2012

網路服務平台安全學習手冊

教育部全民資安素養推廣計畫

出版日期： 101/06/20

網路服務平台安全學習手冊

前言

全球上網趨勢

依據國際電信聯盟(International Telecommunications Union, ITU)在 2011 年 12 月所公布之世界 ICT 指標資料庫[4]，全球的上網人口數在 2010 年已經突破 20 億，在 2011 年甚至成長至 24 億，換言之，全球每一百位人口中，就有 35 個人可以上網。全球 20 多億的上網人口在網路上所從事的活動類型，或網友經常使用的網路服務平台種類，可從網站流量調查公司 Alexa 的統計結果來瞭解。表 1 為 Alexa 在 2012 年 5 月 15 日所公布的全球流量最大的前 20 名網站清單[1]。

表1. Alexa 全球流量最大的前 20 名網站

（統計日期：2012 年 5 月 15 日）

#	Alexa Global Top 20	#	Alexa Global Top 20
1	Google	11	Blogspot.com
2	Facebook (臉書)	12	LinkedIn
3	YouTube	13	Google India (Google 印度)
4	Yahoo!	14	Taobao.com (淘寶网)
5	Baidu.com (百度)	15	新浪新闻中心
6	Wikipedia (維基百科)	16	Yahoo! Japan (雅虎日本)
7	Windows Live	17	MSN
8	Twitter (推特)	18	WordPress.com
9	QQ.COM	19	t.co
10	Amazon.com	20	Google Deutschland (Google 德國)

資料來源：www.alexa.com，製表：NII 產業發展協進會

Contents

數字會說話

國內外上網相關統計調查很多，各調查機構因使用的統計方法不同，故即使相同的調查項目也可能產生不同的調查結果。然這些統計數據仍提供了參考依據，讓我們理解目前網路發展與應用的整體趨勢。

以臺灣的上網人口數為例，除本手冊引用的行政院研考會公布的調查數據外，其他經常被引用的類似統計還有：

- 資策會的「我國網際網路用戶數調查」[39]，依其於 2012 年 3 月所公布的數據，截至 2011 年 12 月底止，我國經常上網人口為 1,097 萬人。
- 臺灣網路資訊中心的「臺灣寬頻網路使用調查」[40]，依其於 2011 年 7 月所公布的數據，截至 2011 年 3 月 4 日為止，臺灣地區 12 歲以下民眾約有 156 萬人曾使用過網路；12 歲以上民眾有 1,539 萬人曾使用過網路；總計 0-100 歲之民眾有 1,695 萬人曾使用過網路。

在這些受到全球網路使用者歡迎的前 20 大網站中，有超過一半是與廣義的社群網站類型服務有關聯，例如 Google 的 Google+ 社群服務、全球最大社群網站 Facebook、在歐美較流行的 Twitter 與 LinkedIn 社群服務、強調分享功能的部落格服務 Blogspot 與 WordPress、影音分享平台 YouTube、提供即時通訊服務的 MSN 等。另外，此前 20 大清單中包含 7 個網站有提供電子郵件服務或傳訊服務的網站，如 Google、Yahoo!、Windows Live 等。

臺灣上網趨勢

依據行政院研究發展考核委員會所公布的「100 年個人/家戶數位機會調查報告」[25]，我國 12 歲以上民眾中有 72.0%曾使用過網路，換言之，我國 12 歲以上的網路使用人口約有 1,478 萬。

再檢視臺灣上網人口的網路服務應用特徵，以 Alexa 在 2012 年 5 月 15 日所公布針對臺灣流量最大的前 20 名網站[1]為依據，如下表 2 所列。

表2. Alexa 臺灣流量最大的前 20 名網站

（統計日期：2012 年 5 月 15 日）

#	Alexa TaiwanTop 20	#	Alexa Taiwan Top 20
1	Yahoo!	11	PC home 電腦報
2	Facebook (臉書)	12	Yam 天空
3	Google	13	Mobile01
4	Google 繁體中文搜尋	14	HiNet
5	YouTube	15	udn.com 聯合新聞網
6	無名小站	16	露天拍賣
7	伊莉心情車站	17	Blogspot.com
8	PIXNET 痞客邦	18	Wikipedia (維基百科)
9	巴哈姆特電玩資訊站	19	臺灣蘋果日報
10	Windows Live	20	Baidu.com (百度)

資料來源：www.alexa.com，製表：NII 產業發展協進會

此清單中有超過一半的網站為提供網友與網友間互動、交流、分享的社群網站類型之平台服務，Facebook 亦為最受臺灣網友歡迎的社群網站服務，其他包括 Yahoo!、Google、YouTube、無名小站、痞客邦、天空、Blogspot、Windows Live、PC home、以及討論區或論壇服務，如 Mobile01 等。

再參考行政院研究發展考核委員會的「100 年個人/家戶數位機會調查報告」[25]有關網路近用及使用情形的統計，在資訊搜尋方面，臺灣的網路族最常透過網路搜尋的前六大資料類型依序是新聞、娛樂、消費、工作相關、旅遊及股票財經，比率高於 5%的還包括社群網站、生活、課業相關及音樂等項目，圖 1 為臺灣網友上網經常使用的資料類型比重之示意。

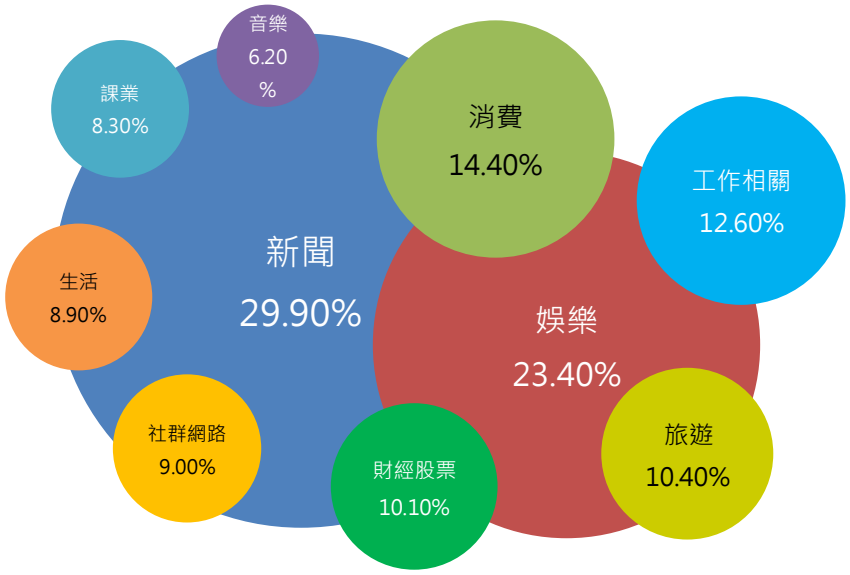


圖1.　臺灣網友上網經常使用的資料類型比重之示意

（資料來源：行政院研考會「100 年個人/家戶數位機會調查報告」；製圖：NII 產業發展協進會）

上述調查報告亦指出，網友使用比例最高的網路應用為收發 e-mail，其次是線上影片、線上音樂。其他使用率高於五成者有線上購物、線上傳訊、線上遊戲、網路社群、建置部落格等。

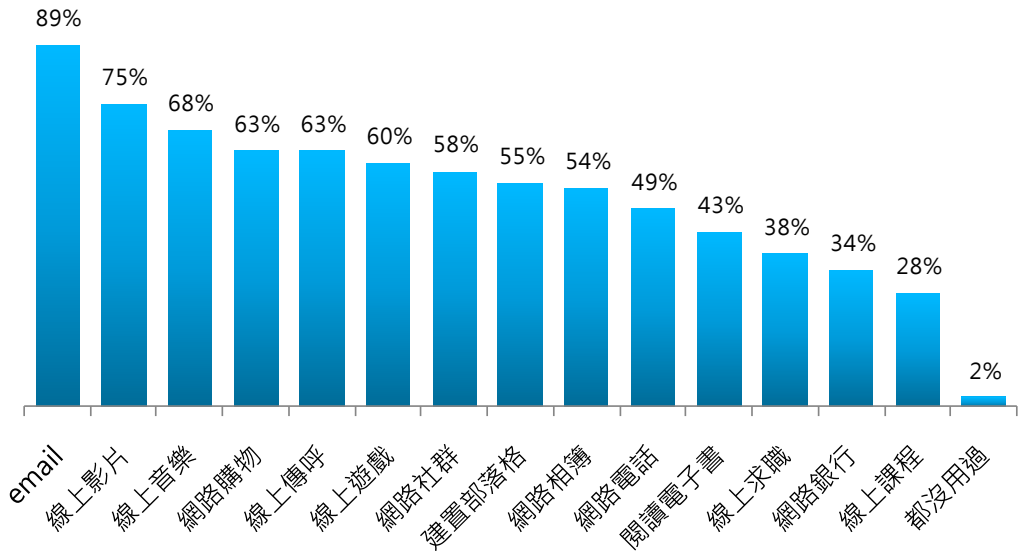


圖2.　臺灣網路使用者曾使用的網路應用功能

（資料來源：行政院研考會「100 年個人/家戶數位機會調查報告」；製圖：NII 產業發展協進會）

綜合前述有關全球與臺灣網路使用者的網路行為與趨勢，在包羅萬象的各式網路與應用當中，本學習手冊將以電子郵件及社群網站最常被使用的兩大服務平台為主題，除說明此兩大應用服務內容的特色之外，也將就民眾與網友在使用這些網路應用服務時可能會面對到的安全風險進行介紹，並就各項安全風險提出因應處理建議。

Source: 微軟 Microsoft 圖像資料庫 http://office.microsoft.com

主題 1. 電子郵件安全

電子郵件已是當今社會活動中相當普及的聯繫工具，根據美國市場調查公司 Radicati Group 今年 4 月份所公布的電子郵件統計調查報告[6]，全世界的電子郵件帳號數預計將從 2012 年的 33 億成長至 2016 年的 43 億。此外，市場上越來越多免費電子郵件服務的提供，無論是商務或政府應用、以及個人通訊用途，電子郵件是便利、迅速且成本低的通訊方式已是不爭的事實。

隨之而來的是電子郵件的安全威脅，例如電子郵件夾帶電腦病毒或木馬等惡意程式、垃圾郵件氾濫、網路詐騙活動、商業應用於傳輸重要文件的機密性管理等，已成為企業、政府機關、以及個人在相關應用上應關注與瞭解且不可忽視的課題。

主題 1 將分別從 ❶電子郵件威脅、❷電子郵件安全小撇步、以及 ❸防範垃圾郵件等三個次主題，談電子郵件之安全因應。

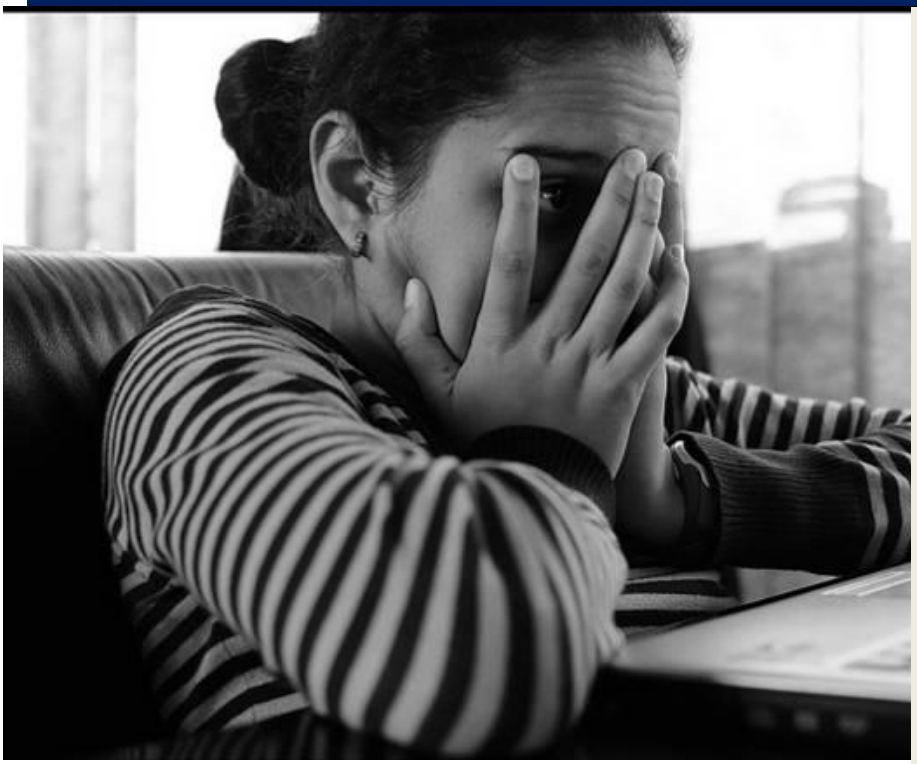
❶ 電子郵件威脅

本節將電子郵件的安全威脅分為以下三個類別，並將逐一說明其安全威脅之內涵。

❶-1 夾帶病毒及惡意程式

❶-2 社交工程

❶-3 垃圾郵件



❶-1 夾帶病毒及惡意程式

電子郵件是傳播電腦病毒、蠕蟲、木馬程式……等惡意內容的常見管道，若收件者不慎開啟夾帶有惡意程式的電子郵件，或由於系統漏洞造成電腦病毒的感染，不但有可能造成系統資料毀損，或成為殭屍電腦而任由駭客擺佈其電腦（例如利用中毒的電腦濫發垃圾郵件或更多的病毒郵件），也可能造成整個內部網路服務的癱瘓，部分電腦病毒甚至會關閉掃毒引擎，造成防毒功能失效等。

病毒郵件已演化到不須開啟附檔案，只要出現在郵件預覽窗格中，就有可能讓電腦感染到病毒，同時會自動運用通訊錄中的名單，再自動由該感染者寄送病毒郵件給通訊錄內的地址，加速病毒散播。

根據資安廠商賽門鐵克 2012 年 2 月份的安全情報報告(Symantec Intelligence Report: February 2012)[9]指出，全球電子郵件夾帶病毒率為 0.37%，換言之，每 274.0 封郵件當中，就有 1 封電子郵件是帶有病毒的。

資安素養 A to Z

- Malware（惡意軟體）

惡意軟體泛指一般未經使用者許可，擅自植入使用者電腦，且會對於電腦程式與檔案文件造成破壞與損傷的程式，通常惡意軟體是由駭客設計並且刻意散發，以造成他人電腦中毒或癱瘓。如電腦病毒、蠕蟲、特洛依木馬病毒、間諜程式與後門程式等，都是屬於惡意軟體的一種。

- Virus（電腦病毒）

電腦病毒是一種會自行複製且破壞電腦運作的程式，通常是在使用者下載網路軟體或使用已受感染的隨身碟或文件而遭受感染。

一旦感染，電腦病毒會在未經使用者同意之下，擅自改變電腦運作方式（如電腦無法開機、硬碟格式化、檔案容量變大……等）；電腦病毒具有自動破壞檔案系統與複製病毒主檔的特性，能透過已感染的主檔案複製相同的病毒並進而感染其他檔案。

