「塑造資安文化、推升資安產值」關鍵推動方案（99年至102年）架構下所規劃措施方案，就環境面、應用面與資安面以更明確、具體的政策目標與相對應之內涵加以規劃，透過電子商務網站身分識別輔導機制，協助消費者辨識正牌網站，輔導電子商務業者重視消費者資料傳輸安全與個資保護，在政府與民間通力合作下，達成「強化電子商務整體交易安全」之目標。

計畫目標

本計畫之目標在於協助電子商務業者導入網站身分識別機制、並提升消費者辨識正牌網站能力與交易安全認知，依照輔導電子商務業者與宣導網路交易安全方式，透過以下五個步驟，有效強化電子商務交易安全：

1. 檢核網站身分識別機制以發現問題及應改善項目
2. 導入網站身分識別與高等級安全加密憑證，建立有效機制
3. 導入掛馬偵測技術機制，增強網站對惡意程式之防護能力
4. 強化業者與消費者資安意識，以落實個資防護行動
5. 透過消費者交易安全認知宣導，提升電子商務消費信心



輔導申請

為推動網路交易主體確認機制、消費者安全防護認知宣導與意識強化，中華民國資訊軟體協會承辦經濟部商業司102年度「電子商務網站身分識別機制推廣計畫」，推動全國電子商務網站業者實施「交易主體確認企業實體身分識別與電子商務網站身分識別機制」，協助業者降低冒名交易、釣魚網站等網路詐騙活動。

一、 網站身分識別標章機制：

電子商務業者可向本計畫申請網站身分識別標章機制輔導，通過資格審核後進行輔導作業、於網站上刊登網站身分識別標章，同時由後端管理中心介接EV SSL憑證與標章系統，即時動態顯示與控管使用狀況，而消費者藉由網站身分識別標章，辨識與查詢網站身分。

此外，計畫標章系統已完成介接工商憑證資料庫與商工登記資料庫，達成EV SSL憑證、工商憑證之雙重網站經營者身分識別，以標章動態顯示(若有問題則顯示失效標章，見下圖)，避免消費者誤觸釣魚網站，進階保障消費者權益。

二、 輔導內容說明：

計畫提供電子商務網站輔導名額，各輔導網站將**免費**獲得總市價約10萬之服務內容：

◆ 一年期EV SSL憑證服務
(提供加密與防偽功能)
◆ 一年期網站惡意程式監控服務
(避免網站被惡意掛馬)
◆ 一年期網站身分識別標章服務
(協助消費者識別網站)

年度輔導名額數量請洽詢ec-security@mail.cisanet.org.tw，額滿為止。

除上述之服務外，本計畫亦將不定期辦理廣宣活動，推廣消費者對本計畫輔導網站使用EV SSL憑證與網站身分識別標章的認知，提高輔導網站知名度，達到提升網站交易安全信賴感與擴大商機之效果。

三、 申請資格：

◆ 中華民國境內依法登記之企業。
◆ 具獨立網址、獨立ip之B2C電子商務網站。
◆ 申請前一年之電子商務交易營業額新台幣30萬元以上或交易筆數達500筆者。
◆ 營業項目為零售業、餐飲業、智慧財產權業。
(經濟部公告之營業項目代碼為F2、F3、F5、F6開頭者；或營業項目代碼為ZZ999 ，並實際經營上述之業務者)

※營業類別查詢請參考http://gcis.nat.gov.tw/cod/html/fulltxt.htm

四、 申請方式：

請至計畫網站(http://www.ec-security.org.tw)下載並填妥「電子商務網站身分識別標章輔導申請書」後，傳真或mail至本會辦理申請作業。

填寫時如有疑問時，歡迎洽詢本計畫承辦窗口
聯絡電話：(02)2553-3988
傳　　真：(02)2553-1319
E-mail:ec-security@mail.cisanet.org.tw

有效標章

失效標章

了解網路常見的威脅攻擊手法，保持正確的上網習慣，
以及對自己個人資料的保護，才能遠離詐騙、安全悠遊網路世界。

你必須懂的

網路威脅與詐騙手法

網路購物消費之後就接到詐騙電話令人生氣，但除了生氣、上論壇發表文章抱怨之外，你可以有更積極的作為。先從了解網路常見的威脅與詐騙的手法，培養正確的上網習慣開始，重視自己的個人資料隱私，拒絕不重視客戶個資的網站，要求業者共同創造一個值得信賴的網路交易環境。

詐騙手法變變變

一切從 盜帳號 開始

詐騙手法變變變 一切從盜帳號開始

網路世界蓬勃發展，社交網站：Facebook、噗浪、Twitter…形形色色的網站出現，網路多樣性讓人沉迷，各種商業交易均透過網路來傳遞，包括網路銀行、網路購物等，許多人仰賴網路更深。正因為大量交易在網路上進行，許多網民沉迷於網路卻不知網路世界的陷阱，再加上訊息傳遞方式的多元，於是熟悉網路技術的犯罪集團便利用各種訊息管道組合不同手法進行詐騙。

在現實生活中，身分證可以代表個人真實身分，而在網路世界最基本的就是帳號、密碼。於是駭客最終的目的就是要騙取用戶們的帳號、密碼等可通行於網路、並取代其身分的資料，如電子郵件、即時通訊、網路購物、線上遊戲、網路銀行等帳號與密碼，再藉此擴大進行詐騙行為，以獲取金錢財物。

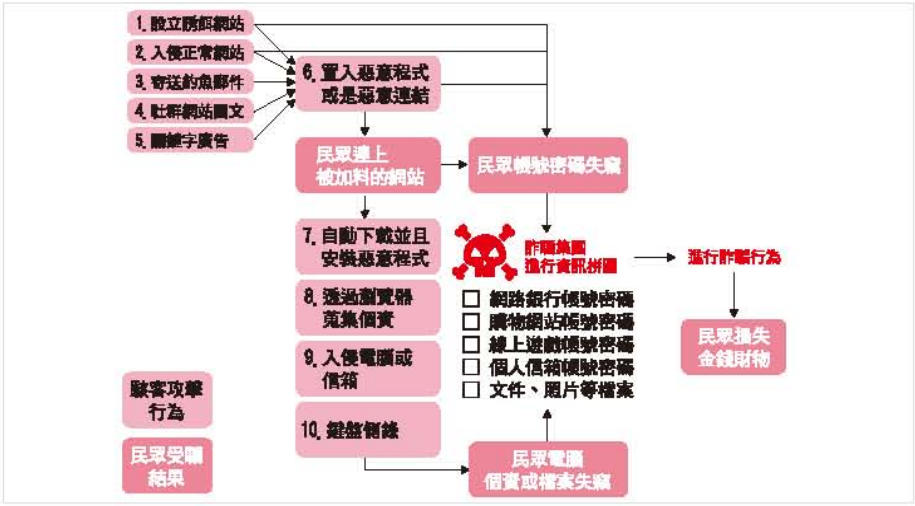


圖1. 個資外洩、網路犯罪關係圖

從上圖1來看，網路犯罪新興手法不外乎透過網站、電子郵件、即時通訊、關鍵字廣告、社群網站之類的媒介，利用網友缺乏警覺性或有好奇心的弱點，引誘、偽造、欺騙其上當，騙取用戶點選惡意連結連上惡意網站、開啟有惡意程式的Email附件或者在釣魚網頁輸入個資，統稱為**社交工程**手法。

在美國網路服務業者Verizon Business的2010年資料外洩調查報告(DBIR, Data Breach Investigations Report)中，發現主要的資料外洩事件原因，有7成是來自於外部的不肖份子，其中使用偷來的身分帳號密碼(38%)直接登門入室最多，因為其障礙與犯罪成本最低，這些不肖份子取得重要資料的方式，就是前述所提到的網路釣魚以及詐騙所取得的帳號密碼與權限。

網路世界裡的帳號密碼猶如真實世界中的個人身分證，只要竊取你的帳號密碼，就可以代表你的身分在各種網站進行消費行為。因此許多安全機制比較好的網站，除了要求基本的帳號密碼之外，都開始增加更多重身分認證機制，以防遭人偽冒，我們將在下一章**<如何選擇安全的電子商務網站>**仔細介紹。

以下是常見的網路威脅攻擊方式，這些攻擊手法使用已久，駭客不斷透過新的新聞事件或知名人物等素材吸引使用者點選，千方百計要讓你的電腦中毒。當然，對於已經有一定資安意識的使用者，駭客也會有新的花招。

各種網路威脅

攻擊 交叉組合

電子郵件圖片、附件隱藏病毒與木馬

駭客利用社交工程的概念，透過吸引人的信件主旨吸引收件人點閱，並將病毒、蠕蟲與惡意程式等隱藏在電子郵件中。這些看似朋友所寄來的郵件，卻是應用社交工程的電子郵件陷阱，例如過去造成重大損害的I LOVE YOU蠕蟲，就是一種利用社交工程散播的電腦病毒。

信件當中夾帶明星或色情圖片，是許多惡意程式慣用的社交工程技巧之一，這些都是利用使用者的好奇心來散佈惡意程式，之前Sobig網路病毒出現在某個含有色情內容的網路討論群組，網友點選了其中像是裸照的內容就會感染病毒，而該病毒總共導致了約10億美金的損失。

除了利用圖片誘惑外，偽裝成軟體的修補更新程式，或免費防毒軟體也是常見的手法，因為一般使用者不會覺得這是來路不明的程式，不知社交工程也會利用這個漏洞，而將惡意程式隱藏其中。使用者若安裝了這個檔案，不但不會修補作業系統的任何漏洞，還可能被安裝了遠端竊取資料的木馬程式。

釣魚郵件導引至冒牌網站騙個資

偽裝成電子商務網站、銀行等企業或機關客服部門寄發的電子郵件(如信件主旨：通知您的信箱即將過期被封鎖)，通知收件人必須重新驗證密碼或登入某網址輸入個人資料，並假造

圖2. 收到疑似釣魚郵件，應多方查證

真實網頁頁面，像是網路信箱、網路銀行、購物網站登入等等，以聳動的標題吸引用戶輸入個資與帳號密碼，這種詐騙手法稱為**網路釣魚**，是一種典型的社交工程攻擊。收件人若未小心求證而點擊郵件中的鏈結，可能就下載了惡意程式；或者在假網頁上輸入了帳號密碼或信用卡資料等，造成銀行戶頭被盜領或盜刷等的嚴重後果，這是近年來造成個人與企業極大損害的犯罪手法。

另外還有**魚叉式網路釣魚**，也稱為針對性的攻擊，攻擊者會先在網路上，包括社群網站、個人部落格等蒐集目標對象的相關背景資訊，了解社交關係，進而編造出相關題材的郵件，吸引目標開啟或是輸入資料。