資料來源：i-Security 網站
www.i-security.tw

❶-2 社交工程

所謂的社交工程(Social Engineering)是以運用擬真並極具吸引力的方式，來欺騙他人以獲得有用的資訊。夾帶病毒及惡意程式的電子郵件為吸引收件者開啟，則常會利用社交工程的方法，誘騙使用者開啟信件，並且讓受害的使用者不知不覺間再助長這些惡意程式繼續擴散。電子郵件社交工程類型主要分為「設計吸引收件者開啟郵件的主旨」、「偽裝寄件者」、「釣魚郵件」等三種。

類型 1. 設計吸引收件者開啟郵件的主旨

此類的電子郵件會誘發人們的好奇心，或是偽裝成來自合法組織、時下流行的話題等，讓收件者以為收到的是無害的電子郵件，但其實收到的是電腦病毒。

例如，今年全球與臺灣都流行的林來瘋，就在 3 月中美國職籃紐約尼克隊迎戰溜馬隊且連勝時，網路上出現一封叫做「NBA 超級新星林書豪，令人難以相信的故事」的 e-mail，裡頭暗藏惡意程式，只要打開該電子郵件，就會出現一個 WORD 附夾檔，一旦開啟該檔案，就會被植入針對微軟 office 弱點的木馬程式，該木馬程式會利用漏洞安裝後門程式，竊取使用者電腦內的重要資料[2]。

此類型的病毒還會透過其他熱門的新聞話題進行散播，例如今年 2 月份過世的惠妮休斯頓，也有人以「I Cried watching this video. RIP Whitney Houston（看著影片我哭了，哀悼惠妮休斯頓）」為主旨，將藏有惡意程式的超連結以影片連結的方式吸引網友點選。在 2011 年底，也發現了一封主旨為金正日死訊的郵件，打開附夾的 pdf 附檔後會顯示金正日的照片，暗中卻植入名為「TROJ_PIDIEF.EGQ」的惡意程式，為網路犯罪者開啟遠端遙控使用者電腦的大門。

夾帶病毒及惡意程式的電子郵件主旨，也會利用看似合理、或故意模仿為傳送一份給您的文件方式，來引誘收件者開啟附夾檔案。這一類看似無害的電子郵件標題舉例如下：

- 公文 09-881234567 號
- 週休二日的最好去處
- RE： 關於訂單出貨資訊
- 2012 年度招募計畫
- 宜蘭童玩節好好玩！
- 過年賞櫻秘境大公開

by Joffley (CC BY-NC-SA 2.0)
http://www.flickr.com/photos/joffley/

根據 Websense 安全實驗室所發布的 2012 最新威脅報告(Websense 2012 Threat Report) [13]顯示，排名前五大的電子郵件惡意誘餌為：訂單通知、票券確認、送貨通知、測試郵件、以及退稅資訊。

類型 2. 偽裝寄件者

駭客除了用信件主旨來吸引收件者開啟電子郵件外，也會假冒使用者所認識的人寄出郵件，讓使用者誤以為是可信任的對象所寄來的信件而相信該電子郵件的內容，進而去開啟這些附件或超連結，並啟動木馬程式。例如偽裝成朋友寄來的信件，標題為「我要結婚了」，並且附夾了「婚紗照.zip」的檔案，如下圖所示。

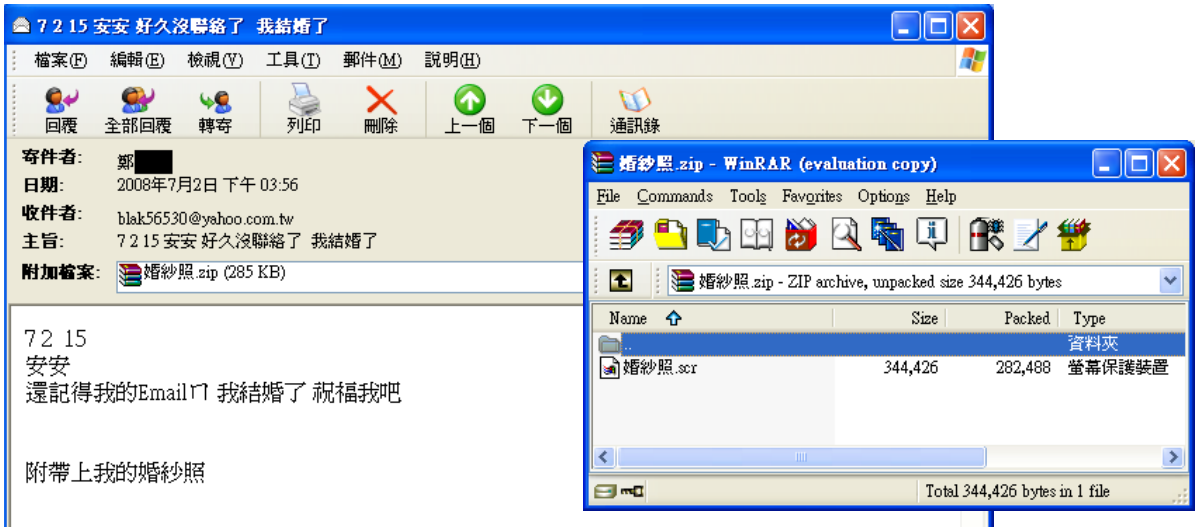


圖3. 偽裝寄件者之電子郵件圖示（製圖：NII 產業發展協進會）

2009 年自由時報曾報導，國內有一位大學講師接獲昔日論文指導教授的求助電子郵件，指導教授在信件中自稱人在國外因皮包遺失，要借 2,800 美元應急，該講師回信詢問要如何協助，冒牌教授隨即回信，還指定透過西聯匯款。一直到匯款完後才發現自己的指導教授根本都在國內，也沒有發求救信要求匯款，進而報警處理。

警方偵辦發現，被害人的指導教授幾天前曾接到一封冒充信箱管理員發出的確認帳號信件，他填寫帳號、密碼、身分證號碼並回信，不久就發現信箱一整天無法使用。警方研判發信的詐騙集團可能是先以駭客方式入侵被害人指導教授的 e-mail 通訊錄，再假冒其名義寄出借錢郵件[24]。

小專欄 – 電腦可能中毒之徵兆

- 電腦系統運行速度異常緩慢或當機頻率增加
- 異常的系統訊息通知
- 來自防毒軟體的警告訊息
- 電腦無故自動關機或不斷重新開機
- 螢幕顯示異常， 例如畫面突然一片空白
- 上網速度越來越遲緩，或網路速度時快時慢
- 網路流量異常，例如沒有使用網路服務或收發電子郵件， 但網路的連線燈號卻一直閃爍
- 瀏覽器自動出現產品廣告或色情網頁
- 沒有上網卻還是一直看見廣告視窗
- 上網瀏覽器的首頁被更改成奇怪的網站
- 瀏覽器多出沒有安裝過的工具列、搜尋工具，且無法移除

資料整理：NII 產業發展協進會

假冒寄件者方式可能透過假冒寄件者顯示名稱或直接透過假的電子郵件帳號方式。例如，駭客可能會設定自己的電子郵件顯示名稱為收件者朋友的姓名，但實際上並非朋友的電子郵件。例如，收信軟體或免費電子郵件都有提供使用者自行輸入寄件者顯示名稱（或寄信用名稱），有的人可能會輸入自己的英文名字或綽號，但惡意人士可能就會輸入其他隱藏自己身分的名稱，例如由其他管道得知您通訊錄裡朋友的名字，或輸入像是某銀行客服部等名稱，若不多加留意，可能會誤會該封電子郵件來自於自己所信任的對象。請參考下圖為寄件者自行輸入寄件者名稱，然後再寄出電子郵件給他人，收件者的信箱中所呈現的畫面。

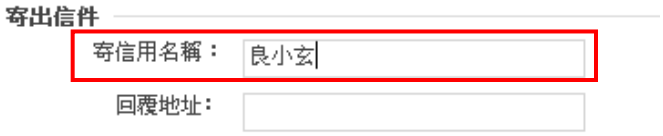


圖4.　以 web mail 界面自行輸入寄出信件之名稱範例

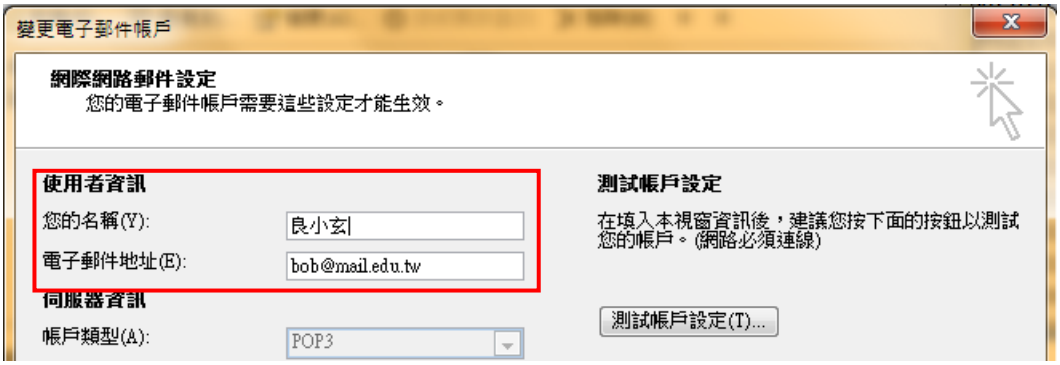


圖5.　以收信軟體提供之帳號變更界面自行輸入寄件者之名稱範例

圖6.　收件者收到用假寄件者名稱寄出的電子郵件範例

惡意人士也有可能透過假的電子郵件帳號寄信給您，為了混淆收件者的視覺及騙取其信任，其會利用並稍微變更大家所熟悉的電子郵件帳號，如下所示。請注意，以下為範例，並非真實的Y!拍賣電子郵件帳號：

Y!拍賣管理者的電子郵件帳號	auctions@yahoo-inc.com	假設此為官方帳號
假冒的 Y!拍賣管理者的電子郵件帳號	auctions@yahoo.com.tw	@後半段網址不正確
	auctions@yah00.com.tw	Yahoo 單字末兩個字母 oo 變成數字 00

類型 3. 釣魚郵件

釣魚郵件的常見模式為網路詐騙者發送帶有偽冒網站超連結的電子郵件，引誘不知情者前往該山寨版的網站並輸入自己的帳號與密碼，因為山寨版網站的外觀與實際的官方網站十分相像，也讓其有機會剽竊受騙者的帳號密碼。根據資安廠商賽門鐵克 2012 年 2 月份的安全情報報告(Symantec Intelligence Report: February 2012)[9]指出，全球每 358.1 封電子郵件中就有 1 封(0.28%)是帶有某種類型的釣魚攻擊郵件。

仿冒知名銀行或網站的釣魚郵件

網路釣魚所用的誘餌千奇百怪，在早期多是偽裝成為知名銀行或線上購物網站發出的釣魚信件進行詐騙，通知使用者資料過期、無效需要更新，或者是基於安全理由進行身分驗證，要求使用者重新確認銀行帳號密碼或信用卡號。只要使用者一時不察，經由電子郵件指引的網址連結到偽造得一模一樣的帳號登錄頁，個人的銀行帳號、密碼或信用卡等資料，馬上進入駭客的口袋。

2007 年時，在臺灣就發生了真實案例，當時有不肖集團以國內某大銀行的網站為樣本，製作與該銀行首頁一模一樣的網頁，並以該銀行名義發出數十萬封以「銀行系統轉換，重新登錄」為標題的電子郵件，要求銀行用戶點選郵件內的網址，上網重新確認帳號及個人密碼。當用戶連上該偽冒網站時，即被植入木馬，竊取個人密碼及信用卡資料；歹徒隨後更利用相關資料盜領存款、盜開支票，甚至複製信用卡詐欺取財。

另一個比較近期發生的案例是在去(2011)年底，南部某一位議員向警察局提出檢舉，表示他收到一份電子郵件，該電子郵件提供的超連結是連線到偽造的「XX 航空網路訂票網頁」。山寨版的「XX 航空網路訂票網頁」也使用了該航空公司的梅花標誌，但是標誌圖片呈現在網站上的位置跟真的網頁左右相反，字體大小也稍有差異，網頁背景的藍天白雲也都不見了；山寨版的網頁中也留有臺北辦事處的連絡電話。該議員因對該網頁外觀產生質疑，在與 165 反詐騙專線查證後，確定是「釣魚網頁」，而沒有被騙到個資[17]。

資安素養 A to Z

- Social Engineering
  （社交工程）

社交工程主要是利用人性的弱點而進行詐騙。社交工程是一種非技術性的入侵，是藉由與人透過社交手段進行犯罪行為。現代病毒已開始結合社交工程概念，例如"ILOVEYOU"病毒就是透過在電子郵件中以「我愛您」為附加檔案的檔名，誘導使用者打開附件，然而在使用者打開附件的同時，即被植入病毒，這就是利用社交工程入侵電腦的一個範例。

- Trojan Horses
  （特洛依木馬程式）

特洛依木馬程式是一種惡意程式，通常夾帶於電子郵件中或瀏覽網站時植入使用者的電腦，使用者電腦一旦被植入特洛依木馬程式，入侵者可以透過程式遠端遙控破壞電腦或竊取使用者電腦中的個人資料。

資料來源：i-Security 網站
www.i-security.tw

Source: 微軟 Microsoft 圖像資料庫
http://office.microsoft.com

仿冒社群網站服務或政府機關、政治人物的釣魚郵件

根據 Openfind 電子郵件威脅實驗室 2012 年第一季電子郵件威脅調查報告[44]，針對臺灣地區電子郵件威脅樣本的觀察，近年因為社群網站及電子交易平台的興起與流行，駭客會佯裝成這些知名社群網站，提供用戶資訊安全服務等訊息，待用戶進一步登錄自身的帳號及密碼後，再詐取個人機密資訊。防毒軟體公司賽門鐵克的最新調查報告也提出類似的結論，其提到針對社群媒體所形成的釣魚網站占整體網站的 4%，且集中在少數幾個知名社群網站。

除假冒知名的社群網站、電子商務網站外，也有假冒讓民眾容易鬆懈警覺心的政府單位發出的釣魚郵件，例如在今年 1 月中就發生了不明人士假借經建會名義廣發研討會邀請函，該封電子郵件主旨為「中華民國 101 年國家經濟建設與兩岸關係發展研討會」，內文並註明主辦單位為行政院經濟建設委員會，協辦單位為行政院大陸委員會，並有附檔。經建會查證後表示該邀請函應是釣魚郵件，並提醒民眾不要開啟附檔[16]。

2011 年的總統大選期間，總統參選人蔡英文女士也特別公告有駭客假冒小英部落格名義，寄發釣魚信件，該封信件的主旨為「蔡主席的博客全新改版」，寄件者為 KWCH，信件內容為「謝謝大家對小英的故事長期閱讀，近期關於蔡英文的訊息，請大家前往 www.wretch.cc/blog/ingw...」；若不慎點進釣魚網頁，電子信箱的帳號和密碼都會被盜取[18]。

釣魚郵件除了可能會誘騙不知情者前往假造的網站，部分的假造網站甚至會在網頁中暗藏木馬程式，縱使受騙者具有高度警戒心，未被騙取帳號密碼，但只要瀏覽該網頁，即會讓瀏覽過的電腦被植入木馬程式而成為殭屍電腦，被駭客冒充其名義散布垃圾郵件，或作為發送垃圾郵件、攻擊郵件、病毒郵件等的跳板。

資安素養 A to Z

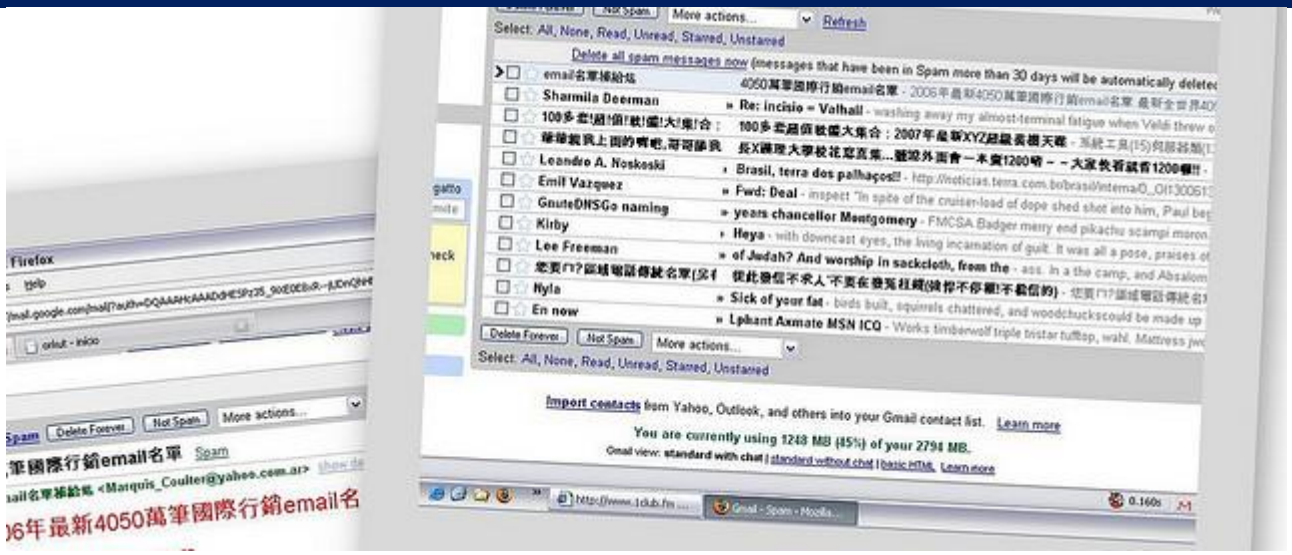
- Worm（蠕蟲）

蠕蟲是電腦病毒的一種，同樣具有自行複製散播的能力。蠕蟲病毒能自行複製許多相同的病毒碼，並且在使用者尚未發現時，即自行發送蠕蟲病毒，受感染的程式碼能自行在網路間流竄，更進一步感染在同一區域網絡的他人電腦。蠕蟲因為在網路間自行複製發送的特性，容易造成電腦資源的耗損，以致電腦速度變慢與網路癱瘓。

- Zombie Networks（殭屍網路）

「殭屍網路」指的是遭受駭客透過系統漏洞或後門植入遙控程式的殭屍電腦所組成之網路系統。植入遙控程式的電腦會喪失自治能力，換言之，被植入遙控程式的電腦會受到駭客的遙控，進行任何駭客指定的工作而無法自行控制，就好像聽從指令般。殭屍網路裡的電腦通常被用於進行網路詐騙、垃圾郵件濫發、傳播病毒等不法用途。

資料來源：i-Security 網站
www.i-security.tw



by Daniel F. Pigatto (CC BY-NC-ND 2.0)
http://www.flickr.com/photos/pigatto/

❶-3 垃圾郵件

一般民眾打開電子郵件信箱時，都有收到垃圾郵件的經驗；所謂的「垃圾郵件」是指未經受信者同意而寄送到電子信箱裡的信件，也有人稱之為廣告信、大宗郵件。這些垃圾郵件的內容大多是商品廣告，例如：藥品、情色、美容、快速賺錢、愛心募款、低利息貸款等誇大訊息居多。

根據資安廠商賽門鐵克 2012 年 2 月份的安全情報報告(Symantec Intelligence Report: February 2012)指出[9]，至 2 月份為止，全球每 1.47 封郵件中就有 1 封是垃圾郵件，雖然垃圾郵件數量發展之趨勢持續下降，但這並不表示網路罪犯在放棄垃圾郵件攻擊，這些駭客只是把重點放在設計出危險性更高的垃圾郵件。

參考 Commtouch 2012 年第一季網路威脅趨勢報告[45]，全球平均每日有 94 億封垃圾郵件與釣魚信件，而平均每日有 27 萬台殭屍電腦在發垃圾郵件，和 2011 年的第四季比較，成長了將近 30%。該報告中也列出全球熱門的垃圾郵件標題種類，分別為藥品廣告、販賣贗品、以及情趣產品等三種。

對於一般電子郵件使用者而言，垃圾郵件帶來的困擾包括：垃圾郵件灌爆信箱影響正常信件收發；收信匣中垃圾郵件氾濫，不容易找到想要的信；浪費時間刪除垃圾郵件，而且可能在刪信的過程中不小心刪掉重要信件；以及透過廣發垃圾郵件進行網路釣魚和散布電腦病毒、木馬程式等惡意軟體……等。

垃圾郵件的氾濫對企業的網路管理者而言，更是一個頭疼的問題，不但會造成郵件伺服器處理大量信件而癱瘓，未進行防範設定的郵件伺服器也可能被駭客用來當作跳板代發垃圾郵件，不但會防礙企業郵件服務正常的傳輸，甚至會使企業郵件伺服器被列入垃圾郵件寄送者黑名單。其他的問題還包括：網路阻塞、浪費頻寬、影響員工生產力、隱藏病毒資安危機……等。

❷ 電子郵件安全小撇步

因應各式各樣的電子郵件威脅，防範因不當使用 e-mail 而受到惡意程式、病毒攻擊或個資外洩，本節將說明在使用電子郵件時的基本認知與防範措施的內涵，提供民眾可操作的 7 個小撇步，包括：❷-1 安裝防毒軟體，不安裝來源不明的軟體、❷-2 更新軟體修補程式、❷-3 不要啟用郵件的預覽窗格、❷-4 謹慎開啟電子郵件的附夾檔案、❷-5 辨識釣魚郵件五大重點、❷-6 寄出郵件前再次檢查收件者的正確性、以及❷-7 注意隱私。

❷-1 安裝防毒軟體，不安裝來源不明的軟體

電腦安裝防毒軟體為最基本的病毒防護措施，除安裝防毒軟體外，並應下載及使用最新的病毒碼。因為病毒的種類及型態一直在改變，新病毒也每天不斷地被產生，如果不經常更換最新的病毒碼，再強悍的防毒軟體也會有失靈的一天。

通常防毒軟體會定期自動幫您檢查是否有更新，並在您的電腦連上網際網路時進行最新病毒碼的更新。若您在安裝防毒軟體時選擇「手動更新」或其他非自動更新的選項，或者您已經很久一段時間沒有使用電腦或不確定是否防毒軟體有進行更新時，仍可透過以下步驟來瞭解狀態。以下以賽門鐵克防毒軟體為例，提供使用者如何知道自己的防毒軟體的病毒碼狀態，以及如何進行病毒碼的更新。請注意，不同的防毒軟體可能在步驟與呈現文字方面稍有差異，若仍不清楚自己的防毒軟體是否正常運作，建議詳細閱讀您的防毒軟體廠商所提供的操作者或使用者手冊之說明。

當開啟防毒軟體，可檢視防毒軟體的「狀態」，通常在「狀態」的說明中會清楚呈現您的防毒軟體的安全相關定義檔的更新日期，若這些日期為今天的日期，或只有 1-2 天的差距，那麼您的防毒軟體的病毒檔更新狀況為最新。若您的病毒檔更新日期超過 3 天以上，建議您可用手動方式來進行病毒碼之更新。更新病毒碼時，請確認您的電腦是處於連網狀態的。

以賽門鐵克的防毒軟體為例，其軟體開啟後可清楚看到病毒定義檔的日期，其手動更新是以「LiveUpdate」這幾個字來呈現，按下此按鈕後，軟體便會開始更新病毒碼。

以趨勢科技的防毒軟體 PC-Cillin 2012 為例，其軟體開啟後的頁面最上方會直接呈現您的防毒軟體更新狀態，正常情況下應呈現「您已取得最新的防護」或類似的文字說明。

以小紅傘防毒軟體(Avira)為例，在開啟小紅傘控制中心後，畫面中會出現「上次更新」之日期，並以紅色 X 符號之圖示提醒使用者應該要進行更新。

以卡巴斯基防毒軟體 (Kaspersky Anti-Virus)為例，在開啟軟體主控台後，點選左邊視窗的更新中心，並點選開始更新。

❷-2 更新軟體修補程式

電腦系統與軟體通常在推出後，軟體開發業者會根據使用者所反映的意見，針對軟體的功能、效能、系統安全漏洞或錯誤等進行加強與修正，然後推出更新的軟體版本；也因此，當我們的電腦安裝軟體一段時間後，軟體開發廠商可能就會通知使用者有更新的軟體版本出現，請消費者進行版本的更新或安裝修補程式。通常，軟體在進行更新之後在運作上會更為順暢，或者因為新功能的強化，使軟體變得更為好用。

病毒等惡意程式之所以能夠破壞使用者電腦，是因為電腦軟體的系統漏洞讓這些惡意程式有機可乘，也因此保持電腦重要軟體與系統的最新狀態，亦即進行軟體修補程式的更新，有助於保持電腦安全。接續以常見問與答的方式來說明更新修補程式的注意事項。

問題：我要如何知道我目前使用軟體的版本？

回答：以網頁瀏覽器 Mozilla Firefox 為例，打開瀏覽器後，選擇工具列上的「說明」，再選擇「關於 Firefox」，接著就會出現關於 Firefox 的新視窗，視窗中會提供您的電腦所安裝的 Firefox 軟體目前的版次為何。如下圖所示。

圖7.　如何知道軟體版本 – 以 Firefox 為例（製圖：NII 產業發展協進會）

大部分的軟體說明其版本資訊的所在位置都差不多，再以另一種常見的 IE 瀏覽器為例，與尋找 Firefox 版本資訊的步驟幾乎一致，只是版本說明呈現的畫面稍有不同而已。

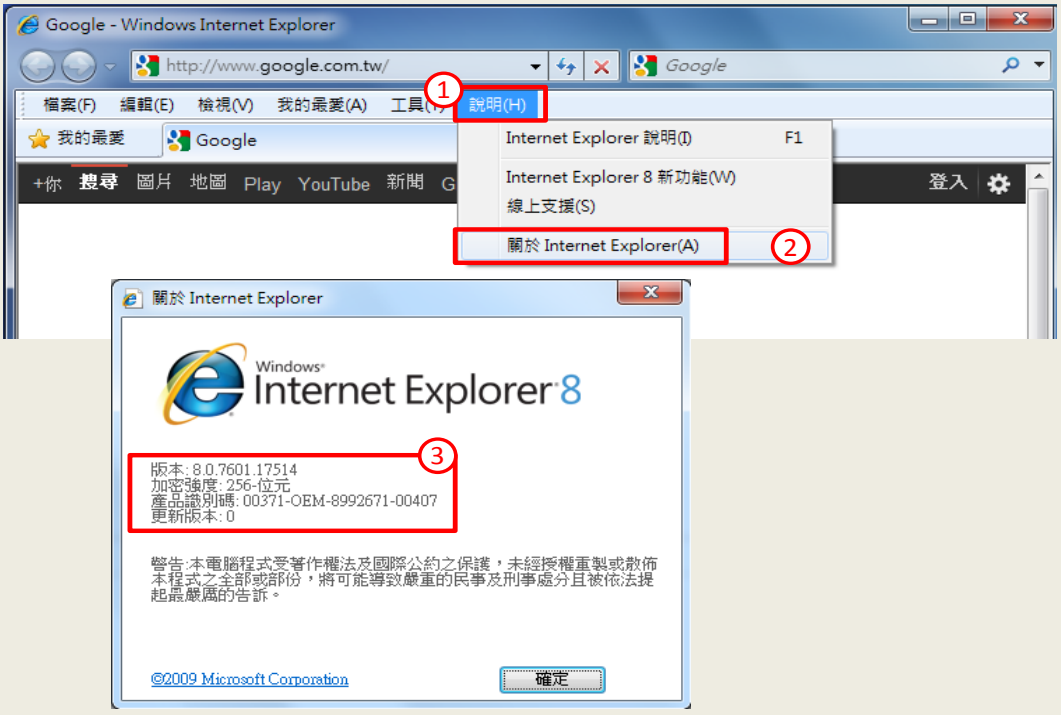


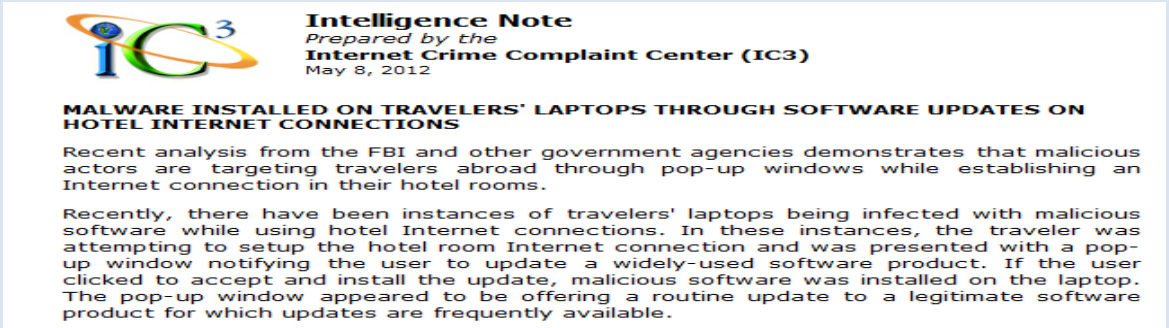
圖8. 如何知道軟體版本 – 以 Internet Explorer 為例（製圖：NII 產業發展協進會）

資安小專欄

軟體更新也有假冒的！

今年 5 月中，美國聯邦調查局(FBI)在網路犯罪投訴中心（IC3, Internet Crime Complaint Center）網站上發出警告，提醒海外差旅人士特別注意近期多筆在旅館內因假冒的軟體更新而遭感染的案例。在這些案例中，使用者在旅館內準備設定網路連線時，螢幕會跳出看似正常的軟體更新要求，當使用者按下「確定」鍵後，其電腦也因此被安裝了惡意程式。

參考資料：iThome, FBI 警告：飯店上網小心中毒, 2012.5.11



Intelligence Note
Prepared by the
Internet Crime Complaint Center (IC3)
May 8, 2012

MALWARE INSTALLED ON TRAVELERS' LAPTOPS THROUGH SOFTWARE UPDATES ON HOTEL INTERNET CONNECTIONS

Recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while establishing an Internet connection in their hotel rooms.