網頁掛馬先污染合法網站 瀏覽網頁就中毒

即使是合法的網站，也可能因為網頁設計缺失的關係而被植入惡意連結，俗稱**網頁掛馬**，駭客可在正常網頁中安插看不見的隱形碼，利用這段隱形碼攻擊用戶電腦，同時也稱為偷渡式下載(Drive-by-download)或強制下載(見圖3)，或是在網頁中安插惡意程式，如木馬、間諜軟體等。利用受害者瀏覽時將惡意程式植入、潛伏在用戶的電腦中，伺機操控電腦並竊取所需資料。除可遠端操控受害電腦外，還有可能側錄鍵盤輸入，並將帳號密碼傳送出去。

圖3. 躲在正常網站後的惡意網站連結

搜尋引擎被駭客欺騙 提高惡意網站排名

搜尋引擎也隱藏危機。駭客會欺騙搜尋引擎的搜尋與評分機制，使惡意網頁搜尋結果排名大大提高，而其網頁內容為刻意製造出來愚弄搜尋引擎，就像是對搜尋排名模式「下毒」，**稱為SEO下毒**(圖4)。駭客經常在網頁中加入大量的關鍵字來誤導，提高搜尋排名，加上惡意網頁的連結後，只要使用者點選這些頁面，就會被導引到惡意網站並被安裝木馬後門。更有駭客利用技巧來產生容易被搜尋引擎爬到的網頁，包含自動更新熱門關鍵字、自動產生網頁，這樣就可輕易被搜尋到並被點閱，接著再將使用者導向惡意網站，使其電腦中毒。

圖4. 搜尋引擎被駭客欺騙，惡意網頁的搜尋結果在自然排序區中大大提高。

殭屍電腦與跳板 成為幫兇不自知

利用惡意程式控制受害者電腦，如同殭屍般聽令駭客，此類型惡意程式多半內含高階規避技術可躲避防毒軟體偵測，駭客會竊取各種個資及隱私資料，並且指揮殭屍電腦大量用於網路攻擊。利用這一類的跳板電腦進行攻擊，不易被追查攻擊源頭，而受害用戶往往成為冤大頭，卻不自知。

假好心防毒軟體 不裝沒事裝了中毒

不是真正的防毒軟體，而是利用網頁內容警告您電腦已經中毒，要您依照指示下載其掃毒工具，安裝假好心的假防毒軟體，實際上卻安裝了惡意程式於電腦中。

USB隨身碟蠕蟲

USB外接式儲存裝置十分普及，其具備之裝置體積小、容量大、隨插隨用等特色十分便利，也因此透過USB隨身碟中的病毒來感染目標電腦，一台一台傳染，也成為一種常見的攻擊手法。

即時通訊詐騙

除了電子郵件外，社交工程傳播惡意程式的途徑也擴大至即時通訊軟體，如LINE、SKYPE、QQ等。近來人氣狂飆的通訊軟體LINE，其詐騙方式也層出不窮，2013年2月過年期間就出現了一個 LINE 免費貼圖的粉絲團，打著免費贈送 LINE 貼圖的方式，短短四小時就吸引了十六萬人按讚，也因此也得到眾多LINE ID。LINE ID就像是你的手機號碼一樣，有了這個 ID 就可以傳送各種訊息給民眾，進一步有更多詐騙行為產生之可能，網友不可不防！不認識的帳號千萬不要隨便同意加入聯絡人。

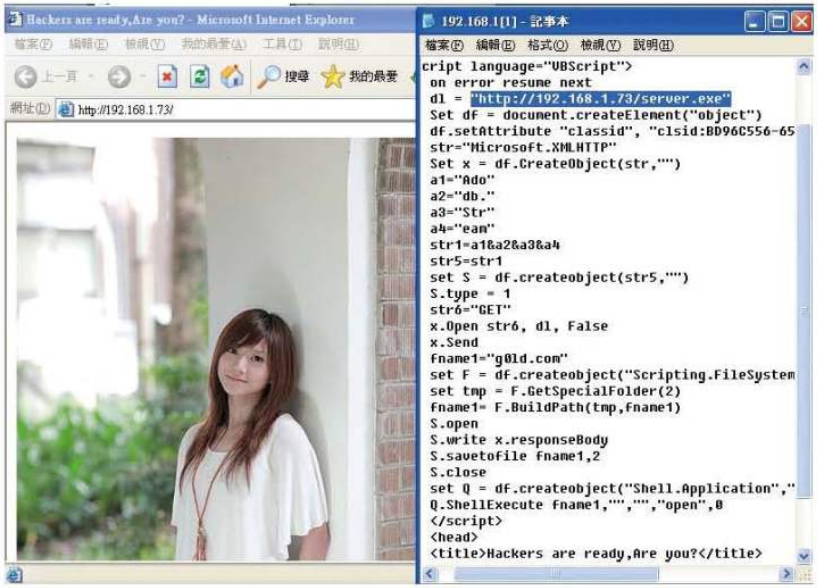


圖5. 遭駭客植入後門程式電腦範例。

零時差攻擊 絕對命中

利用新發現、尚未被公開的電腦系統漏洞弱點所進行的攻擊，稱之為**「零時差攻擊」**，由於該漏洞弱點尚未被揭露，因此零時差攻擊發生時，往往會造成比一般性漏洞更大的危害。

零時差攻擊弱點可能是各種類型的應用程式，包括OFFICE檔案、PDF檔案、瀏覽器程式，駭客可夾帶任何存有弱點文件檔案，並誘騙使用者開啟，一旦使用者開啟了這些具有攻擊程式之文件，就會被植入木馬，既無法及時阻擋、防護也失效，唯一的徹底解決之道，便是由應用程式之開發者或開發公司提供修補程式。

駭客可以在網路上散播含有零時差手法的網站，如範例使用者只是在網路上瀏覽美女照片，但實際上電腦除了會顯示照片外，還會連結到駭客中繼平台(見圖5)，下載後門程式並安裝，安裝完畢後會通知駭客這有一台電腦可以遠端監控，這時你的電腦就多一雙眼睛，在遠端偷偷監看所有操作行為。

惡意程式比一比

惡意程式	木馬程式 Trojan	病毒程式 Virus	蠕蟲程式 Worm	間諜軟體 Spyware	殭屍網路 Botnet	後門程式 Backdoor
說明	時下最流行的惡意程式。通常會假冒合法的檔案，實際內藏惡意程式。	會感染並破壞主機，但卻不具備自我複製的功能；形態上像極了蠕蟲，病毒會被用來在系統上安插其他犯罪軟體，通常還有偷取資料的能力。	會自我複製的病毒，一旦藏於系統之後，它便能刪除或加密檔案，也能夠透過email方式散佈這些有害檔案，甚至會採取其他手段入侵系統，獲取用戶資料。再者，它還能經由網路途徑，將自己傳播到其他網路。	未經使用者同意，蒐集使用者個人資訊的電腦程式，包括廣告軟體、鍵盤側錄程式等都是。	一群遭入侵的電腦系統，只受某人的指揮與控制；傳統上，都是經由木馬和蠕蟲等途徑來傳染和聚集起來的。	允許攻擊者與受害者連線，卻不必先經過登入授權程序。
自我散播能力	無	有，會造成檔案間的散播	有，造成電腦間的散播	無	無，但會透過郵件、網頁大量散播	無
影響規模	小	大	大	小	大	小
變化	高、特製化	低	低	高、特製化	高	高、特製化
目的	控制電腦、收集資料	以繁衍為目的	以繁衍為目的	以收集資料為目的	以控制電腦與頻寬、攻擊為目的	以控制電腦為目的

如何辨識 可疑的釣魚網站

在電子郵件中常見釣魚招數包括以下幾種：

1. **偽造的信件主旨與內容：**
   過於聳動的主旨與緊急的要求，一定要多方查證之後才得以信任。

2. **偽造寄信來源：**
   許多釣魚信件中的寄件者，偽裝成合法的寄件來源，獲得收件者的信賴。以下社交工程範例(圖1)是結合時間並利用假冒寄件者來誘騙開啟郵件。

圖1. 真實社交工程郵件範例

詳細觀察郵件，會發現其寄件者是假冒麥當勞寄送肯德基折價券，其郵件是利用有期限的肯德基折價券訊息夾帶惡意檔案，因為折價券訊息的是真實也可以列印到商家消費，打開郵件同時電腦也自動下載並安裝後門程式的

過程中，使用者往往沒有任何感覺。

遇到類似情況，不要直接開啟信件，在收件匣中的信件上按下滑鼠右鍵，進入[選項]，在網際網路標題裡面可以看到信件來源。但是，也不能百分之百據此判斷信件的真偽，萬一寄件電腦已經遭受入侵，那寄件來源顯然會是正確的。

3 似假還真的信件內容：

通常釣魚客會將正版的信件內容複製修改，包括圖片與文字敘述皆相同，唯一不同的是信件內，可能有掩飾過的網頁連結，連結到惡意網站，或者透過信件內附表格直接誘騙受害者輸入並蒐集所需資訊。

一旦經由電子郵件、網路連結或即時通訊的訊息，連結到釣魚網頁，可就要更小心了，在網頁中的釣魚招數可稱得上技高一籌，以下是常見的類型：

(a) 全然是偽造的內容：很容易就可以從網頁上的瑕疵分辨出來。

(b) 相近類似的網址：例如paypal.com 曾經被偽裝成 paypa1.com 變成數字的『1』，或網址中的英文『o』中用數字的『0』替換，如果警覺性不高或未仔細察看，則；不容易發覺。也有利用URL網址使用上的技巧，來矇騙受害者，例如：http://www.hinet.net:index.cfmThfz@fake.com.tw/?sessTGTS，這樣的連結內容是合法的表示，看起來是連結到中華電信網頁，而實際上則會連結到fake.com.tw。

(c) 不正確而且未經偽裝的網址：在網址列直接使用不正確的網址，有時候就直接用數字IP，或使用免費網頁之網址。很容易就可以發現其中蹊蹺，因為正常的網站是不會使用這種數字IP或奇怪的網址。

4 蒐集資料用的表格：

在這些網路釣魚的案例中，共通點就是都會要求使用者輸入資料，所以在網頁上也會有蒐集資料用的表格，一旦遇到這一類的網頁，就要提高警覺，更勿斷然輸入資料送出。

5 假造的URL位址列：

此種類型值得特別注意，目前已經發展出好幾種偽裝手法。其中一招是關閉正常的URL位址列，再利用文字與圖形造出一個假的位址列或者在網頁存取之後貼上假造網址，而這個假造網址會跟正牌網址完全相同；另一種方法則是在網頁的網址列之上，用一個位於上層的浮動視窗，將假冒的網址覆蓋住，再填上正牌的網址。

破解之道1：按下滑鼠右鍵看網頁內容可以初步判定網址是否一致，但是也要小心按下右鍵所跳出來的功能表(pop-up)是真的還是假的。比方說正牌的網址是「http://www.ebay.com」，但是按下滑鼠右鍵，選內容所看到的可能是「http://203.X.X.11/index.htm」，這就是偽造的網址。如果釣魚網頁是位於國外網站上，其產生的假網址列，所呈現的樣式為英文版網頁瀏覽器的外貌，與中文介面會格格不入，稍微留意即可發現。