Recently, there have been instances of travelers' laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to setup the hotel room Internet connection and was presented with a pop-up window notifying the user to update a widely-used software product. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available.

圖像來源: Internet Crime Complaint Center

問題：我要如何知道軟體需要更新？

回答：以 Acrobat 的 Adobe Reader 軟體為例，若想了解該軟體版本是否需要更新，可在開啟軟體後，選擇「說明」並點選「檢查更新」後，得知目前是否有更新版本需要下載，如下圖。

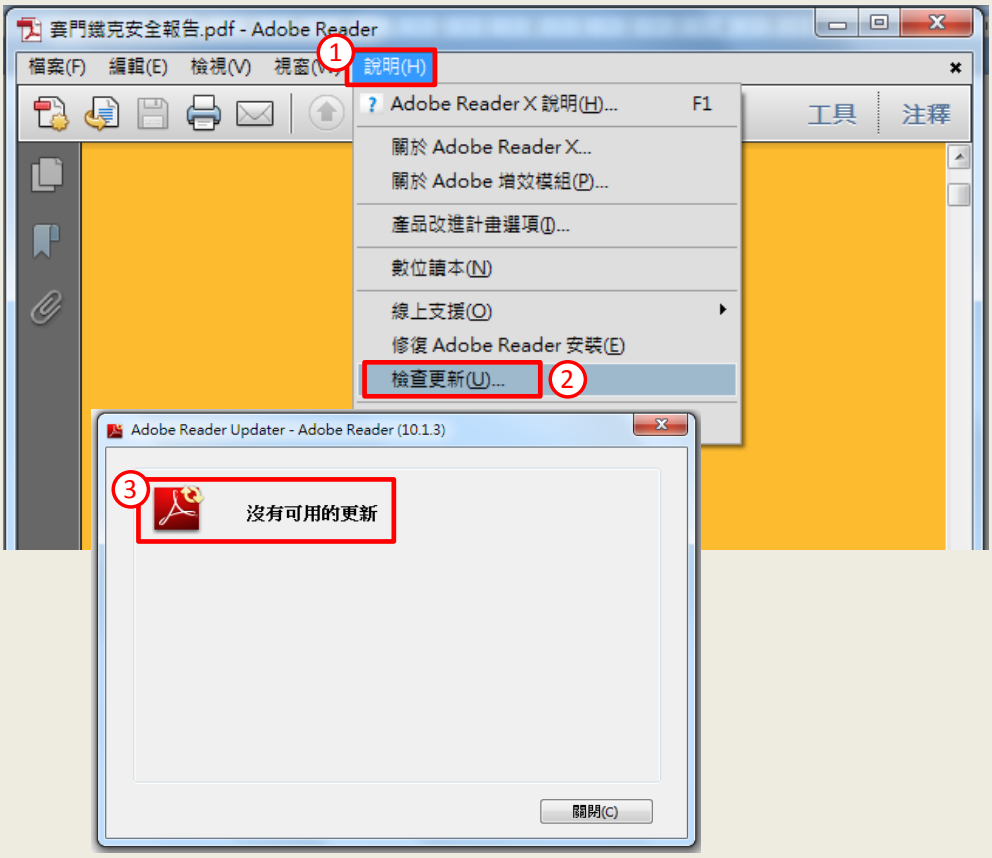
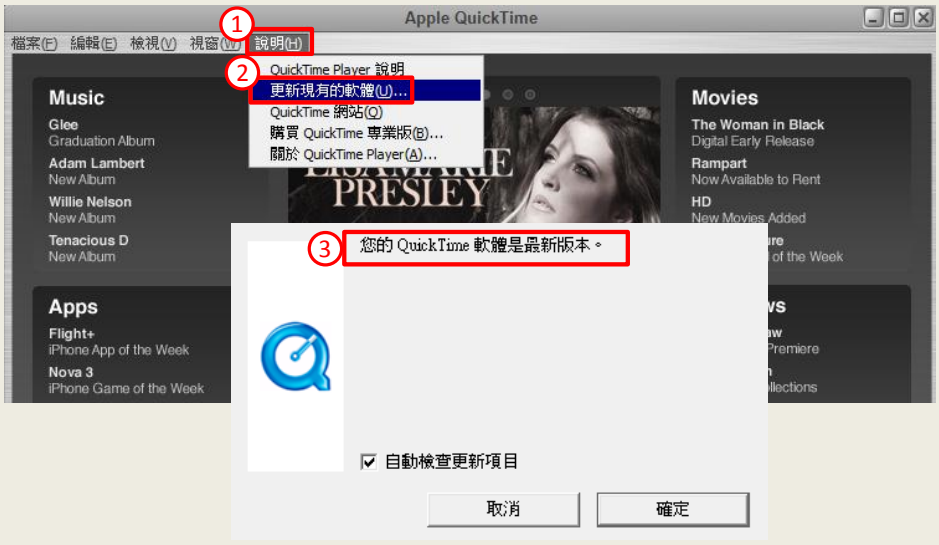


圖9. 如何知道軟體需要更新 – 以 Adobe Reader 為例（製圖：NII 產業發展協進會）

大部分具規模的軟體都會提供類似的軟體更新檢查功能，而瞭解軟體是否需要更新的步驟也都差不多，再以 Apple 的影音播放軟體 Quick Time 為例，其檢查軟體更新的步驟說明如下圖。



問題：如何設定微軟的系統自動更新？

回答：一般而言，軟體的更新方式有很多種，有線上更新、下載更新軟體等方式；為便利使用者對重要更新訊息的掌握，許多軟體會提供所謂的「自動更新」功能，讓使用者不必擔心遺漏了重要的軟體更新訊息。以大家常用的微軟作業系統為例，微軟提供了自動更新功能，使用者就不必自行到網站上搜尋是否有系統更新的需求，也不必擔心電腦遺漏 Windows 作業系統的重大更新，只要設訂妥 Windows Update，作業系統會自動為電腦檢查最新的更新。即使一開始安裝作業系統時沒有開啟自動更新的選項，使用者仍然可以隨時開啟。

若您的電腦採用的是 Windows 7 作業系統，參考微軟官方網站所提供的 Windows 7 說明和使用方法中有關「開啟或關閉自動更新」的說明，依循以下步驟可開啟或關閉您的作業系統有關自動更新的功能：

(1) 請按電腦螢幕左下角的 [開始] 按鈕。

(2) 在搜尋方塊中，輸入 Update，然後在結果清單中按一下[Windows Update]。

(3) 在左窗格中，按一下[變更設定]。

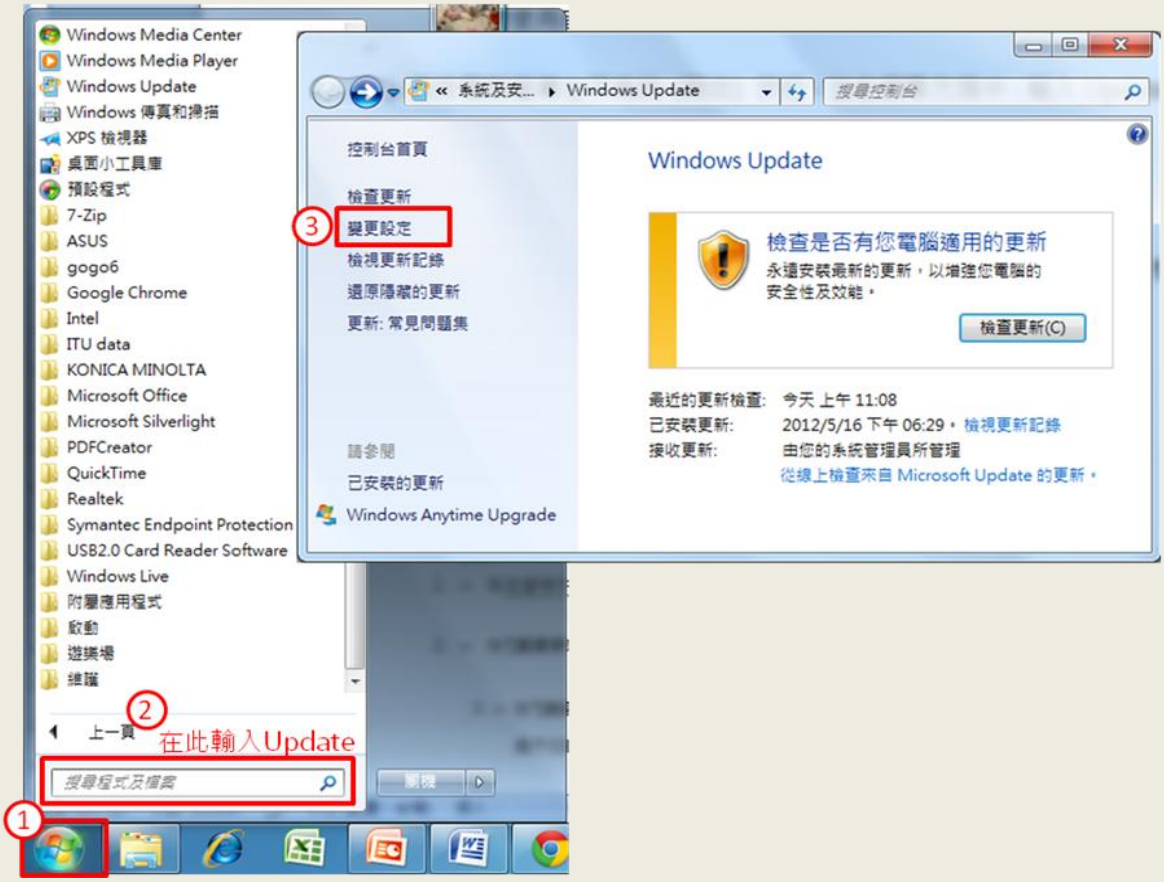


圖10.　開啟或關閉 Windows 7 作業系統自動更新的功能圖示一

(圖像來源：Windows 7 作業系統 / 製圖：NII 產業發展協進會)

(4) 在 [重要更新] 之下，選擇所要的選項；在 [建議的更新] 之下，選取 [提供建議更新與接收重要更新的方式相同] 核取方塊，然後按一下 [確定]。

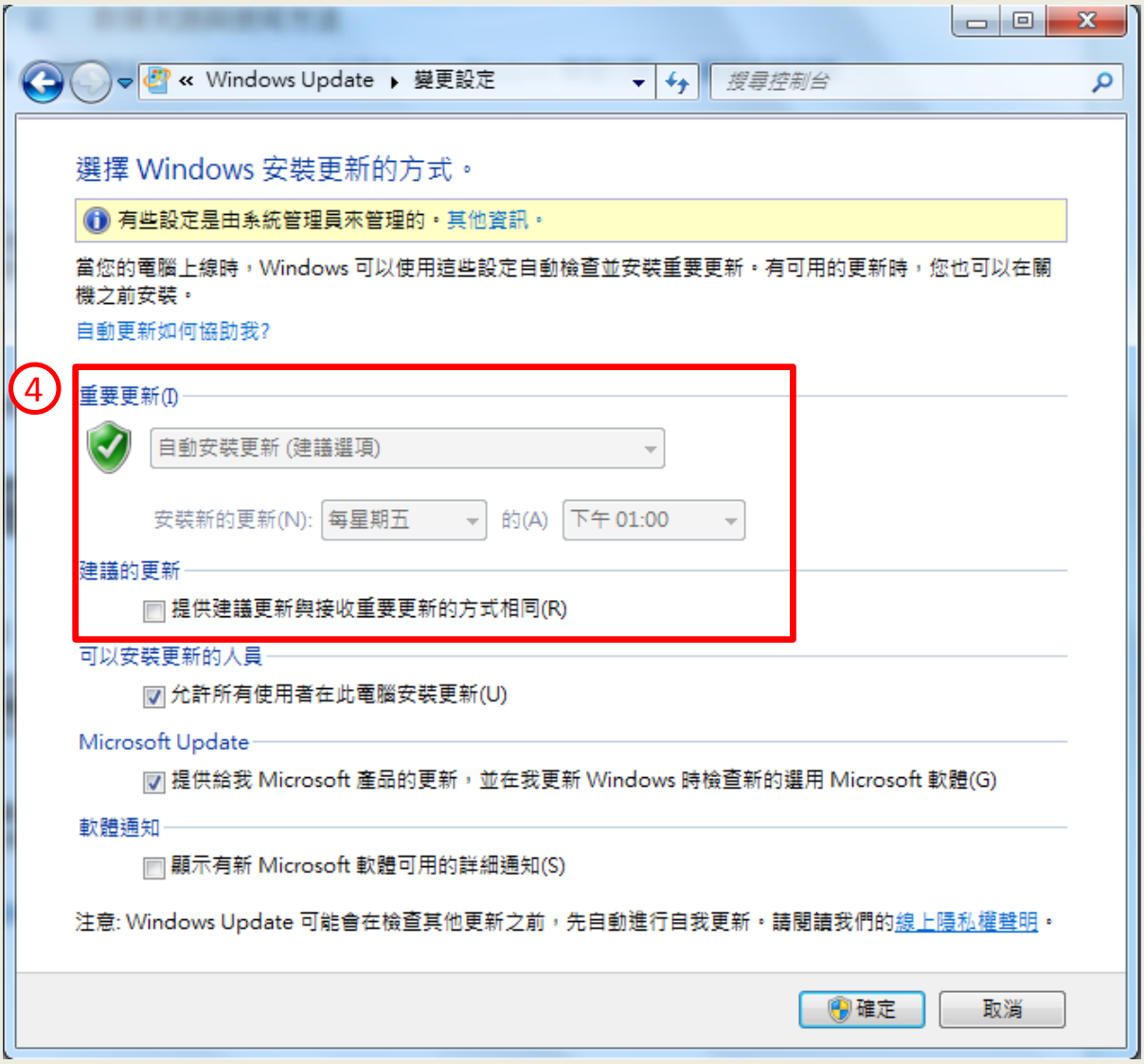


圖11.　開啟或關閉 Windows 7 作業系統自動更新的功能圖示二

(圖像來源：Windows 7 作業系統 / 製圖：NII 產業發展協進會)