破解之道2：針對使用浮動視窗，將假冒的網址覆蓋住這種手法，可以按下右鍵看內容，會出現一個視窗，將此視窗拖曳到網址列上方，若對方使用此方式遮蔽網址列，則假造的網址會浮在這個視窗上面，而一般正常的頁面則不會有此現象。

6 進入正牌網站後，跳出一個要求輸入資料的對話視窗：

雖然透過連結進入正版網頁，但是會跳出一個視窗要求輸入帳號等資訊，而這個視窗通常看不到網址列。這可能是先引誘受害者進入假造的網頁，再由這個網頁一邊連結到正版網頁，一邊產生假造的資料蒐集畫面。基本上這個轉向的動作會自動完成，因此受害者看到的網頁是真正的「正牌」網頁，但是跳出來要求輸入的對話視窗則是「釣餌」。

破解之道：按下右鍵觀看該對話視窗的網址。遇到要求輸入資料時請再三確認。

社交陷阱

小心社群網站詐騙

新的媒介，新的手法：透過社群網站攻擊

社群網站夯到不行，你每天花多少時間在瀏覽社群網站呢？小心悄悄落入社交陷阱中！

狀況1：

錯把駭客當好友，一不設防就落入詐騙陷阱

目前網路社群都可以透過搜尋的功能加到好友名單，並透過加入好友來取得與對方連繫的管道，但加入好友真的是你的好朋友嗎？這可不一定，千萬不要別人來加入好友就一頭熱的加入。

社群網站訊息攻擊中，其中一項即是透過搜尋功能，找尋個人訊息或是相關資訊，在留言板上留下惡意連結，讓網友在不知不覺點選後中，電腦即感染中毒。或是被要求幫忙接收手機簡訊碼認證，一個不防，手機號碼洩漏之外，還可能被盜刷信用卡。

狀況2：

點選轉貼PO文或圖片連結，卻誤上惡意網站

在知名社群網站Facebook上轉貼連結，張貼資訊的位置可輸入任何的網址，當然駭客也可以透過此種方式散播惡意連結，以誘人的標題提高被開啟的機率，例如「票選網路正妹」、「玩遊戲拿贈品」，吸引網友前往釣魚網站。

圖2. 在社交網站上的網址連結也容易被造假，勿輕易點選。

若是由好朋友的名義轉貼的連結，更可能因警覺心不高，自然而然就會直接去點擊連結來看內容。

狀況3：

回應文章列表，暗藏釣魚陷阱

你喜歡回應好朋友的PO文內容嗎？或是有加入某個知名藝人、名人的粉絲團呢？在社群網站上，眾人針對某一則PO文內容回應訊息是常見的事，但是長串的回應訊息中，往往暗藏不肖份子的釣魚陷阱，以簡短對話加上惡意網址連結，吸引討論的網友們點選，例如「快看這個網頁！」、「最新新聞」，若網友一時不察、過於好奇點入，就有可能被引至釣魚網站或中木馬程式。

狀況4：

加入臉書團購社團，便宜撿不成反被詐騙

如果不慎將不肖份子加入好友，或有朋友被盜帳號，就有可能陷入另一種新興詐騙陷阱中—團購社團。不肖份子會先預先設立好的團購社團，利用盜帳號或其他方式把受害者的好友群全數加入社團中，提供各種便宜的生活用品或時下熱門商品誘使網友產生購買興趣，一旦下單，不肖份子就輕而易舉地拿到被害者的姓名、手機號碼和地址三個重要資訊。

這類型的詐騙社團，往往具備以下幾種特色：(1) 購買價格和付款方式，皆用Facebook訊息傳送詢問 (2)以貨到付款、宅配方式降低心防 (3)不斷要求你提供個人資料。網友每次被主動加入社團時，只要謹記先退出社團，就能不受此類詐騙影響。

資料來源：網路資訊

圖3. 欲購買臉書團購社團商品，相關訊息一律私信告知

網路拍賣

詐騙危機重重

網路交易除了可透過企業開設的購物網站(B2C)外， C2C(民眾對民眾)交易近年更是蓬勃發展，一般常見的C2C交易模式如拍賣網站下標、BBS或社群論壇刊文交易等，囊括新品販售與二手買賣，其特色為價金便宜、配送速度快，買賣雙方皆能透過市場機制各取所需，然而，潛藏的危機也讓人不可忽視。

危機：私下交易

不肖的賣家透過各類販售平台，刊登交易資訊與聯絡電話、E-MAIL、SKYPE等方式，聯絡時告知不要下標可折抵費用，以優惠價格連哄帶騙吸引民眾進行私下交易：

1. 不透過拍賣平台，匯款後寄出貨物。
2. 另開下標區，誘導買家快速匯款。

危機：假帳號交易

駭客透過各種手法，盜用久未登入的帳號刊登商品資訊；或是盜用正在進行的賣場，以假商品插入眾多販售的商品中，令買賣雙方皆難以發現。此外，這類商品交易資訊多複製其他賣場，如商品名稱、商品圖片、商品介紹等，多直接抄襲，不易查覺。

資料來源：網路資料

圖1. 網拍詐騙案例：商品名稱抄襲其他賣家

危機：指鹿為馬

透過刊登多類商品，不肖賣家故意選取錯誤的販售商品類別，躲避商品檢查，如利用知名熱門的3C產品，刊登於較冷門的生活文具類別。

危機：超短期刊登

部分不肖賣家專門刊登短期商品資訊。透過短週期頻率轉換刊登資訊，創造商品賣出快速的錯覺，並減少被發現之可能，如針對節慶假日販售禮品、以天氣變化販售小型家電詐欺。

危機：假交易評價

交易評價為目前各類拍賣交易平台常見、用以判斷買賣雙方信用之手法，然平台本身設計評價機制若未完善，則有可能淪為詐騙的工具。不肖賣家以“洗”評價的方式，同時扮演買家與賣家，先衝高交易評價，以高評價騙取更多民眾下標交易。

這麼多潛藏的危機，是否網路拍賣就是不值得信賴？其實答案是否定的，我們將在第二章<**如何選擇安全的電子商務網站**>教導民眾透過簡單步驟，輕鬆判斷、找對良好賣家。

十大網路攻擊現象與詐騙手法整理

	網路攻擊現象與詐騙手法	影響
1	電子郵件隱藏電腦病毒	電腦中毒，導致電腦中的資訊外洩
2	電子郵件網路釣魚	個資、帳號、密碼被騙取 導致網路相關資產的損失
3	網頁掛馬	攻擊網路瀏覽器，導致電腦被入侵
4	Web phishing網頁釣魚	個資、帳號、密碼被騙取 導致網路相關資產的損失
5	假廣告隱藏真危機	攻擊網路瀏覽器，導致電腦被入侵
6	PDF與Flash檔案的零時差弱點攻擊	攻擊PDF與Flash的讀取程式，導致電腦被入侵
7	殭屍病毒橫行	攻擊沒有更新的電腦，或透過其他管道入侵，控制電腦變成跳板做非法的攻擊行為
8	P2P 與軟體下載惡意程式	下載的檔案中包含惡意程式，自己把木馬裝到電腦中
9	社交網路弱點攻擊親友關係	親朋好友誤信惡意訊息，導致財物損失或電腦遭入侵
10	智慧型手機的弱點攻擊	透過手機簡訊入侵手機本身，安裝手機木馬監控並竊取個資

網路上潛藏各種威脅，駭客處心積慮要竊取你的網路身分，也就是各種線上交易的帳號密碼，舉凡入侵電腦植入木馬、架設釣魚網站等各種手法傾囊而出。因此，想要悠遊網購在加入會員前，必須張大眼睛慎選安全的電子商務網站。

如何選擇
安全的電子商務網站

撰稿人：臺灣網路認證股份有限公司

一個網站的安全設計如何，是否妥善儲存會員的個資，內部資料處理流程是否控管嚴謹，光是瀏覽網頁並無法得知。以下是最基本的辨識方式，也就是電子商務網站至少應該要具備的機制，包括建立安全傳輸通道，以及辨識各種網站認證標章等。最後，你也可以慎選、善用網路上的資源來協助辨識可疑的釣魚網站。

電子商務網站的基礎
建立安全傳輸通道

在進行各種網路購物、刷卡訂票等交易時，網站往往需要消費者加入會員，輸入包括身分證字號等個人資料，這些極度私密的資訊若未妥善管理，很容易成為駭客攻擊目標。為了保護這些在網路上傳輸的個人資料以及使用者登入系統所輸入的帳號密碼安全，許多網站都已在加入會員、登入會員等網頁使用加密保護，甚至部分更有資安意識的網站，從登入開始到登出的整個過程，全程都是經過加密保護，如Gmail、Hotmail、PayPal等。有了這層傳輸通道的加密保護，就猶如銀行僱用保全人員戒護運鈔車一樣，確保這些鈔票不會在中途被輕易攔截。

SSL(Secure Socket Layer) 憑證

如前述所提，電子商務網站建立了安全傳輸通道，可以保護你所輸入的個人資料不會在網路傳輸過程中被有心人士側錄，而此一安全傳輸通道之技術被稱為**SSL (Secure Socket Layer)**，電子商務網站可藉由已安裝於伺服器上之 SSL 數位憑證來啟動安全傳輸通道，其提供了兩大安全優勢：

第一、傳輸過程全程加密

在網站伺服器與使用者瀏覽器間，建立起兩端點間之全程加密傳輸通道，能有效保護資料於網路傳輸時不被竊取，並確保這些資料只能為雙方所存取；於網站網址前指定使用“https” 作為連線方式，即可讓瀏覽器知道接下來在與網站進行連線時，要啟用 SSL安全傳輸通道；當成功啟用 SSL 安全傳輸通道後，瀏覽器會特別標示出此一安全狀態，例如：在瀏覽器IE 6以前版本，視窗右下角會出現一個掛鎖圖示(如圖1)，在IE 7以後

圖1. SSL顯示狀態

版本則是在網址列的右側(如圖2)。

第二、網站身分識別

於啟用 SSL安全傳輸通道之同時，瀏覽器會自動檢測網站所使用之SSL數位憑證，是否安全值得信賴，以協助使用者判該網站是否確實為欲連結的合法真網站，而非冒牌的假網站。

刑事局曾發現，駭客會部署側錄工具，專門在沒有使用https安全傳輸通道加密的網站外擷截資料，守株待兔直接撈取這些未經加密的會員資料；或是透過釣魚郵件、想盡辦法入侵使用者電腦以竊取你的網路身分或個人資料。因此在輸入個人資料前：

第一步

必須先查看網址列是否為https以及有熟悉的鑰匙鎖頭

圖片來源：Payeasy

圖2. 查看網址列是否為https以及有熟悉的鑰匙鎖頭

第二步

使用者可以透過點選憑證內容（如圖3），查看是否為合法第三方數位憑證服務商所簽發（請見數位憑證服務商列表表1），並查看憑證是否過期或是有假冒、可疑之處。檢查數位憑證是為了避免惡意人士冒充合法網站，製造假的憑證欺騙使用者。因此如果使用者沒有檢查可疑的憑證，仍舊可能會被欺騙。

表1. 數位憑證服務商一覽

名稱	Versign (台灣賽門鐵克)	BALTMORE 臺灣網路認證公司 (TWCA)	Global Trust (寰宇數位認證中心)	GeoTrust 匯智 SSL 數位憑證服務中心(WIS)
營運模式	通過稽核憑證機構	通過稽核憑證機構	銷售代理商非憑證機構	銷售代理商非憑證機構
認證標章	VeriSign Secured / Norton SECURED powered by VeriSign	TWCA	Global Trust	GeoTrust Authorized Partner geotrust.com

圖3. 憑證內容

建立一個SSL安全傳輸通道

1. 使用者送出一個請求，要求網站伺服器建立SSL/TLS連線。
2. 網站伺服器送出一個由認可的憑證機構所發行的SSL 數位憑證，例如Verisign或TWCA，憑證內包含網站之相關資訊及公鑰，以供使用者作身分識別之用。
3. 使用者驗證伺服器的 SSL 數位憑證後，會再產生一個連線專用金鑰，以伺服器之公鑰加密送回，伺服器以私鑰解密後取得該連線用金鑰，即可建立一個安全傳輸通道。

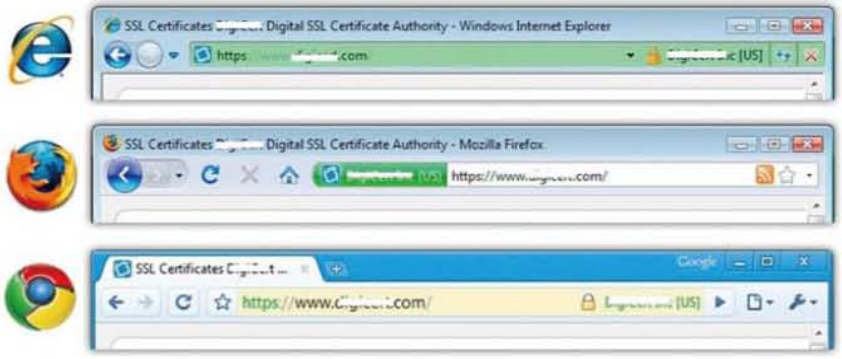
EV SSL (Extended Validation SSL) 數位憑證

鑑於網路電子商務的蓬勃發展，對於 SSL 數位憑證的需求亦日益成長，於2007年，由全球各大憑證管理中心(CA) 與瀏覽器廠商所共同組成的CA/Browser Forum 國際性組織，正式推出了更嚴謹的延伸驗證 SSL 數位憑證(EV SSL, **Extended Validation SSL**)，國內最大的民間憑證管理中心 - 臺灣網路認證公司亦為其中的少數亞洲會員之一，參與該組織的相關會議與決策。

EV SSL藉由 CA 與瀏覽器廠商之合作，當使用者連結到受 EV SSL 憑證保護的網站時，在支援EV的瀏覽器（如 IE 7, Firefox v3及以上版本）將會讓網址列變成綠色，並出現一個新區塊，以顯示擁有該憑證之組織名稱以及核發該憑證之CA 名稱等資訊，使網路釣客和山寨網頁無法假冒誘騙使用者上當。若使用舊版本(IE 6或Firefox v2)之瀏覽器，其顯示方式則和SSL一樣。

圖4. SSL憑證優點

圖5. 安裝EV SSL憑證之網站具備綠色網址列



資料來源：網路資料

圖6. EV SSL在不同瀏覽器有不同顯示狀態

EV SSL除了以更顯目的方式在使用者瀏覽器上標示網站身分外，網站要申請EV SSL認證的程序也更嚴謹，網站必須提出文件證明其合法性，包括：證明商業實體的設立與運作、上述商業實體必須合法擁有登記的網域名稱，並能完整掌控該網域名稱之運用、網站管理人必須獲得商業實體負責人授權管理該網站、網路使用者點選EV SSL標章時，可以看到該企業相關的身分登記資料，以確認其真實性等。同時，憑證管理中心必須採用經過驗證的資料，而非憑證申請者自行提報的資料來為消費者把關，而憑證管理中心本身也必須正確遵循EV準則並通過審核。

不管是使用SSL 或 EV SSL，都只保證資料在傳輸過程中有經加密保護，也就是有保全戒護的運鈔車，但不表示存放鈔票的銀行後端金庫中，是否有層層防盜監控。同理，網站後端如何營運管理、儲存個人資料，通常不是我們可以肉眼看得出來。若連最基礎且使用者可見之傳輸過程都無使用 SSL 做加密保護，那麼網站其他部分之安全措施之規劃與落實，更著實令人存疑。

此外，還有一點必須特別強調，不要在無線網路環境中進行線上購物或其他網路交易服務，尤其是該電子商務網站沒有提供任何SSL加密時，那將代表你所輸入的任何資訊，都能非常輕易地被攔截，並導致身分被冒用竊取。國外一位電腦高手為了突顯許多網站仍未使用SSL加密，尤其是社群網站，在2010年10月發表了一個名為Firesheep的應用程式，只要你使用WiFi無線網路，並連結到未提供SSL加密的網站，你在社群網站的使用者名稱及照片就會直接顯示在Firesheep的視窗中，安裝了Firesheep的人只要點選你的名稱就可以直接冒用你的身分登入該網站，而你完全不會察覺。

網購認明

網站身分識別標章

除了加密傳輸資料外，為了讓瀏覽網頁的使用者，或者進一步要從事網路交易的會員，能夠確認這不是一個釣魚網站，而且是一個可以提供真實身分認證的網站，許多網站會申請各類網站認證標章。

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進行檢驗；通過驗證之網路商店，驗證機構會提供「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。然而目前台灣常見的網站認證標章，多是不涉及技術內涵的網路隱私權保障與網路交易信賴機制，其缺點為易遭冒用、發證單位無從管考或不易控管等。有鑑於此，經濟部商業司特創建電子商務網站身分識別標章。

凡取得此標章的電子商務網站，將具備兩大特色：1.具備EV SSL驗證及顯示網站中文資訊；2.通過網頁掛馬安全檢測。以下深入說明：

讓上網的民眾，藉由標章確認瀏覽或交易的網站不是釣魚網站，
而是可安心交易的正確網站。

圖1. 網站身分識別標章

1 具備EV SSL驗證及顯示網站中文資訊

如前所述，EV SSL是通過嚴謹認證的數位憑證，許多已取得EV SSL標章的網站，都是透過台灣代理商把網站資料送回國外總公司確認，所以網站基本資料多半都是以英文呈現，且部分企業網址、網站名稱與公司名稱，消費者很難直接聯想，造成一定程度的辨識障礙，也失去了消費者辨認網站真偽的本意。因此電子商務網站身分識別標章提供消費者完整的電子商務企業的中文身分資訊，網友們僅須點選效期內的「網站身分識別標章」即可看見。

2 遠端安全監測避免網頁掛馬

網頁掛馬，是指駭客利用網頁設計缺失，污染合法的網站，植入惡意連結，使瀏覽網頁的網友們電腦中毒。同時駭客也會一步步取得該網站控制權。因此在計畫中，將涵蓋網站防偽安全機制輔導計畫，提供「網頁掛馬遠端安全監測服務」，能避免電子商務網站被惡意轉址，並減少消費者誤入釣魚網站的可能。

圖2. 網站身分識別標章認證程序

未來希望電子商務業者不論採用哪一種營利事業機構發給的EV SSL認證，（VeriSign、COMODO、Global Sign或 TWCA）都必須同時將台灣版的「網站識別標章」同時標示於網頁中。

網站身分識別標章運作如下：

當營利事業機構發給的EV SSL身分認證標章到期，電子商務業者未續約或是商工登記資料非屬”核准設立”時，「網站身分識別標章」放大鏡中的綠色打勾，就會自動變成紅色打叉的圖案。同時EV SSL身分認證顯示網址的長框中的綠色就變為紅色。

圖3. 網站身分識別標章特色

圖4. 網站身分識別標章揭示中文資訊

善用網路資源

避開問題網站

最後，網友在網購前要避免掉入釣魚網站陷阱，查看網站是否有SSL／EV SSL機制，以及檢查標章內容都只是基本步驟，無法完全保證所選擇的電子商務網站就足夠安全，你的會員資料在傳送到網站後端之後，不會被外洩。在面臨各式各樣的網站，還有兩點你必須特別注意：

❶ 小心需要安裝附加元件的網站

許多網站為了提供更多網頁效果，會要求使用者必須安裝附加元件（在IE瀏覽器是叫Acitve X元件，FireFox是Add on，還有Google Chrome Extentions），常見於網路銀行、網路ATM網站等。然而駭客所製作的假網站也會藉此，將惡意程式包裝在Acitve X裡面，讓你自己將惡意程式下載安裝。所以，如果非必要，請不要任意安裝Active X元件，或者一定要確認該網站的真實性，非可疑的釣魚網站才安裝。

❷ 小心Cookie洩漏過多你的隱私

Cookie是一種遠端網站在你的電腦中讀取或是記錄的資訊。設計的本意，是讓網站對不同的使用者進行上網行為的了解與分析，進一步提供更貼切的服務。例如：連線到「國家圖書館遠距圖書服務系統」，從網頁右邊的資訊顯示為「第4次光臨」這個網站，或者讓你以後登入時提供個人化首頁。雖然Cookie的設計本意十分良善，也不一定有嚴重的危害，但卻可能淪為不當的使用，因此你可以透過瀏覽器當中的隱私權設定，決定接受或拒絕各網站的cookie。

此外，目前網路上有許多資源可以提供使用者辨識可疑的網站，網友們可以多加利用：

網頁過濾機制來源與網站信譽評等服務

目前網路服務業者也提供家中上網的網頁過濾機制，使用者不必安裝任何軟體或設備，也不必做任何設定，就能達到阻擋不適當網頁的目的。而台灣網站分級推廣基金會亦有提供網站過濾軟體，針對色情、暴力等內容的網站做過濾。

同時，資訊安全業者也已經在防毒軟體中提供網站信譽評等服務，透過雲端蒐集各種現行犯的黑名單，在使用者上網時幫你做安全把關。並且提供免費瀏覽器外掛程式(for IE & Firefox)，可針對網頁上的內容，提供瀏覽網頁時的安全性建議，諸如網頁

釣魚、廣告程式、間諜軟體、垃圾郵件等，並且以顏色區分嚴重性(綠、黃、灰、紅)；此外透過此外掛程式使用搜尋引擎(Google、Yahoo等)時，會直接在搜尋結果上以色塊來表示該網頁的安全性，以達到防護的效果。