❷-3 不要啟用郵件的預覽窗格

若您使用像是 Outlook 或 Windows Live 等收信軟體來收發您的電子郵件，建議將讀信模式調整為「整頁模式」或「關閉讀取窗格」。在非關閉讀取窗格的的讀信模式中，例如信件內容在郵件清單底端或右方出現，使用者在進入信件匣時，系統會自動開啟最新的信件（如下圖紅框處），這樣很有可能會直接誤觸病毒信件，故在資安考量下，將讀信模式設為整頁模式或關閉讀取窗格，可確保所有未讀取信件都呈現未開啟的狀態，避免因預設開啟而誤觸病毒信件。以微軟的 Windows Live Mail 為例，選擇工具列的「檢視」，並選取「讀取窗格」、「關閉」即可。

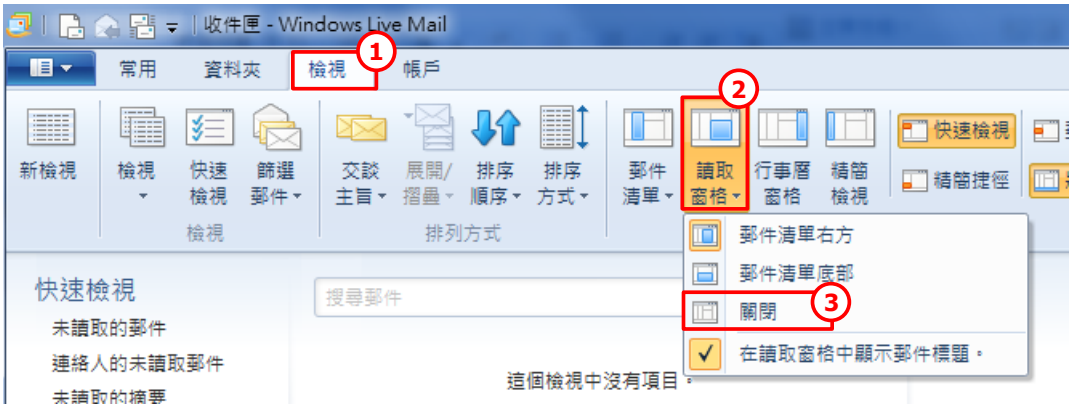


圖12. 如何關閉 Windows Live Mail 的讀取窗格（製圖：NII 產業發展協進會）

部分的 Web-based 電子郵件服務也提供關閉預覽窗格的功能，以雅虎奇摩電子郵件為例，如下圖所示，選擇「不分頁顯示：使用捲軸瀏覽信件（隱藏預覽窗格）」之選項即可。

圖13. 如何關閉雅虎奇摩電子郵件的讀取窗格（製圖：NII 產業發展協進會）

❷-4 謹慎開啟電子郵件的附夾檔案

夾帶病毒檔案的電子郵件通常都會使用特別的標題吸引人閱讀，因此遇到特別的信件主旨，千萬不要因一時好奇而開啟；就算是熟人寄來的信件附檔也不要貿然打開，若有任何懷疑，請直接與寄件者聯絡確認後再決定開啟檔案與否。如何辨識哪些電子郵件主旨可能有問題，以及讀到哪些郵件內容必須產生質疑，請參閱第❷-5 點有關「辨識釣魚郵件五大重點」之說明。

❷-5 辨識釣魚郵件五大重點

所有的網路使用者都應該了解什麼是釣魚郵件，有時候這些郵件確實難以辨識，但通常這些釣魚郵件都會要求使用者點選一個連結網址，引領至一個假造網站，然後再要求您提供、更新或確認機密的個人資料。以下彙整了辨識可疑釣魚郵件之五大重點：

重點 1. 觀察信件主旨

有心人士的詐騙或釣魚電子郵件最常使用引人感興趣的電子郵件主旨，來吸引及誘騙收信人開啟郵件，當收到以下類型的電子信件主旨時，不要因為一時好奇，就馬上開啟郵件或附夾檔案，請謹慎思考該封信件的真實性。

(1) 當下流行或熱門的話題，例如：林書豪限量球衣拍賣、女神卡卡演唱會門票、劉德華女兒相片曝光、前往倫敦看奧運、王建民重返洋基隊……等。
(2) 服務或系統管理者通知信，例如：電子郵件系統更新、臉書帳號停權通知、網路銀行密碼確認、即時通系統管理員通知、您的訂單出貨通知、退稅通知……等。
(3) 生活資訊分享，例如：賞櫻秘境大公開、節稅小撇步、好康優惠、實用軟體免費下載、如何提高中獎機率……等。
(4) 色情影音下載，例如：網站直接觀賞成人電影、露點聊天室、全亞最大情趣用品……等。
(5) 政治話題，例如：藍綠立委選舉登記、加入候選人粉絲團、選舉買票舞弊揭密……等。

重點 2. 檢視信件內的超連結

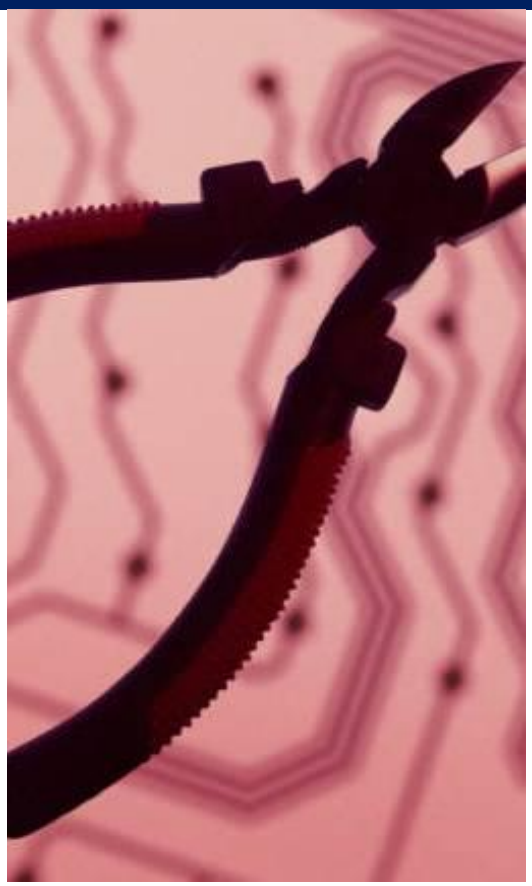
當您覺得某一封電子郵件很可疑時，請特別注意該信件中所包含的超連結網址，檢視方式為，不要立即點選該超連結，而是將您的電腦滑鼠移至該超連結的上方，且注意不要點擊，稍微等候幾秒鐘後，您的郵件視窗下方會出現該超連結真正會連往的網址，此時請確認超連結的網址是否和顯示的文字一樣，如果發現不一致，很可能是釣魚郵件，請勿點選該連結，並立即刪除該信件。

圖14. 釣魚郵件檢視信件超連結之圖示（製圖：NII 產業發展協進會）

重點 3. 信件內文以索取您的個人資料為重點，並包含威脅文字

網路犯罪者為達到其目的，會在釣魚郵件中製造出讓您緊張與受到威脅的氣氛，因為收件者可能在緊張的情緒下更容易點選可疑網站的超連結。此外，釣魚郵件也會要求您提供個人姓名、生日、身分證字號、ATM 密碼或預借現金密碼、信用卡有效日期、網路銀行的帳號與密碼，或其他相關的個人資料，這樣的郵件八九不離十是屬於詐騙信件。

常見的製造緊張或威脅氣氛的手法舉例如下，若您收到類似文字的電子郵件時，請多加留意其真實性，不要直接回覆該電子郵件或點選內含的超連結，並利用其他方式直接向您的服務業者或寄件者確認其真實性後再予以處理，例如：撥打客服專線、直接從官網搜尋相關資訊、查詢警政署 165 詐騙專線……等。



Source: 微軟 Microsoft 圖像資料庫
http://office.microsoft.com

製造緊張之釣魚郵件範例 1（資料來源：台灣 Visa [47]）

寄件者：Visa Service xxxxxx@visa-security.com
收件人：xxxxxx@morabits.com.
主旨：Visa 客戶安全資料更新

親愛的先生/女士：

我們接獲銀行的通知，表示您的信用卡也許在您進行網路購物的時候，個人帳戶資料（含信用卡號碼）外洩，並遭人竊取或盜用。為了協助補償您的損失，以及防止這類詐騙事件或帳號錯誤情況再度發生，我們建議您進入我們的網站，將安全表格填妥後回傳，並申請我們的免費「零風險方案」，這將能協助我們確認此案件的真實性，以作更深入的調查。

Visa 支援部助理 Alwin Desagun 敬啟

製造緊張之釣魚郵件範例 2（資料來源：台灣 Visa [47]）

寄件者：Visa Service xxxxxx@visa-security.com

收件人：xxxxxx@morabits.com

主旨：重要客戶通知

親愛的 Visa 客戶您好：

由於我們的系統發生嚴重錯誤，導致客戶資料遺失，為避免您的信用卡發生故障而無法使用，請填妥下列連結的認證表格，以協助我們盡速解決此問題。我謹代表 Visa 國際組織，向您致上最高的歉意。請點選以下連結，以重新驗證您的 Visa 信用卡，避免您的財務損失。

http://www.vissa.com/credit_card/verify.html

Visa 國際組織信用卡部門 敬啟

製造緊張之釣魚郵件範例 3

寄件者：電子計算機中心

收件人：xxxxxx@mccc.edu.tw

主旨：電子郵件系統更新

各位 XX 大學的同學，

因本校電子郵件系統已改版，請立即更新您的電子郵件帳號之密碼，否則您的電子郵件帳戶將無法再繼續使用。請點選此連結以進行更新。

XX 大學電子計算機中心 系統組 敬啟

製造緊張之釣魚郵件範例 4

寄件者：X 拍賣管理者

收件人：xxxxxx@yohooooo.com.tw

主旨：您的帳戶可能被盜用

親愛的會員，您好，

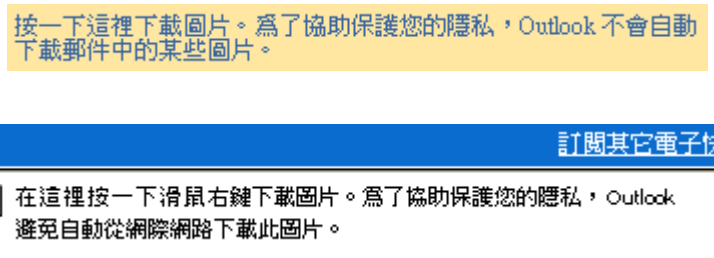
我們察覺您的網拍帳號資料可能被冒用於詐騙用途，須請您進一步提供您的其他身分證明資訊以進行更新與確認帳號之真實性，若您未更新資料，本公司將刪除此帳號。為避免您的帳號被停權，請透過下列連結確認您的資料。

X 拍賣管理者 敬啟

重點 4. 信件從知名的組織或公司寄出

釣魚郵件經常會冒用知名公司或政府機構的名義寄出，其郵件外觀設計上可能會引用這些知名公司、機構或品牌網站上的 Logo 圖片，讓收信者不留意之際，會以為是從官方網站寄來的信件。目前大部分的電子郵件收信軟體或 web 介面的電子郵件服務，在您開啟郵件時，都預設了不下載電子郵件中圖片的功能，讓您收到信件時，不會立即看到這些可能混淆您視覺的圖片，或因為疏忽誤點選了含有惡意程式的超連結。大部分正派經營的大規模網路公司或銀行，都不會以電子郵件的方式通知用戶須提供帳號密碼或其他個人資料（如身分證號碼、生日…等）。

以微軟 Outlook 為例，在封鎖郵件中的自動圖片下載時，郵件上方資料列會通知您正在執行封鎖動作(如下圖)，郵件中顯示已封鎖之圖片區域會取代為紅色的 X 預留位置，並顯示說明性文字。



重點 5. 注意郵件提供者的警示標語

許多 web mail 服務會自動篩選掉具有安全疑慮的電子郵件，不過這些服務為避免誤刪除您的重要電子郵件，通常會將這些可疑的電子郵件歸類在「垃圾郵件」資料夾中，由使用者自行進行刪除。在您檢查或確認歸類在垃圾郵件資料夾中的電子郵件時，可能會發現服務業者特別在某些電子郵件中標示警告標語（如下圖），建議您看到此類郵件時，立即予以刪除。

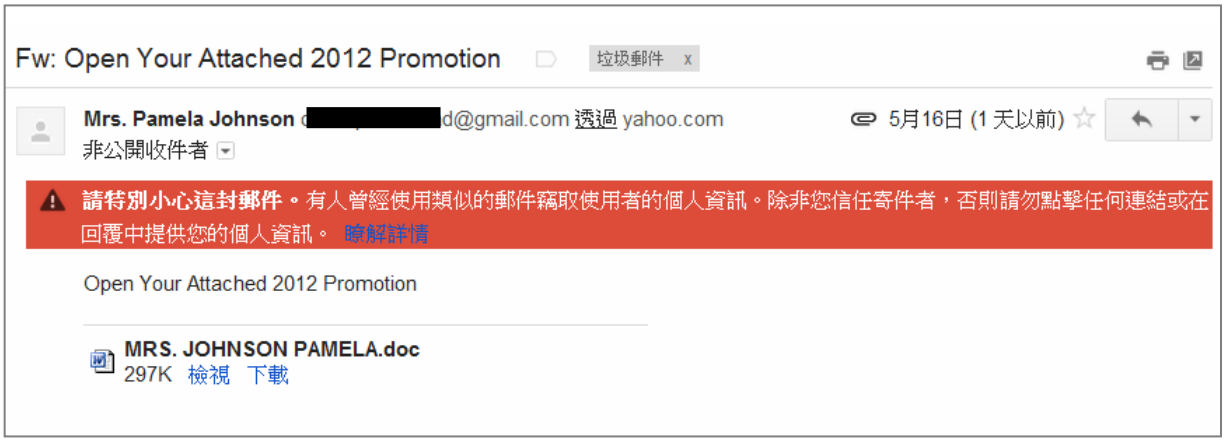


圖15.　Gmail 電子郵件中標示警告標語圖例（製圖：NII 產業發展協進會）

若您使用的是如 Outlook 收信軟體，則可透過防毒軟體掃瞄附檔是否含有病毒；關於郵件內容篩選部分，則可透過 Windows 更新時，自動下載篩選垃圾郵件的更新檔，Outlook 會依垃圾郵件篩選器，將可疑郵件丟到其「垃圾郵件」資料夾下。因此建議使用收信軟體的使用者，應確實執行防毒軟體與 windows 的更新動作。

❷-6 寄出郵件前再次檢查收件者的正確性

當寄送電子郵件給朋友或同事，在輸入其 e-mail 地址時，大多數的郵件收發軟體、甚至是 web 界面的網路郵件服務，都提供了便利的 e-mail 自動補全功能，亦即，您不必記住所有朋友或同事的 e-mail 帳號，只要輸入收件者的姓名或 e-mail 部分文字，郵件軟體會自動為您選擇相似姓名的郵寄地址。