此外，現在較新版本的網頁瀏覽器亦提供相關的網頁安全警示與過濾，像是彈跳的廣告視窗、釣魚網站、於網頁中要求額外安裝軟體元件、以及已經被列為黑名單的網頁，都可以做基本的阻擋與過濾。

資料來源：重灌狂人

圖1. 出現疑似釣魚網站，Google Chrome瀏覽器畫面出現顯目的紅色警告。

安全圖章認明真實網站

某些電子商務網站會提供由用戶自行上傳圖檔，作為個人安全圖章的機制，使用者一旦連線到該網站就會出現用戶自己設定的圖章，可以讓使用者判斷是否瀏覽到正確的網頁，接著才輸入帳號密碼登入。通常運用於網路銀行等需要高安全或經常被偽冒的電子商務網站上，避免用戶瀏覽到假網站，不慎輸入密碼。

現在的網站偽造技術越來越高竿，伴隨著各種網路威脅在蔓延。善用上述資源，輸入個人資料前，小心辨識真假網站，甚至直接電話洽詢電子商務網站客服人員，才能確保自己個人資料的安全。

資料來源：Yahoo!奇摩

圖2. Yahoo!奇摩提供安全圖章的設定

網路安心購物小叮嚀

1. 加入電子商務網站會員，填寫個人資料時，選擇EV SSL加密（或至少有SSL加密）、網址列有https的網站。
2. 檢查網站的數位憑證，看憑證是否仍在有效期限內，以及是否為合法第三方數位憑證服務商所簽發。
3. 填寫資料前，也可查看網站是否有取得第三方認證標章。
4. 安裝提供網站信譽評等服務的防毒軟體。
5. 開啟瀏覽器提供的網頁安全警示與過濾功能。
6. 不要使用無線網路進行線上購物，尤其是未提供SSL加密的網站。
7. 使用電子商務網站提供的安全圖章功能，認清圖章才登入網站。

拍賣

詐騙防範 心法

除了一般購物網站可利用上述說明之方式找到安全的網站，網路拍賣也可搭配正確的使用方式，透過簡單步驟，就能輕鬆判斷、找對良好賣家。

第一步

進到賣場，先看賣家基本資訊「關於我」

民眾往往因為商品限量或下標時間快到了而急著下標，這樣就容易誤觸陷阱。

進入賣場首要進行的，即是觀看賣家基本資訊是否齊全且正常：

1. 可透過多樣聯絡管道聯繫賣家，電話或手機尤佳
2. 基本資料提及之販售類別，與實際販售商品類別相同
3. 配送方式有明確說明，若有長期配合之貨運商尤佳

資料來源：網路資料

圖3. 網拍詐騙案例：「關於我」無任何資訊

第二步

挑選幾項賣場販售的其他商品看看

不僅要仔細觀察欲購買的商品，其餘商品內容也需要看看對方是否有善盡良好賣家之責：

1. 刊登商品圖片來源，若皆為官網圖片需特別注意
2. 商品狀況清楚(含製造日期、有效期限、保固狀況等)
3. 商品刊登期間正常，無過多商品短期內上架又下架
4. 商品資訊或「問與答」中未出現簡體字

第三步

善用交易評價與安心賣家制度

交易評價不能只看表面！而是要觀察交易評價的獲得期間、獲得商品類別、獲得來源對象等：

1. 獲得期間未集中於特定期間
2. 交易後與獲得評價的時間間距，沒有過短(10分鐘內)的狀況
3. 獲得商品類別與目前銷售類別相符，無短期內大量轉換的情形
4. 獲得來源對象，沒有互評、互拱的狀況
5. 交易金額沒有以1元或低價大量交易狀況
6. 評價資訊說明正常，特別注意負評的說明

此外，還能透過拍賣平台設置的安心賣家制度，與完成「真實身分驗證」、並且「啟用帳號保護」相關設定的拍賣賣家進行交易，提高保障。

資料來源：Yahoo!奇摩

圖4. 選擇安心賣家有助避免遭受網路詐騙

除了以上幾個步驟一定要做到外，**如果不是直接面交、貨到付款，千萬不要透過「私下交易」向賣家購買商品**，否則一旦遭受詐騙，將難以追討損失，落入財物兩失求助無門的窘境。

網路 反詐騙資源

1. 165反詐騙諮詢專線(http://www.165.gov.tw/)

提供各種詐騙檢舉、報案、查詢管道，及預防詐騙宣導。

2. 網路釣魚通報單一窗口（www.apnow.tw）

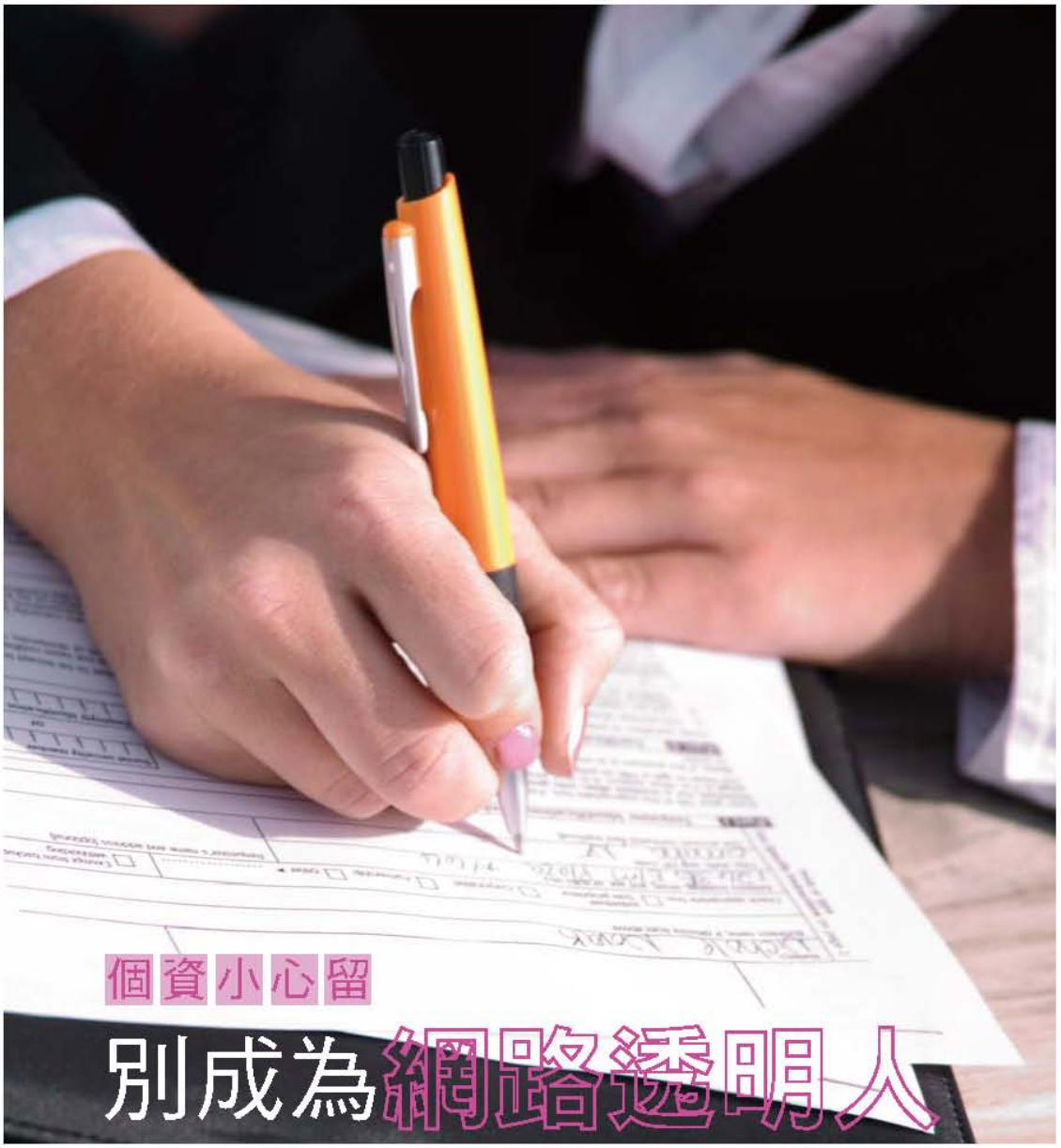
發現網路釣魚，請通報臺灣網路危機處理暨協調中心（TWCERT/CC），提供網路釣魚通報單一窗口。

3. 網路不當內容通報單一窗口(www.win.org.tw)

發現網路不當內容，涉及犯罪，請通報臺灣網站分級推廣基金會——「WIN網路單e窗口」，提供民眾檢舉不良網路內容。

十大網路 攻擊手法與對應招數

	網路攻擊現象與詐騙手法	資安意識	對應招數
1	電子郵件隱藏電腦病毒	不要開啟、不要點擊	安裝防毒、電腦更新
2	電子郵件網路釣魚	不要開啟、慎填資料	防垃圾郵件與釣魚郵件過濾；掌握新知
3	網頁掛馬	不要開啟、不要點擊	網頁過濾機制來源與網站信譽評等服務；安裝防毒軟體、電腦更新
4	Web phishing網頁釣魚	不要開啟、慎填資料	網頁過濾機制來源與網站信譽評等服務；掌握新知
5	假廣告隱藏真危機	不要開啟、不要點擊	網頁過濾機制來源與網站信譽評等服務；安裝防毒軟體
6	PDF與Flash檔案的零時差弱點攻擊	不要開啟可疑的檔案，對系統發生錯誤要有警覺	安裝防毒軟體、電腦更新(尤其是PDF與Flash套件)
7	殭屍病毒橫行	電腦、網路緩慢可能是其徵兆	安裝防毒軟體、電腦更新、開啟防火牆
8	P2P 與軟體下載惡意程式	不要亂下載，不要開啟來路不明的檔案	安裝防毒軟體、電腦更新
9	社交網路弱點攻擊親友關係	不明訊息應向本人確認、不要開啟可疑的連結	掌握新知
10	智慧型手機的弱點攻擊	不明簡訊應多加注意	安裝手機防毒



個資小心留

別成為網路透明人

填寫個人資料時，應掌握個資安全原則，才能不被犯罪集團完整蒐集，減少受騙上當的可能。

網路世界，不管你要進行任何網路活動，使用網路服務、線上購物消費，多半都需要你加入會員、留下個人資料。再加上在實體世界，我們早已在各政府機關、電信公司、金融機構，甚至路邊問卷等場合留下各種個人資料，可以說個人資料早已不是秘密，廣泛散佈在各類公私立機關單位的資訊系統中。

一旦這些擁有民眾個人資料的機關網站，不慎遭到入侵發生資料外洩事件，或是其中員工電腦中毒，皆可能導致資料被竊。犯罪集團掌握了這些機關所擁有的個人資料，馬上就假冒各機關客服人員，打起詐騙電話，或者寄發釣魚郵件等各種詐騙手法。