自動補全功能在處理相似名字時會出現問題。例如，您可能想寄信給您的同事 William Huang，但自動補全功能可能幫您選擇了前一個任職公司的主管 William Chang，若在信件寄出前沒有再仔細檢查一次收件者是否正確，可能會將公司的重要或敏感資訊寄送給不相關的對象。

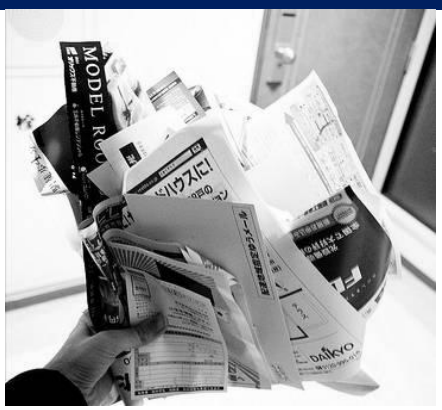
❷-7 注意隱私

若您非常重視隱私資訊，可能就必須考慮此類隱私資訊透過電子郵件發送是否合適，因為電子郵件的隱私非常不容易保護，不像是電話或面對面的交談，一旦您將隱私資訊透過電子郵件方式發出後，後續控制信件再向外傳播的困難度相對高，因為電子郵件可以非常輕易地轉寄給其他人，或者直接剪貼內文張貼在網路其他公開處，例如討論區或論壇上，並且這些資訊一旦公開在網站上，便很有可能會永久留存在網際網路上，即使後續再多的刪除補救，都不容易真正地刪除所有資訊。

此外，若同時寄送電子郵件給多位收件者，特別是這些收件者彼此並不認識或無關聯時，例如，公司欲寄送最新產品資訊給過去一個月曾經下單採購產品的客戶時，或者個人要寄送結婚喜宴通知訊息給一群親朋好友時，這群客戶或親朋好友彼此並無業務往來或彼此不認識，在這樣的狀況下，為保護每位收件者的個人資料，建議善用收件者列為密件副本的功能（如圖 16）。

圖16.　密件副本圖示（畫面來源：Gmail / 製圖：NII 產業發展協進會）

❸ 防範垃圾郵件



by xsix (CC BY-NC-SA 2.0)
http://www.flickr.com/photos/xsix/

電子郵件對於網路使用者而言，是一種快速又方便的資訊取得來源，對企業而言，也是取代傳真、郵寄等傳統通訊方式的行銷管道；但是，許多企業試圖以數取勝，可能每天寄送多次產品資訊給客戶，這樣的寄送頻率常常超越了合理範圍，猶如疲勞轟炸般，讓客戶無從分辨何者為優、何者為劣，久而久之只有「刪除全部」一途，使得這些郵件均成為垃圾郵件。

像是每年 5 月份的母親節，溫馨的節慶也成了垃圾郵件與病毒散布者利用的對象，各式各樣以「母親節」為主題的垃圾郵件充斥氾濫，像網路訂花服務、母親節禮品購物網站廣告等。部分垃圾郵件甚至夾帶電腦病毒、或以偽裝成大型購物網站的連結騙取使用者密碼、銀行帳號等隱私資訊。本節內容包括：

❸-1 垃圾郵件傳播者如何取得您的電子郵件
❸-2 如何降低收到垃圾郵件的機會
❸-3 各種常用電子郵件軟體的垃圾郵件過濾設定方式

❸-1 垃圾郵件傳播者如何取得您的電子郵件

參考國際資安推廣組織 Get Safe Online 之相關報告[48]，垃圾郵件傳播者可透過以下方式取得您的電子郵件：

- 利用猜測方式。垃圾郵件傳播者會利用自動化的程式產生電子郵件位址。
- 從公開網站中撈取。當網頁中含有 e-mail 位址時，可透過類似搜尋引擎的程式工具，搜尋到這些公開的 e-mail 位址。會公開 e-mail 的網站例如：網路聊天室、社群網站的個人資料、學校網站、新聞討論區等。
- 從線上註冊管道。若您曾經在隱私權政策標示不清楚或根本沒有隱私權政策的網站上提供您的 e-mail 位址（例如：註冊成為會員、註冊參加抽獎活動……等），這些網站可能會將所蒐集到的 e-mail 位址賣給第三方。
- 從其他的垃圾郵件傳播者取得。販售 e-mail 位址清單是相當普遍的行為。
- 從偽造的「取消訂閱」服務取得。某些電子郵件會提供收件者所謂「取消訂閱」的服務，無論是連結到取消訂閱的頁面，或直接透過 e-mail 回覆方式取消訂閱，您都會將您的 e-mail 再次提供給對方，惡意的郵件散布者其實真正想做的是蒐集您的 e-mail 位址，或利用您「回信」的動作來確認您的電子郵件信箱是正確無誤且是有在使用中的。換言之，當回覆信件的同時，您的 e-mail 可能被放入另一個郵寄清單中，繼續成為垃圾郵件發送的對象。

❸-2 如何降低收到垃圾郵件的機會

對於降低收到垃圾郵件的機率，使用者應對垃圾郵件防範和郵件收送有正確的認知，包括：

- 絕對不回覆垃圾電子郵件訊息，因為這樣會讓寄件者知道您的信箱是有效的。而此處所提到的「不回覆」包括：不回信給寄送者說明希望未來不要再收到對方的電子郵件，甚至是郵件當中原本就存在的「取消訂閱」或「請將我從電子郵件清單中移除」等連結，也不要點選。
- 若有任何人或公司透過電子郵件向您索取個人資料，或是傳送個人資料請您確認或更新時，請保持高度警覺。當需要進一步打電話確認時，請確定電話號碼是否可靠或打 104 查詢，切勿使用電子郵件中提供的電話號碼。也避免向不請自來的電訪人員透露任何個人資料。
- 不購買垃圾電子郵件的廣告商品，這樣只會鼓勵寄件者持續不斷的寄發，並且也避免電子郵件地址被加入到出售的電子郵件清單中，進而降低收到的垃圾郵件量。
- 不轉寄串接式的電子郵件，例如聲稱不轉寄給 10 個人就會倒楣的電子郵件。這樣的轉寄行為所累積的電子郵件，是垃圾郵件寄送者蒐集電子郵件信箱的技倆。
- 需要寄送同一訊息給許多收件者時，可採「密件副本」方式來進行，勿將所有收件者的電子郵件信箱曝光於「收件者」欄位中，以避免遭廣告信業者蒐集電子郵件地址。
- 刪除寄件者為空白的電子郵件。
- 非必要不將自己的 e-mail 提供給他人，避免收到過多垃圾郵件，耽誤正事增加困擾。如果需要在網站中留下個人資料或電子郵件時，仔細閱讀網頁中有無包含「未來是否希望收到新資訊及新產品介紹」之選項，並仔細閱讀留下資料的網站隱私權保護聲明，了解電子郵件信箱會被使用的用途。
- 使用垃圾電子郵件過濾軟體。
- 善加利用電子郵件收信軟體所提供的自動過濾、自行設定篩選垃圾郵件功能。

資安素養小專欄

為何垃圾郵件的縮寫是 SPAM？

垃圾郵件又稱為 SPAM，關於 SPAM 的由來有兩種說法，其一是源自於英國某個喜劇影集中的橋段，當時英國的 Hormel Foods 公司所生產的豬肉罐頭(Specially Processed Assorted Meat)相當受到歡迎，劇中有一對夫妻在餐廳想要點不含 SPAM 的餐點卻無從選擇，而餐廳裡的一群維京人則是不斷地高唱著「SPAM, SPAM, SPAM…」，後來 SPAM 就被延伸為氾濫成災、剝奪他人選擇權利之意。

另一種說法為，SPAM 是「同步刊登廣告」(Simultaneously Posted Advertising Message)的縮寫，大量寄發 SPAM 的人就稱為 SPAMMER。

根據 2003 年 2 月 9 日紐約時報的報導，世界上的第一封垃圾郵件為 1978 年由 Digital Equipment Corporation 發出的產品介紹信。

參考資料：

- 呂宗翰，企業的 Anti-SPAM 大作戰
- Yahoo!奇摩反垃圾信特別企劃

❸-3 常用電子郵件軟體的垃圾郵件過濾設定方式

由於垃圾郵件氾濫，目前幾乎所有的收費或免費電子郵件、電子郵件收信軟體，皆提供自動過濾、自行設定篩選垃圾郵件的功能。自動過濾是指系統會自動判斷所收到的電子郵件是否為垃圾郵件，然後將垃圾郵件集中到垃圾郵件匣；自行設定篩選則是使用者自行設定相關關鍵字篩除垃圾郵件。兩種作法步驟說明如下：

- 在 Web 郵件上設定過濾垃圾郵件寄件者

  以 web 介面的電子郵件服務 Gmail 為例，下圖紅框標示的「垃圾郵件」資料夾，為 Gmail 自動過濾出的垃圾郵件歸類處。

使用者也可以將收件匣中的垃圾郵件選取，並點選「回報為垃圾郵件」的按鍵，回報系統選取的郵件是垃圾郵件，這樣下次就不會再收到相同的垃圾信。

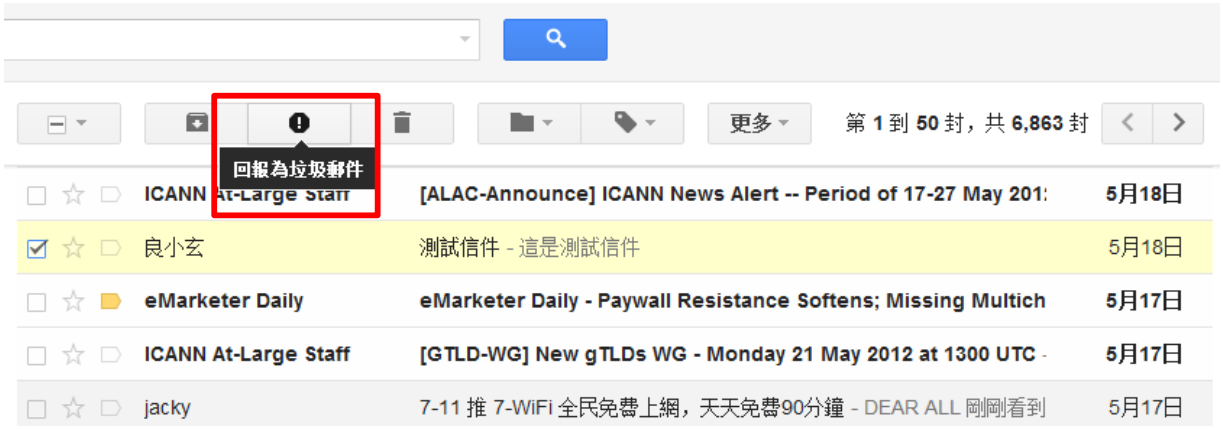


圖17. 在 Web 郵件上設定過濾垃圾郵件圖示（畫面來源：Gmail / 製圖：NII 產業發展協進會）

- 設定收信軟體的關鍵字過濾功能

  大多數的電子郵件收信軟體都提供了簡易的郵件篩選功能，以 Microsoft 的 Outlook 為例，若要將信件主旨中出現「在家工作」、「高薪」等關鍵字的郵件列為垃圾郵件，並直接將信件移動到垃圾郵件資料夾，其設定方式的步驟說明如下：

步驟一：選擇「工具」→ 選擇「規則及通知」

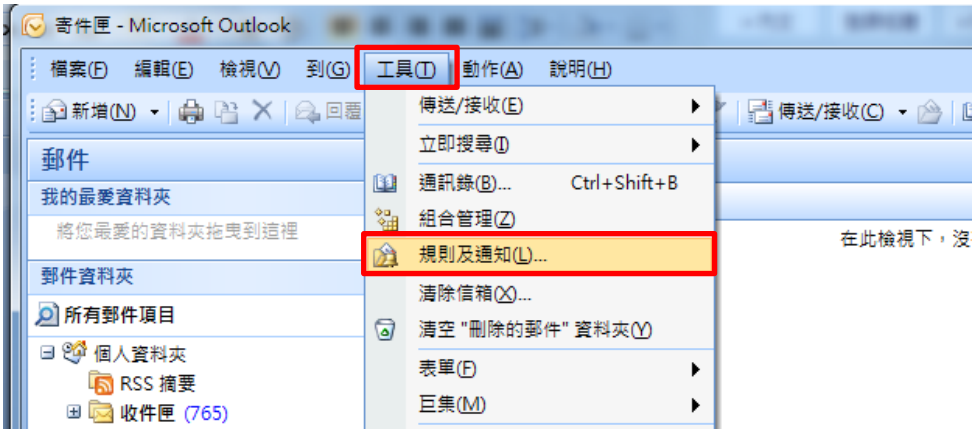


圖18.　如何設定 Outlook 關鍵字過濾功能 (製圖：NII 產業發展協進會)

步驟二：選擇「電子郵件規則」選單 → 選擇「新增規則」→ 點選規則精靈視窗中的「移動主旨中有特定文字的郵件至資料夾」。

步驟三：繼續在步驟二的下方框框中點「特定文字」。出現「搜尋文字」視窗，輸入垃圾郵件的郵件標題關鍵字，例如「在家工作」，然後按「新增」鍵，再按「確定」鍵。

步驟四：點選步驟二框框中的「特定」資料夾，出現「規則及通知」視窗，點選垃圾郵件資料夾，然後按「確定」回到「規則精靈」視窗，然後按「完成」結束「規則精靈」，再按一次「確定」鍵結束設定。完成此郵件規則設定後，當收到的信件其郵件標題中有「在家工作」這個關鍵字時，信件就會自動被移到垃圾郵件夾。

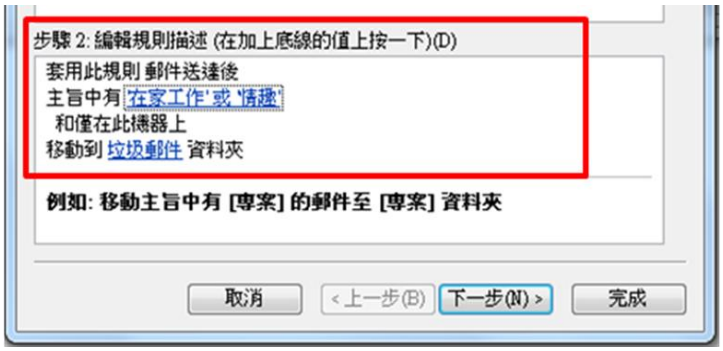
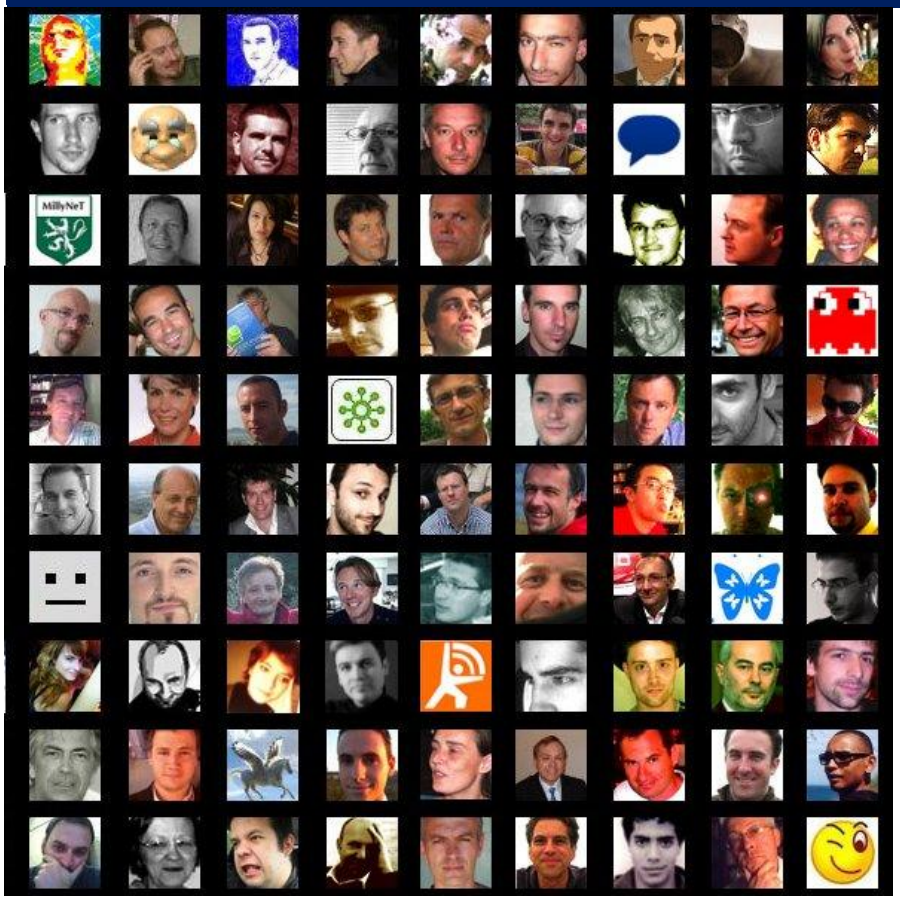


圖19.　設定 Outlook 關鍵字過濾功能結果 (製圖：NII 產業發展協進會)



By @jbtaylor (CC BY-SA 2.0) http://www.flickr.com/photos/jbtaylor/

主題 2.社群網站服務安全

網際網路上目前最流行的就是社群網站或社交網路了，民眾普遍所認知的社群網站服務以臉書(Facebook)為主，其實，社群網站服務已經存在於網路世界中一段時間了，例如 BBS 就是古老的社群網站服務，一群群志同道合的人，透過網路建構的交流平台，針對不同的主題，網友們可就其有興趣的題目與他人進行討論。本節將從社群網站服務的定義談起，介紹國內外受歡迎的社群網站，並說明其共同特色，及利用統計數據來闡述社群網站服務受歡迎的程度。本節重點內容包括：

❶ 社群網站服務的特色

❷ 社群網站的安全風險

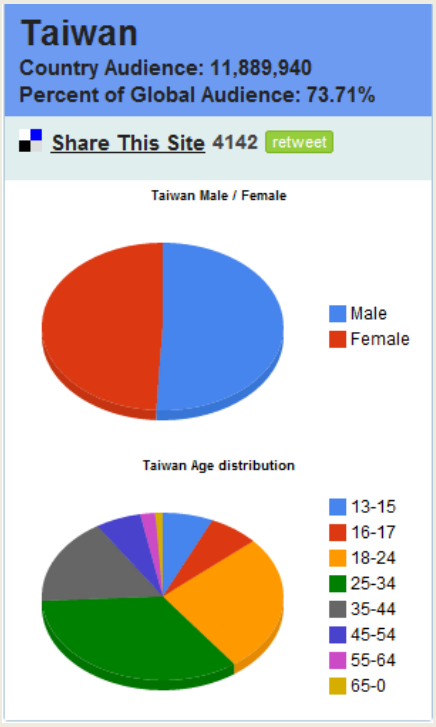
❸社群網站安全使用五大要點

數字會說話

臺灣的臉書用戶概況

根據 Checkfacebook.com 的統計顯示，臺灣的臉書註冊用戶已經超過 1.18 千萬，其中男性用戶的比例為 50.8%，女性用戶數則為 49.2%。

在年齡層方面，以 25-34 歲族群為最大宗，佔 34.3%；其次為 18-24 歲族群，佔 26.4%。第三大族群是 35-44 歲，佔 16.7%。換言之，18-44 歲族群佔了臺灣臉書用戶數的 77.4%。



資料來源：Checkface.com

數據日期 ：2012.05.22

❶ 社群網站服務的特色

根據維基百科，社交或社群網站服務（英文：Social Networking Service）主要是為一群擁有相同興趣與活動的人所建立的線上社群。此類服務為用戶提供各種聯繫、交流的管道，並且通常會透過朋友，一傳十、十傳百地把網路展延開，類似樹葉的脈絡，在臺灣一般稱為「社群網站」。多數社交網路服務會提供多種讓使用者互動的方式，例如聊天、寄信、影音、檔案分享、部落格、討論群組等。

大家最熟悉的社群網站服務是臉書、噗浪、微博、Google+、推特(Twitter)、Linkedin 等服務。依維基百科的定義，社群網站服務還可以包含強調與他人分享的網路服務，像是 Flickr、Picasa 等網路相簿服務；或是如 YouTube 等的影音分享服務；再者就是結合文字與影像的生活故事或經驗分享的部落格服務，例如：無名小站、痞客幫、天空部落格……等。

其他像是以結交新朋友為目的之網站，例如：愛情公寓、MySpace……等；集合共同興趣或嗜好的一群人針對相同主題進行討論與交流的討論區與論壇服務，例如：Mobile01、背包客棧……等；甚至是時下流行的多款線上遊戲，其實都提供了玩家與玩家之間進行互動與交流的功能，均可以泛稱為社群網站服務。

社群網站不僅只是上提幾個近年才成功發展的服務而已， 早在十多年前就開始流行的即時通服務，如 MSN、雅虎即時通、ICQ 等；以及 BBS 服務，例如批踢踢等，因提供了聯繫、分享、交流、互動等功能，都屬於社群網站類型之服務。

這些社群網站服務大多非常受到網路使用者的歡迎，例如，社群網站龍頭 – 臉書，其在全球的用戶數已經超過 8.4 億，有人比喻，若將臉書當作是一個網路上的虛擬國度，那麼臉書將會是全世界第三大國，人口數僅次於中國和印度。

數字會說話
其他國家的社群網站應用概況

- 在歐洲，平均每個人會加入 1.9 個社群網站
- 73%的歐洲網路使用者有參加社群網站
- 在美國，平均每個人會加入 2.1 個社群網站
- 網友每次停留在臉書的時間約 37 分鐘，停留在 Twitter 的時間是 23 分鐘
- 超過 4 億個網友每天都會使用臉書；超過 6 億個網友每天都會使用任何一種社群網站服務
- 超過一半的社群網站使用者追蹤特定的品牌
- 人們成為某個品牌的臉書粉絲團成員是因為他們喜歡其產品，而不是因為廣告的緣故
- 在日本，前三大社群網站服務分別是 Twitter, Facebook 以及 Myspace
- 最常被使用的手機 APP 類型是社群網站服務

資料來源：Insites consulting, Social media around the world 2011

多樣化的社群網站中，有幾個共同的特色，而這些特色也是吸引大量使用者持續使用社群網站服務的重要原因。

- 簡單上手

幾乎所有的社群網站都設計得非常容易使用，即使不具備專精的電腦技能，都可以輕易地完成會員註冊並以直覺方式學會基本操作，有些連電腦操作都不大熟悉的年長者，甚至都已經學會如何在開心農場中偷菜了呢！

- 好玩

多樣化的社群網站服務，不僅提供與既有朋友交流的功能，也提供了拓展社交圈與其他志同道合朋友互動的機會；此外，以文字、聲音、影像、動畫、多媒體的呈現方式，還有像是小遊戲、小測驗等殺時間或可以成為話題的應用程式，都是社群網站好玩且容易對使用者產生「黏性」的特點。

- 分享

多數的社群網站都強調了分享功能，透過分享，與親朋好友及新網友產生互動。此處所提到的分享內容可能是抒發自己心情的短文、網路上看到笑話或啟發的轉寄、出國旅行的紀錄、家中寶寶的成長照片、自己創作的音樂影片等。我們透過分享來展現自己，其他網友也透過您的分享與您結識。

- 免費的

幾乎所有的社群網站都是免費註冊的，此特性提供使用者可在同一個社群網站上擁有多個不同的身分，便於管理不同的朋友，不過這也讓惡意人士有機可乘。

by hank grebe (CC BY 2.0) http://mediaspin.com/blog/

社群網站小專欄

形形色色的社群網站服務，您認識幾個？

- Facebook：起源於美國校園的社群服務網站，使用者可以在 Facebook 上建立自己的個人專頁，加入其他用戶作為朋友並交換信息。透過塗鴉牆方式公告給所有朋友知道自己的動態，也提供聊天室、傳訊息、分享照片與影片、遊戲等服務。Facebook 在臺灣多被稱為「臉書」。
  參考資料：維基百科

- Linkedin：專門針對商務人士的社交網站，於 2003 年正式對外服務，該網站主要提供使用者維護其在商業往來中認識並信任的聯絡人，或稱之為人脈 Connections，使用者還可以邀請他認識的人成為人脈。
  參考資料：維基百科

- Twitter：微網誌的老祖宗，允許玩家以 140 字短文互通聲息，這些消息也被稱作「推文」，也因此 Twitter 被形容為「網際網路的簡訊服務」。使用者可透過官網、聊天室、電子郵件、即時通、手機及其他應用軟體來發出推文。
  參考資料：維基百科

- 和您認識與信任的朋友一起分享

社群網站的分享功能基本上是與您同意的朋友清單上的朋友一起分享，這些網站也假設您同意加入成為朋友清單一員的人都是您熟識與信任的朋友。

但事實上，您所分享的資訊不見得只會與您認識與信任的朋友分享，您所透露的哪些資訊希望跟哪一群朋友分享，並不容易透過電腦與技術的簡單分類，或透過相對複雜與不易瞭解的隱私權設定，就能夠符合人們對於人與人之間複雜關係的需求。

❷ 社群網站的安全風險

縱然社群網站服務很好玩，每一位社群網站使用者都應該瞭解相對應的使用風險有哪些，本小節將歸納常見的五大安全風險：

❷-1 隱私權侵害

❷-2 不當言論

❷-3 惡意程式與詐騙

❷-4 垃圾郵件

❷-5 社群網站沉迷

❷-1 隱私權侵害

許多人透過社群網站分享私人訊息，包括個人照片、「打卡」資訊、朋友、興趣等個人資料，在分享的同時，也暴露自己的隱私，這樣矛盾的關係，多年以來一直讓社群網站的隱私權問題受到矚目，隨著社群網站提供的服務內容越來越多元化，隱私權問題也日益重要。

形形色色的社群網站服務，您認識幾個？

- Plurk（噗浪）：創立於 2008 年的微網誌社群網站，在臺灣、東南亞、香港等地區快速受到使用者的喜愛，每次最多可鍵入 140 個字，除了可供使用者記錄生活點滴，亦具備快速的訊息傳遞特性。
  參考資料：噗浪官網

- 新浪微博：由中國新浪公司推出的微博網站，佔中國微博用戶總量的 57%，自 2009 年 8 月推出至今已超過 3 億用戶註冊，使用者橫跨兩岸三地。
  參考資料：維基百科

- YouTube：創立於 2005 年 2 月，提供全球使用者一個可彼此聯繫、交流資訊、激發創意靈感的平台，目前全球已有超過數十億人會透過 YouTube 搜尋、觀看及分享原創影片。
  參考資料：YouTube 官網

- Flickr：受歡迎的網路相簿服務，其自詡為「幾乎可以肯定是世界上最好的線上相片管理和分享應用程式」，其服務強調了協助人們讓與其相片有關的人可以看到這些相片，以及啟用組織相片和視訊的新方式。
  參考資料：Flickr 官網

圖像來源：Plurk, YouTube, flickr, 新浪微博官網

社群網站服務隱私侵害的三種來源

一般而言，社群網站服務的隱私權侵害可能來自於包括第三方、其他社群網站服務使用者、以及社群網站本身等三種來源。

- 隱私侵害來源一：第三方

第三方可以從社群網站上取得您的個人隱私資料種類，大多是直接從您填寫在社群網站中的個人資料或隱私訊息。例如，許多人註冊社群網站之目的為結交新朋友，特別是青少年有較高的比例會透過像是臉書等社群網站結交網友，也因此，這個族群的使用者會在社群網站的個人資料頁面中填寫有關自己的詳細資料，以尋求志同道合的夥伴或朋友。以臉書為例，其個人資料頁面涵蓋了包括姓名、居住地、性別、生日、血型、性向、任職公司、就讀學校或曾經就讀的大學與高中、畢業年度、手機號碼、嗜好、興趣等，如下圖所示。

圖20.　社群網站的個人資料檔案設定頁面

(圖像來源：Facebook，製圖：NII 產業發展協進會)

社群網站服務以社群連結為號召，使用者很容易對個資的分享少了警覺性；倘若使用者在隱私權設定上又不夠周全，這些個人資料或所分享的訊息很輕易地就會被第三方取得，例如透過 Google 搜尋引擎就可以搜尋得到，也讓有心人士有機可乘。

去年底在台中即發生了利用臉書綁票的真實案例，警方破獲了一起擄人勒贖案，逮捕綁架 1 名大學生且向其家屬勒索贖金 100 萬元的 4 名歹徒，警方意外發現嫌犯透過被害人的臉書帳號掌握情資，確認被害人每天清晨 4 點 40 分都必須到飯店實習，因此選定時間動手綁架。

不只是在社群網站上的個人資料頁面過度揭露個資可能會產生問題，許多網友喜歡在部落格上分享自己的生活點滴，例如大啖美食、慶生會活動、母親節大餐、同學會、婚宴、旅行遊記等，這些行為也都具有風險。根據婦女救援基金會在 2010 年的「國中生網路行為調查報告」指出，將近七成五的青少年有部落格，其中有六成會在部落格上公開自己的個人資料，14%的學生認為只要有加密或上鎖，部落格上即可上傳私密照片；5%的學生認為：「放上去還蠻酷的，可以秀自己！」。這些私密照片一旦透過部落格公開在網路上，就永遠都將流傳在網路上，即使未來後悔想要刪除，也不容易百分百地清除。