許多網友不了解個人資料安全的重要性，以為接到電話不要理睬、不要轉帳就沒事，而這樣的態度正好讓部分不肖業者繼續坐視網站安全問題不管。殊不知當犯罪集團透過**資料拼圖**的手法，從A網站得知民眾的基本個資，從B網站得知所使用的金融商品或近日消費內容，兩相組合，就可以編造天衣無縫的釣魚郵件，或更精巧的詐騙話術，若不特別提防，十分難以辨識。

社群網站、Blog 讓你變成 透明人

近來，在報章媒體上出現一新名詞"人肉搜索"，所謂人肉搜索就是利用關鍵字加上資料拼圖手法，即可以一步一步找到當事人姓名、住址、電話、畢業學校、或任職公司等資料，而這些資料往往都是自己填寫並存放在網路上。

網路平台處處都會留下使用者個人資訊及使用者記錄，凡不必要的資料勿留於網際網路上。許多人每天在社群軟體、網路上寫部落格留下記錄的同時，也等於把個人隱私給公開了。千萬不要相信把重要資料留在網路平台上，設有密碼就是安全，

不會造成資料外洩，特別是將個人機密資料。甚至有些使用者可能怕密碼忘記，還特別輸入密碼提示，用來提示自己密碼，但往往自己不知，透過Google資料拼圖手法，或是自己在網站留下的個人資料中，就已經大方的公佈密碼出來(圖1)。

因此，在任何需要留下個人資料的場合或網站都要謹慎。嘗試利用自己的名字搜尋，看是否有過多的個人隱私訊息被放在公開網站上，小心保護個資隱私才能降低詐騙成功率。

圖1. 資料拼圖手法

保護個資 5要點

以下是保護個資安全的基本觀念，盡量不要讓自己的個資被犯罪集團完整蒐集，就能減少被詐騙成功的可能。

1 注意網站隱私權保護政策

在註冊加入會員或輸入個人資料時，應注意該單位或網站的信用情形，留意網站是否有隱私權保護政策的宣告，以及對於敏感個人資料是否加密等。不要未察看會員條款或隱私保護政策，就輕易按下「我同意」的按鈕。

2 不想被看到的資料不要上網

在填寫個人資料時，除設定密碼要多用心，避免被人猜中外，更重要的是不要把重要的資料或個人隱私留在網路上，包括將個人生活作息細節公開在網誌上。否則都會有外洩的疑慮，當網站資料發生外洩時，往往是自己無法控制。

3 能用化名就用化名

除了對政府提供的資料以外，其他各種買賣交易或路邊問卷能用化名的場合，就不要用真名。甚至在不同網站所留的姓名都取不同，將來還可以識別是在哪家留的資料。例如，在Y購物網就是王小虎，在P購物網就是王小家，這樣將來若接到詐騙電話就知道是哪家購物網站出問題。

每個網站留不同的資料做為識別

方法1：送貨地址加上寢室號碼

在不同購物網站加入會員留資料時可以動一點手腳，例如把送貨地址做不同標示，例如在A購物網的地址留：XX路X號X樓201室，而在B購物網則留202室，這樣一來，商品一定都能送達，而自己也能識別是在哪家留的資料。

方法2：不同網站留不同名字

不要留真名，在不同網站所留的姓名最後一個字都不同，例如在Happy購物就是王小樂，在P購物就是王小家，這樣可輕易分辨資料外流途徑出問題。

4 只填必填的資料

只填寫必須填寫的資料，且不要輕易洩露會危害自身安全的資料。在許多網站的會員註冊資料畫面中(圖2)，可發現其必填項目含有相當多個人隱私資料，要求填寫的越多，一旦網站資料外洩時所造成的傷害越大，例如會員的聯絡地址，只要透過Google Map(圖3)一查，就可快速搜尋出住家位置，包括附近有什麼商店，甚至是距離最近的ATM、銀行等，都可以很快的查詢出來。因此進行網路購物時，可使用超商取貨，就盡量不要留下地址。

圖2. 會員註冊資料畫面

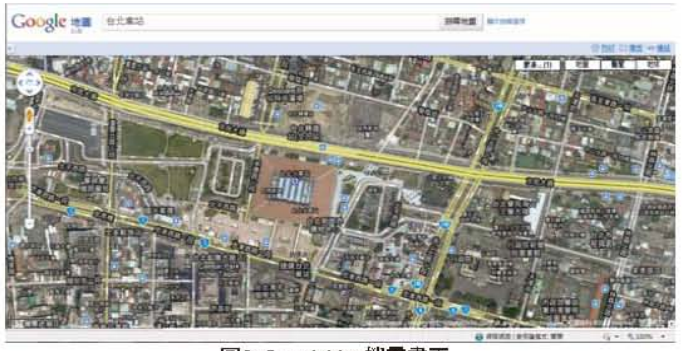


圖3. GoogleMap搜尋畫面

5 設定安全的帳號密碼

在網路上如果沒有設定帳號密碼的電腦，就等於是對網路敞開自家大門，如果遇到駭客或有心人士，透過簡單的工具及猜測，都可以登堂入室，竊取資料。

密碼設定建議：

1. 密碼的長度在8個字元以上
2. 避免使用英文單字或利用鍵盤順序、帳號作為密碼
3. 中英文交雜、混合大小寫與特殊符號及輸入法的組合
4. 不要使用生日、姓名、手機號碼等自身相關資訊
5. 不同的網站應該使用有不同的帳號及密碼，並儘量不要有規則性。

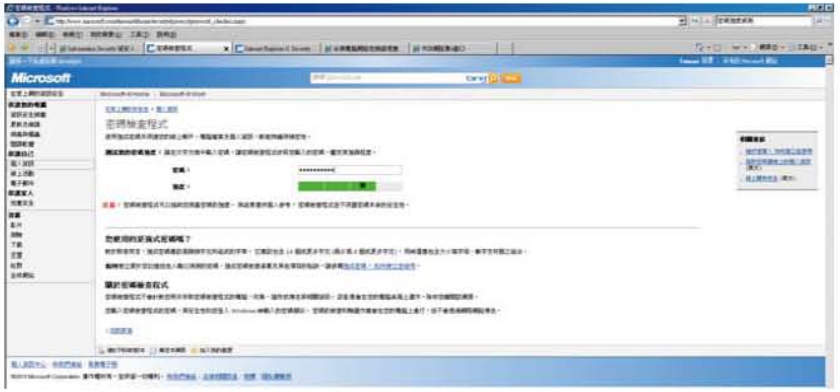


圖4 微軟網站提供密碼檢查程式，可檢測密碼強度

密碼回復機制也要小心。透過其他的資訊或者是電子郵件信箱，可以針對網路帳號的密碼進行回復或重設，所以一定要選擇一個較嚴謹的回復問題與答案，避免被猜測出密碼回復的關鍵字詞。同時，密碼一定要定期做更新，避免遭到盜取後，長時間不知不覺被盜收信件，進而被詐騙。

此外，在電腦安裝防毒軟體與防火牆更是最基本的安全防禦措施。透過電腦防火牆可以將網路面的攻擊先行攔截，並且過濾掉不必要的雜訊影響，而且可以有效阻擋網路蠕蟲的擴散，在 Windows或 Linux平台本身就具備單機防火牆的設定，只要透過簡單的步驟即可開啟；電腦系統與軟體的自動更新機制也需要開啟，以避免駭客利用系統弱點入侵電腦。微軟針對Windows系統推出修補更新時，會通知使用者執行更新程序，可以注意視窗右下角會出現一個提醒更新的圖示（圖5），就是告訴使用者要記得更新修補程式，除了作業系統之外，常見的軟體也必須要做更新，例如Flash Player、PDF Reader、瀏覽器以及微軟Office、iTunes軟體等。千萬不要因為安裝更新程式花費一點時間，而忽略此步驟。

圖5. 定期安裝修補程式是上網安全的基本步驟

認識新版

個人資料 保護法

新版個人資料保護法已於99年5月26日正式公告，並於101年10月1日正式實施，您知道新法與舊法差別在哪嗎？以下就以13個Q&A帶領您快速了解新版個人資料保護法，在網路上交易時更能有效保護自身權益：

Q1 為什麼要有新版個人資料保護法？

A 新版個人資料保護法是由舊版「電腦處理個人資料保護法」修法而來，因舊法的保護範圍有限且內容不合時宜，故新法刪除「電腦處理」的字樣，擴大了個人資料保護的範圍，也讓所有產業皆適用。

Q2 新版個人資料保護法實施後的影響範圍？

A 新版個人資料保護法不僅適用儲存於電腦使用的個人資料，也適用於紙本書面紀錄(含手寫)的個人資料喔! 此外，不僅是「各行各業」要遵守，連「個人」也是，只要是中華民國的國民，不管是在國內或國外，都要遵守個資法。

Q3 新版個人資料保護法保護的資料有哪些？

A 新版個人資料保護法所定義的個人資料，指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。需要特別注意的是，往生者的個人資料並不受個資法保護。

Q4 哪些個人資料處理行為會受到新版個人資料保護法規範？

A 個人資料的蒐集、處理、利用都會受到新版個資法的規範。也就是從個人資料蒐集開始，到資料怎麼處理與利用的目的、程序，整個過程都必須符合規定。

Q5 個人資料蒐集、處理、利用的定義？

A 蒐集：指以任何方式取得個人資料。包含合法紀錄或非法手段取得個人資料，而且不限定媒介，不管是在網路留會員資料、或是路上填寫問卷，都算是蒐集行為。

處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

利用：指將蒐集之個人資料為「處理」以外之使用。例如將蒐集而得的個資拿來進行行銷活動、販售等行為。

Q6 蒐集個人資料時，要注意什麼事情？

A
1. 並不是每種資料都可以蒐集。新版個資法加入了「特種資料」的概念，也就是敏感性資料，包含醫療、基因、性生活、健康檢查、犯罪前科等。在沒有法律明文規定下，蒐集這些資料是違法的。
2. 蒐集個人資料要有特定目的、且合乎個資法規定。對於個人資料的蒐集、處理、利用，都必須符合法務部所公布的「特定目的」內容；此外企業蒐集個資，需符合個資法規定的合法蒐集項目，如與當經當事人同意、與當事人有契約關係等。
3. 善盡告知義務。新版個資法規定蒐集個人資料時，須善盡告知之責，明確以書面、電話、傳真、電子文件或其他適當方式，告知當事人資料蒐集的目的、所蒐集資料的類別、資料利用的方式等項目。

Q7 個人資料被蒐集了，可以隨時請對方更改或刪除資料嗎？

A 可以的!

依據新版個資法，當事人有權利對於個人資料行使查詢、閱覽、製作複本、補充或更正資料，蒐集者必須要在個資法規定的期限內(15-30天)回覆。當事人也可以要求蒐集者停止資料的蒐集、處理或利用，並且可以要求刪除個人資料檔案。

Q8 可以拒絕企業利用我的個人資料進行行銷嗎？

A 可以!

企業在第一次利用當事人資料行銷時，就必須取得當事人同意，並且提供當事人可表達拒絕的方式與費用，當事人表達確定拒絕之意時，就必須立即停止利用個人資料行銷。

Q9 透過別人取得個人資料，也要遵守相關規定嗎？

A 是的!

依據新版個人資料法規定，間接透過第三方取得個人資料，也必須告知當事人，並說明個人資料來源。受第三方委託蒐集資料，也一樣要受個資法規範。

Q10 對於蒐集而得的個人資料，應盡到什麼責任？

A 對取得之個人資料，應善盡保管之責，採取適當的安全管控措施，防止資料被竄改、失竊、遺失或洩漏。

Q11 公務機關與企業違反個資法，要負什麼責任？

A

公務機關：除非是因天災事變或其他不可抗力之因素，公務機關違反個資法需負損害賠償責任。

非公務機關：企業若能證明無故意或過失，則無須負責。反之，若無法證明，則須負損害賠償責任與2萬至50萬之行政罰鍰。

上述的損害賠償責任，包含非財產損害可以請求賠償相當之金額、名譽受損也可以請求適當賠償，若被害人不易或不能證明其實際損害額時，法院得依侵害情節，以每人每一事件新臺幣500元以上2萬元以下計算賠償金額。

此外，同一事件造成多數當事人受害，合計之最高賠償總額以新臺幣2億元為限；但若該事件所涉利益超過2億元者，以該所涉利益為限。

Q12 個人資料受到侵害，提出求償有時間限制嗎？

A

當事人必須在知道事件的2年內提出求償，或在受害事件發生的5年內提出求償，若超出期限則失去求償機會。

Q13 個人資料受到侵害，只能單獨提出求償訴訟嗎？

A

新版個資法可以進行團體訴訟。只要有20位以上個資受侵害之當事人聯合，可以書面授權委託財團法人或公益社團法人，代為提起損害賠償訴訟。

新版個資法下的個人資料保護權益

新版個資法對於個人資料的當事人提供了確切的權益，即使同意將資料提供給他人，也仍具有自主權利，當事人可以對自身個人資料保有決定權。在個資法第3條中，明文規定當事人具有以下5種權利：

1. 查詢或請求閱覽自身個人資料

無論是公務機關或非公務機關蒐集而得之個人資料，都不得拒絕當事人查詢或閱覽。例如民眾可向健保局查詢就診紀錄、成為商店會員後可查閱消費紀錄等。因此，各機關應妥善保管當事人之個人資料，以提供當事人隨時查詢閱覽。

2. 請求提供自身個人資料複製本

民眾若對於想保存自身所提供之個人資料，例如消費明細、健康檢查報告等，可隨時向機關申請提供複製本。

3. 請求補充或更正自身個人資料

若民眾對於自身於機關留存之個人資料有疑問，欲補充或更正相關資料，可請求機關協助維持資料的正確性。例如，因更換租屋處後，一併更改聯絡地址，可請信用卡公司更改帳單地址。個人資料的正確性常與資料蒐集之特定目的有關，若資料錯誤，將造成蒐集目的無法達成，故當事人與機關皆應主動維持資料的正確性。

4. 請求停止蒐集、處理、利用自身個人資料

民眾可主動要求機關停止繼續蒐集、處理、利用自身個人資料，例如因信用卡剪卡後，可一併要求發卡銀行與信用卡公司蒐集相關財務資訊。尤其是在民眾在未被告知的情況下就被蒐集個人資料，可主動行使此項權利，以保障個人資料安全。

5. 請求刪除自身個人資料

若不希望自己的個人資料一直留存於不會繼續往來的機關內，民眾可請求機關刪除自身個人資料。

除了上述5項權利外，個資法尚提供當事人拒絕提供個人資料用於特定目的；在發現自身權益受損時，當事人也能行使損害賠償請求權利。民眾一定要具備足夠的個資保護意識，才能有效行使個資法所賦予之權利，而不致使個資被濫用喔！

行動飆網

安全自保之道

隨著行動裝置越來越普及，行動飆網隱藏的危險也隨之而來，要避免危險上身、個資失竊，必須先建立正確的行動上網意識、養成基本的安全自保習慣，就像在危險海域，立上禁止游泳的告示牌、做好第一道防線。

您發現了嗎？生活中到處都是「低頭族」！

根據資訊工業策進會和經濟部「科技化服務價值鏈研究與推動計畫」於2012年的調查結果，台灣持有智慧型手機或平板電腦的族群約有707萬人；預估到2015年，台灣智慧型手機普及率將達56.8%，平板電腦普及率也將達到24%。

當智慧型手機與平板電腦取代傳統電腦，逐漸成為生活中與朋友互動聊天、分享樂事、上網看新聞、玩遊戲…等隨身攜帶不可或缺的工具，手機與平板電腦也變成駭客攻擊的目標，受到的安全威脅愈來愈多。

建立 行動上網的 正確意識

對於很多人而言，對於手機的安全認知仍停留在許多年前，安全、使用簡單、方便攜帶，然而隨著智慧型手機與平板電腦功能越來越強大，這些裝置都已經可視為一種迷你電腦，舉凡電腦可能遇到的駭客入侵、感染病毒等等，無一不是安全威脅；更遑論上網可能遇到種種資安問題，手機跟平板電腦都有可能遇到！而行動裝置可隨時無線上網的特性，更可能成為不肖份子利用來入侵竊取資料的工具。

以下，我們將介紹使用行動上網必備的幾種正確警覺意識，透過建立正確意識，可有效協助您避免手機或平板電腦被入侵的危機。

1.手機跟平板電腦，一樣都會中毒！

因為行動裝置中毒，往往不像桌上型電腦一樣反應明顯，因此很多民眾不知道自己的手機跟平板電腦，跟桌上型電腦一樣，都會感染電腦病毒、被植入惡意程式。不管是透過上網、與電腦串接，都有可能被入侵、因而中毒。

行動裝置中毒的常見徵兆

行動裝置一旦中毒，雖不像傳統桌上型電腦般容易發現，卻仍有跡可循，當出現以下幾種徵兆，使用者就可懷疑手機或平板電腦是否受感染，可趕緊尋求專業援助，多一分警覺、少一點受害可能：

- ◆ 使用效能無故變差
- ◆ 電池壽命突然變短
- ◆ 莫名其妙通話中斷
- ◆ 電信費用突然爆增
- ◆ 出現自動下載軟體

2.遺失手機跟平板電腦，是重要個資失竊的導火線！

當手機跟平板電腦遺失後，不僅僅是遺失了儲存在內的照片、音樂與影片，還包含通訊錄、簡訊或通訊軟體的訊息紀錄、瀏覽器的會員帳密紀錄等等，這些資料很有可能被詐騙集團拿來使用，進一步利用資料拼圖或拆解等方式，得知交易資訊或信用卡資料，不可不防！

3.不管使用哪種作業軟體，都存在資安風險！

很多民眾被新聞或論壇訊息錯誤引導，誤認為使用Android作業系統的手機或平板電腦才會有資安問題產生。其實，不管是哪種作業系統，都存在著資安風險，切勿抱存僥倖的心理，認為使用冷門的作業系統就不會碰到資安事件，事實上，每種作業系統都不是百分之百安全，好的使用習慣才能保護使用者本身。

4.上網跟下載APP，是駭客入侵的主要管道

相較於傳統桌上型電腦，駭客入侵行動裝置的手法較為單純，主要透過使用者上網瀏覽時的使用疏忽、非法或惡意APP下載為主要管道。使用者在開始行動上網時，一定要當成使用一般電腦，所有注意事項皆須銘記在心，例如不輕易點選網路上的不明連結、填寫個資時再三確認網站為合法正確的網站；下載APP時也能仔細檢查開發者與軟體資訊。

有關於行動上網須注意與建立的安全習慣，我們將在後續章節進一步說明。

常見 犯罪手法

近年來網路詐騙、資安事件不斷，而主要有關行動裝置的犯罪手法，不外乎有三種類型：結合社群網站與社交工程進行手機簡訊碼詐騙、偽冒惡意APP軟體下載、網路釣魚惡意連結，以下我們將逐一擷取新聞案例加以分析說明。

1. 盜帳號佯裝親友，騙取手機簡訊認證碼

新聞案例：詐騙手法轉型　手機簡訊認證碼淪陷

資料來源：ETtoday東森新聞，2012/07/30

詐騙集團會先盜用臉書的帳號和密碼，再利用這個帳號大量發送訊息給親友，騙說自己的手機沒電或故障，請親友代為接收並告訴認證碼。

新聞案例：新式網路詐騙 投票也能騙手機認證碼

資料來源：T客邦，2012/08/20

新的詐騙網站是藉由 Yahoo 攝影來吸引網友進行投票，當你在投票的過程中，網頁會要求你輸入你的手機號碼，並填入一筆認證碼，完成之後，網站就能獲得你的手機認證來進行小額扣款的動作。

手機簡訊認證碼的詐騙事件，已經從以前的MSN(現改為Skype)、Yahoo!即時通轉移至臉書，更進一步擴及通訊軟體APP上(LINE、WhatsApp等)。透過盜帳號佯裝親友的方式，主要目的就是騙取手機簡訊認證碼後，進行網路「小額扣款付費」交易行為，輕則損失幾千元，重則被當成拍賣網站的人頭帳戶。

2. 偽冒知名APP，誘惑民眾下載之惡意軟體

新聞案例：Candy Crush山寨版成駭客竊取個資工具

資料來源：經濟日報，2013/03/31

近來在Facebook以及Android系統平台造成廣大迴響的遊戲應用程式「Candy Crush」，出現針對行動裝置所推出的山寨版，該版本中含有廣告程式ANDROIDOS_LEADBLT.HRY，以竊取裝置的GPS定位、Sim卡國碼、作業系統版本等資訊。ANDROIDOS_LEADBLT.HRY，以竊取裝置的GPS定位、Sim卡國碼、作業系統版本等資訊。

新聞案例：賽門鐵克：行動上網夯 熱門應用程式遭駭客鎖定發動惡意攻擊

資料來源：自由時報，2012/12/06

熱門手機照相應用程式 Instagram 在全球累計已超過 1 億名使用者，但也因此成為駭客攻擊的跳板。賽門鐵克發現，藉由發表評論、假跟隨者（Followers），以及為照片按讚等，駭客在 Instagram 上用各式各樣的方法誘騙使用者至假帳戶點選連結，以騙取個資或誘騙使用者購買付費服務。

買到智慧型手機、平板電腦後，最重要的事是什麼？當然就是把所有熱門APP全部都下載下來用個夠玩個夠！然而，您知道知名的APP在下載過程中，可是有許多危機潛藏。不肖份子抓緊使用者急迫使用熱門APP的心態，在戒心較低的狀態下，以山寨版、偽冒的APP誘騙民眾下載，將惡意程式植入；或是利用APP評等討論、廣告圖片引誘民眾點擊惡意連結，不可不防！

3. 惡意連結藉由社群通訊、APP廣告四處散播

新聞案例：Android出現惡意連結程式　小心被盜個資！

資料來源：Nownews今日新聞網，2012/09/27

Android系統竟然出現惡意連結程式！使用Android系統智慧型手機的民眾要特別注意，國外已傳出，有惡意程式以簡訊、連結甚至二維條碼(QR Code)的形式出現，使用者按下之後，手機會回到出廠原始設定，資料全部洗掉，甚至可能被盜個資。

新聞案例：應用程式廣告成不肖人士騙取個資管道

資料來源：趨勢科技，2013/05/20

近來疑似有詐騙集團利用行動應用程式廣告進行詐騙。該廣告宣稱可以極優惠的價格提供消費者「 iPhone5 」以及「 Samsung Galaxy Note II 」等知名品牌手機，一旦點選該廣告後，使用者將被導向特定網頁，該網頁要求使用者提供手機號碼和詳細住址，造成使用者個資外洩，進一步為不肖人士利用。此類透過行動應用程式廣告的詐騙手法目前已盛行於中國大陸，但不排除有可能針對台灣使用者進行類似的網路詐騙攻擊，民眾應提高警覺。

隨著行動裝置通訊軟體日漸蓬勃發展，當我們享受跟朋友密切聯絡的好處時，更多網路威脅也隨之而來。藉由社群APP、或是透過瀏覽器連上社群網站等方式，行動裝置已能做到與社群無縫接軌。然而，民眾使用行動裝置的安全意識遠低於使用PC、NB時；手機與平板電腦的小螢幕，也常常成了駭客利用的工具。字體狹小、說明不清的惡意網址連結，透過手機簡訊、APP訊息或廣告圖片、E-mail信件內容到處散播，藉由吸引人的文字誘惑使用者點入，一個不察，就會被引導入惡意網站，或是中了惡意軟體或病毒。

4. QR Code:下一代新詐騙工具

新聞案例：掃描換電影票，「QR Code」成詐騙工具

資料來源：TVBS，2012/12/19

大陸出現利用「QR Code」的新詐騙手法，專門針對智慧型手機上網用戶，誘使民眾以掃描「QR Code」的方式，就可以換取免費電影票，然而在連結和下載的過程中，被強制安裝「惡意程式」，一次耗盡200G的網路流量後，儲值卡內的電話費也被吃光光。

行動裝置搭載相機功能已成常態，QR Code(二維式條碼)使用越來越多元，目前已被廣泛應用於廣告文宣、取得購物優惠以及下載連結等行銷用途上，只要輕輕一掃，就能快速取得相關訊息，甚至連知名社群通訊軟體Line也應用於邀請新朋友上。

使用者通常會不加思索地用相機去掃描QR Code，接著進入相關訊息網頁、開始使用服務，也因此成為不肖份子詐騙的管道之一：只要偽造QR Code所連結的網頁，就能輕易取得個資、植入惡意程式進行破壞。

養成 行動上網的 安全好習慣

使用手機、平板電腦竟然有這麼多危機，究竟該如何因應呢？不妨從養成行動上網的好習慣開始，只要具備足夠的危機意識、使用習慣，就等同於築起了第一道防線，讓駭客不容易入侵我們手中的行動裝置，取得我們的重要個資。以下，將介紹幾個行動上網必備的使用好習慣，享受行動方便的同時，也一起來捍衛資訊安全吧！

安裝行動裝置適用之防毒軟體

許多人都會問，拿到手機、買到平板電腦後，第一個APP該下載哪個呢？當然就是手機防毒軟體囉！目前市面上已有多家業者推出手機防毒軟體可供下載，民眾可依需求選擇，下載後，一定要記得啟動自動掃描與定期更新機制，才能確保全面防護到行動裝置安全。

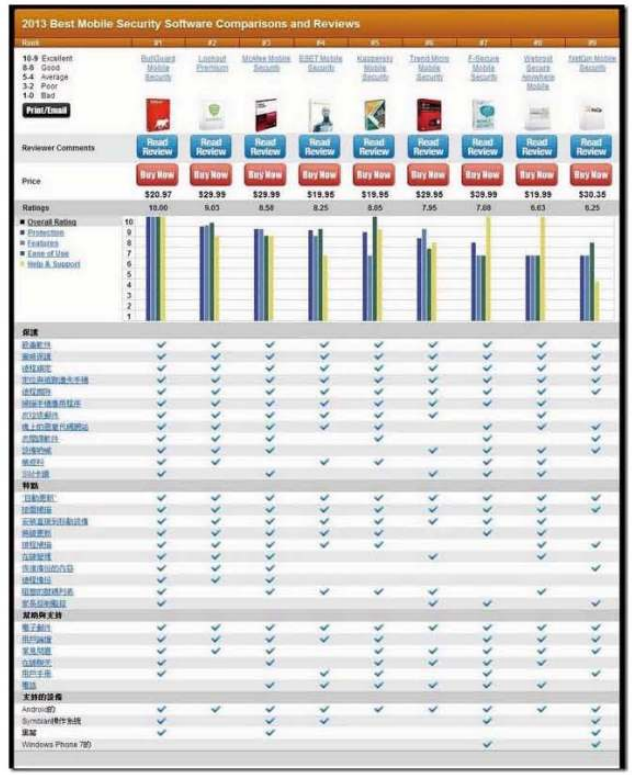


圖1. 2013年最佳行動防毒軟體排行榜
原始出處：http://mobile-security-software-review.toptenreviews.com/
翻譯圖片出處：http://www.kocpc.com.tw/archives/2454

下載APP，注意開發者、評等評論、與授權資訊

使用手機或平板電腦，下載APP是必要的過程。許多駭客即利用行動裝置使用者下載APP時的疏忽，入侵竊取資料或植入惡意程式，因此，在下載APP時能夠有良好的檢查習慣，可以有效避免下載到惡意APP的危險。

下載APP好習慣：

(1)注意開發者

在各類APP購買與下載平台上，皆能取得開發者資訊，除了仔細觀察開發者是否正確外，更必須看看開發者其他上架的APP。如果開發者本身的資訊極少、上架的APP名稱草率取名、不同APP間名稱與功能相似度極高，或是僅有一支APP上架，就必須小心此開發者，避免下載該APP。此外，下載APP應盡量至開發者網站或經過認證的下載平台，以減少下載到山寨版APP的可能性。

(2)注意評等評論

大部分的APP購買與下載平台上，都會有APP評等與評論機制。當評等人數夠高、評論夠多，其參考價值也隨之上升。若評等人數少且評等皆高，或從評論中發現有關使用上的留言，就必須特別注意，尤其是當有網友留言此APP會影響其他APP運作、授權或隱私聲明有問題時，建議不要下載。

(3)注意授權資訊

在下載APP安裝時，許多APP會告知需要取得使用者授權，授權內容包含個人資訊(如聯絡人、GPS位置、通訊錄等)，或是系統功能(如照相功能、上網連線功能等)，大部分使用者對於授權資訊往往略過確認流程、直接快速按下同意鍵，殊不知這就是網路駭客常鑽的漏洞。在同意授權前，一定要再三確認APP的功能與要求授權權限是否相符，如修圖APP可同意取得存取相機功能的權限。

在外不輕易使用免費Wi-Fi無線上網

在許多公共場合，如旅遊飯店、咖啡館、餐廳等地方都會所提供的免費 Wi-Fi上網，而這些並沒有加密或設定密碼保護，往往就成為駭客竊取個人資料的目標。駭客透過攔截封包加以分析，輕易地就能獲取使用者的重要個資； 2012年美國聯邦調查局FBI也曾發現有惡意程式專門針對飯店免費Wi-Fi使用者，以彈跳視窗(pop-up windows)的方式，要求先更新某個應用程式才能使用網路，許多使用者不疑有他，選擇更新後，惡意程式就會直接被下載至電腦或手機中。

避免上述危機的解決辦法，就是不使用免費的Wi-Fi無線上網服務。迫不得已要使用時，也能對於連接上網的步驟特別小心，依循服務提供者的指示進行(如飯店之無線上網說明文件)，一旦連上網，也不輸入任何重要的帳號密碼、個人資料。

點選網址連結、開啟郵件附件時特別小心

利用具吸引力的標題，引誘使用者點擊網址連結或開啟信件，向來為駭客常利用的社交工程技巧，許多惡意程式即藉此方式趁機安裝於使用者的電腦中。因手機、平板電腦等行動裝置上，礙於螢幕較小、民眾使用時戒心較低，更容易遭受引誘，開啟植入於廣告圖片、信件內容等惡意連結，進而被誘導入偽冒網站騙取重要個資。使用行動裝置時，對於各類網址連結、郵件附件更要特別小心，開啟前先確認1.提供資訊者/發信者是否為熟識的人(確認來源是否可靠) 2.網址或信件檔案標題無亂碼資訊3.主動詢問連結或附件是否安全。透過幾個簡單的小習慣，檢視欲點擊的網址連結或郵件附件，避免自己習慣於”順手點擊”而造成資訊安全上的漏洞。

驗明正身 網路安心購物3部曲

1. 網頁出現網站身分識別標章
2. 網址開頭為https://網址列窗格變綠底
3. 點選標章出現網站中文資訊

強化電子商務交易安全

主辦單位 經濟部商業司　執行單位 中華民國資訊軟體協會 CISA

小心 網購個資外洩 詐騙陷阱

跨境整合・打擊犯罪 165 打擊詐騙大行動

內政部警政署關心您 www.165.gov.tw

請牢記

聽 聽來電內容　掛 掛斷電話　查 165 反詐騙專線查證


電子商務 iPad mini 挑戰賽
正牌網站·正港安心
已認證
網站身分識別標章
Authenticated Website


您的網站經營
安全嗎？
詐
面對親手經營的網路事業版圖，
卻不懂得該如何著手保護它嗎？
面對林林總總的山寨版網站頁面，
卻不懂得該如何杜絕嗎？
沒關係～
讓經濟部商業司來幫助您！！！
電子商務資安檢測與輔導計畫
實施資安建置①、②、③
企業資料保護好簡單！
①
技術導入
強化
資安防護
②
顧問協助
建立
資安制度
③
稽核審查
確保
防禦提升
已認證
網站身分識別標章
Authenticated Website
電子商務網站身分識別機制
推廣計畫網站身分識別標章
正牌網站，正港安心。
做好資安防護，經濟部商業司幫助您～
相關申請辦法請洽計畫網站：http://www.ec-security.org.tw/index.aspx

電子商務網站身分識別機制推廣計畫

防詐停看聽 網路購物安全指南

發 行 人：游瑞德
發行單位：經濟部商業司
地　　址：台北市中正區福州街15號
電　　話：(02) 2321-2200
網　　址：http://gcis.nat.gov.tw
執行單位：中華民國資訊軟體協會
出版日期：中華民國一〇二年七月

計畫網址：http://www.ec-security.org.tw

主辦單位：經濟部商業司

執行單位：CISA 中華民國資訊軟體協會 Information Service Industry Association of R.O.C.