- 隱私侵害來源二：其他社群網站服務使用者

除了使用者自己可能會洩漏隱私資訊外，社群網站服務另一種侵害隱私的隱憂就是受到隱私設定較為寬鬆的「朋友」拖累，這些透過社群網站連結上的朋友可能會不小心洩露您的個人資料。以臉書為例，或許您從來不使用「打卡」功能，但在自己或朋友的塗鴉牆討論串中，朋友會提及有關您的近況或資訊（例如：離職規劃、秘密進行中的求婚計畫、低調的婚禮籌備……等），或者朋友會直接上傳包含您在內的大合照，並在照片中標籤(tag)出您的身分，結果可能許多人也都知道了原本您不希望讓太多人知道的訊息。

形形色色的社群網站服務，您認識幾個？

- 無名小站：1999 年由交大學生所創立，在 2007 年被 Yahoo!奇摩併購。無名小站提供使用者免費的相簿、影音、網誌空間及線上揪團等服務。
  參考資料：Yahoo!奇摩

- 痞客幫(PIXNET)：主要提供使用者相簿、部落格、影音、留言版等功能。
  參考資料：城邦媒體控股集團

- 巴哈姆特電玩資訊站：以知名遊戲的召喚獸「巴哈姆特」命名的動漫及遊戲社群網站，1996 年成立時是國內第一個以電玩為主題的 BBS 站，逐漸吸引許多熱愛電玩的學生加入，並轉型為社群網站，提供網友各類動漫及遊戲最新新聞與作品介紹。
  參考資料：巴哈姆特電玩資訊站

- Mobile01：網路論壇服務，簡稱 01，提供網友行動電話、行動裝置、3C 等電子產品與臺灣景點、女性流行、生活娛樂……等多樣化主題的討論平台，在 Alexa 的統計中，為高瀏覽率 3C 資訊討論網站之一。
  參考資料：維基百科

圖像來源：痞客幫、無名小站、巴哈姆特、Mobile01 官網

- 隱私侵害來源三：社群網站本身

無論使用者在社群網站上的隱私權設定得多麼完善，只能限定少數朋友們可以看得到，卻忽略了社群網站本身就是個資外洩的可能來源。社群網站本身可以取得最完整的用戶個人資訊，甚至包括用戶在瀏覽其網站所衍生的軌跡資料，例如：使用者的登入時間、網頁瀏覽歷程紀錄、IP 位址、使用時間、使用的瀏覽器……等。社群網站可能會將會員的個人資料與其他廠商或廣告商分享，或做為其他行銷用途。

❷-2 不當言論

英國曾有一名 16 歲少女因在臉書上抱怨工作內容超無聊而被主管開除，此為社群網站上發表不當言論的真實案例。因為不當言論而危及工作的案例在臺灣也曾經發生過，就在去年（2011 年）日本 311 海嘯事件後，國內某位立法委員的助理在臉書上發表仇日言論，這些言論除被網友炮轟外，也因為上了媒體，導致該名助理因此被解除職務，甚至還有網友將這個訊息翻譯成日文，登上日本雅虎的版面。

由於網路上言論遞送速度快且廣，滿足了許多使用者分享個人情緒或想法表達的需求，在網路上透過部落格或社群網站公開個人想法已經成為普遍的社會現象與趨勢，這也是民主社會所重視的言論自由概念。但許多人在網路上自由表達意見，卻忽略了所傳播的訊息如果涉及他人隱私、毀謗、破壞行為，仍必須面對法律的責任，而不僅只是以上案例提到的丟掉工作而已。

資安素養小百科

臉書上的標籤(tag) 是什麼？

臉書應用程式（相片、影片、網誌）於發布訊息時，有內建的標籤(tag)功能，讓使用者將發布的訊息、相片、影片、網誌能同步在朋友的塗鴉牆上出現，作用是方便人們知道有人在臉書上提及了他，邀請他登入臉書進行回覆，達到通知及擴散的效果。

標籤(tag)的效用雖能達成通知及擴散的效果，但屬於「公開性」的張貼行為，恐易被朋友視為 SPAM 行為甚至有侵犯隱私的疑慮，故應謹慎運用。而部分應用程式也常濫用標籤(tag)功能，自動抓取朋友的 ID，組成人物拼圖擴散張貼，為避免造成他人困擾，建議盡量不要點選此類應用程式。

參考資料：Facebook 使用說明中心

噗浪上的 Karma 值是什麼？

在臺灣、東南亞等地區受網友歡迎的微網誌社群網站 Plurk（噗浪）中，每位噗浪會員都有自己的「Karma 值」，此 Karma 值可以透過邀請朋友加入噗浪或每天發表訊息等方式提升數值，當 Karma 值達到一定等級後，使用者將可使用某些特殊表情符號；相反的，使用者若不常上噗浪，或提出加入朋友邀請卻被拒絕時，都會使 Karma 值下降。

資料來源：噗浪官網

在美國有一名男子家暴，其妻子因此獲得臨時保護令及兒子的主要監護權，隨後該名男子在自己的 Facebook 頁面上寫道：「妳是一個報復心極強的壞女人，一心想毀掉妳丈夫的生活……」。這樣的文字被其妻子看到後，便一狀告上法庭，指責前任丈夫違反臨時保護令。儘管前任丈夫在貼文中並未指名道姓，但法官仍認定此違反了法院授予的臨時保護令，因此做出了 60 天監禁和 500 美元罰款之裁決。

根據媒體報導，去年（2011 年）在新北市發生了某家醫院急診護理人員將病人傷口照片放上臉書的個人網頁上，並描述工作內容，該照片及言論引發網友的撻伐，該名護理人員雖然事後說明只是和朋友分享工作點滴，沒有暴露病人隱私的意圖，但此行為已違反護理人員法第 28 條有關「護理人員或護理機構及其人員對於因業務而知悉或持有他人秘密，不得無故洩漏」之規定，須依法處新臺幣六千元以上三萬元以下罰鍰，並限期令其改善。

前陣子英國有一名大學生將自己在 7 秒內喝下一瓶 1 品脫的伏特加，在 1 分鐘內喝完 1 瓶紅酒、1 瓶白酒與 1 瓶玫瑰紅酒且保持清醒的影片，刊登到網路上，雖然短時間內造成數十萬的點閱率，但也引起各界批評，認為他的行為既愚蠢也可能會造成飲酒觀念誤導，更可能讓自己酒精中毒。而其他常見在社群網站發表不當言論的類型還包括像是毀謗、謾罵、歧視、恐嚇、謠言、製造對立等。

❷-3 惡意程式與詐騙

或許您也有過這樣的經驗，一打開臉書或 MSN，就發現有朋友傳來訊息，對方給您的訊息中包含一個超連結，可能要您去看一個網路相簿或閱讀一則有趣的新聞，若一時不察直接點選該連結，便中了病毒的招，該超連結可能會引導使用者下載檔案，檔案內是蠕蟲惡意程式，只要點開壓縮檔就會在電腦上安裝惡意程式，臉書或 MSN 將自動以您的名義發送訊息給您的朋友。

如同釣魚電子郵件一樣，駭客會利用吸引人的文字或利用重要時事，透過社群網站平台來誘使網友點選含有惡意程式的超連結，例如今年才推出的新 iPad，一上市就立即成為駭客社交工程與垃圾郵件的誘餌，該名駭客以贈送 iPad 3 為誘因，運用臉書及垃圾郵件傳遞 iPad 3 抽獎的訊息，吸引使用者參與抽獎並騙取使用者手機與電子郵件等個人資料；此外，駭客還會要求使用者協助張貼抽獎訊息於自己的個人網站或臉書頁面，以增加中獎機率，此作法讓不知情的使用者不僅洩漏了自己的個資，也成為網路犯罪的幫兇。

Source: 微軟 Microsoft 圖像資料庫 http://office.microsoft.com

臉書並非您唯一會看到免費贈送 iPad 3 的平台，在噗浪、推特、微博、部落格留言板、以及您的電子郵件信箱中，都有可能看得到類似的訊息，無論是 iPad 3 或已經在媒體中沸沸揚揚討論即將推出的 iPhone 5 新產品免費贈送訊息，都不可能真的會送出時髦的蘋果產品。

另一則是由趨勢科技所提供的案例，某位網路使用者從即時通軟體中，收到表妹傳來的對話訊息，訊息中寫道：「試試看這個我在 facebook 臉書上找到的測驗，告訴我你的測試結果。我沒法通過 109，真悲哀 http://www.iq-scores.info/」。一旦點擊訊息中的連結，就被帶到下面這個製作精美的 IQ 智商測驗頁面。

該 IQ 測試一共有 11 個題目，結束後進入結果頁面時，會要求使用者註冊並輸入手機號碼以取得測試結果。若使用者仔細閱讀頁面下方寫得密密麻麻的會員條款就會發現，一旦使用者提供了手機號碼，就視同為同意「手機內容訂閱」，訂閱費用每月從美金 9.99 到 19.99 不等，手機帳單金額也因此暴增。

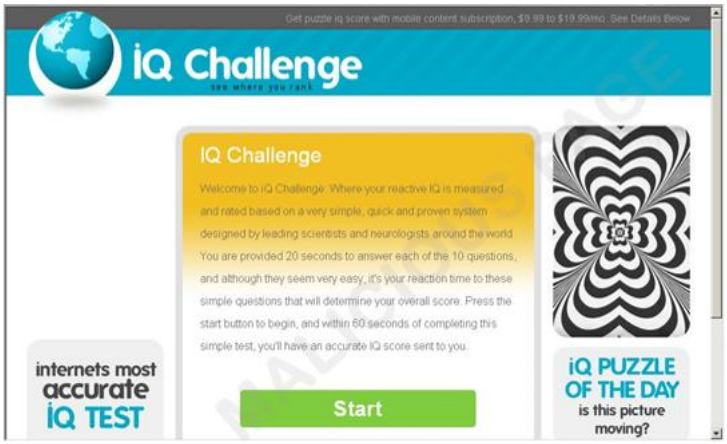


圖21. 利用即時通引導網路使用者前往做 IQ 測驗

(http://blog.trendmicro.com/iq-test-spam-proliferating-via-ims/)

還有一則發生在國內網友玩臉書遊戲因誤按了不明連結而遭詐財的案例。警政署在今年 3 月提出警示，近期有歹徒在臉書塗鴉牆散布不明網址連結，只要網友誤按，不但其帳號會被盜，若使用者曾經在臉書以信用卡消費，卡號也會外洩被盜刷，有網友因而損失 1 萬 5 千多元。該名使用者是因為玩知名的臉書農場遊戲曾經以信用卡購買過農民幣，而交易系統為方便客戶的再次購買，會留存信用卡號碼資訊，以致於其臉書帳號被盜後，信用卡也隨之遭到盜刷。

駭客也針對了不同種類的社群網站使用者設計了不同的惡意程式騙局，例如，玩噗浪的噗友每天會巴望著 Karma 值指數上升，玩 Twitter 的推友，也會以追隨者多寡作為勝利的象徵，看準這樣的心態，Twitter 平台上也曾經出現過一種類似蠕蟲的攻擊行為，吸引想要在短時間內增加大量追隨者的 Twitter 使用者，根據趨勢科技的報導，有超過上萬人受害。該騙局會誘騙使用者使用一個叫 Twittercut 的網站，並輸入其 Twitter 的帳戶名和密碼，一旦輸入後，該惡意網站便會將類似訊息再傳送給被感染使用者所有的追隨者，然後一直串連下去。

其他類似傳播惡意程式或詐騙訊息的真實案例還有，「金光閃閃的 Facebook VIP 用戶粉絲專頁」、「粉紅色的 Facebook 頁面」、「代為轉帳購買遊戲點數」等。

❷-4 垃圾郵件

幾乎各家資訊安全業者都提出類似的警訊表示，新世代溝通社群網站已成為最夯垃圾郵件散播者。除了我們熟悉的垃圾郵件（參照本手冊前一章節），社群網站上的另一種垃圾郵件或訊息，也是許多網友所謂的「洗版」，簡單說，就是當您打開自己的臉書個人頁面時，塗鴉牆上盡是一堆來自於朋友們的罐頭訊息，像是「送你一個蛋糕」、「今天誰是你的幸運星」、「我的超準確心理測驗結果」等。

圖22.　臉書個人頁面上的「洗版」示意（製圖：NII 產業發展協進會）

此類訊息多來自於使用者及使用者的朋友們曾經使用過臉書上的應用程式或遊戲時，也同意應用程式的開發者在自己的塗鴉牆上貼文的結果。在使用者決定要玩臉書上的遊戲或應用程式時，通常會出現以下取得您的某些權限的畫面，不同的應用程式可能會有不同的權限要求，「以你的名字貼文」、「以我的名義發表」、「發送電郵給我」、「取得我的個人資訊」等是幾個常見的授權選項

若沒有仔細閱讀授權項目就按下同意鍵，可能就會發生該應用程式會以您的名義不斷貼文，而不小心也洗了別人頁面的版。

圖23.　臉書應用程式請求授權圖示

（畫面來源：Facebook　製圖：NII 產業發展協進會）

另一種垃圾訊息來自於不小心將熱心人士加入成為朋友，這類的熱心人士可能會大量張貼有關自己公司的產品促銷訊息、或是大量轉寄免費抽獎訊息等等。此類訊息或許內容無傷大雅，只是因為數量龐大，造成您找不到真正有用資訊，或者真正想瞭解的好朋友狀態消息被埋沒的困擾；在這些大量散布的垃圾訊息中，也有可能藏有惡意程式的超連結，使用者必須提高警覺並進一步處理。

Source: 微軟 Microsoft 圖像資料庫 http://office.microsoft.com

❷–5 社群網站沉迷

現在恐怕沒有人沒聽過或不知道臉書或任何一種社群網站了，在臉書看留言、塗鴉牆上寫心情、分享按個讚，也已經成為許多人每天的例行公事；根據 360d 才庫人力資源在 2011 年所公布的「上班族臉書沉迷指數」調查結果，95%受訪上班族有使用臉書，受訪者中也有 21% 每天使用臉書時間超過 3 小時以上，還有 49% 的上班族上網第一個開啟的就是臉書網站。

因為臉書沉迷發生悲慘結果的案例不在少數，去年在美國一位 34 歲的母親因為沉迷於玩 Cafe World 臉書遊戲，導致她連 13 個月大的兒子已在浴缸溺斃都不知道；前年也有一位 22 歲的年輕母親因為玩開心農場遊戲時嫌三個月大的兒子哭鬧太吵，而把兒子搖晃致死，該名母親也因此被控二級謀殺罪。前幾年在南韓也有一對年輕夫婦沉迷於玩照顧虛擬小孩的遊戲，現實生活中卻把自己的孩子活活餓死。

隨著智慧型手機的風行帶動越來越多所謂的低頭族社群網站沉迷者，也造成了新的隱憂，這些到處可見低頭使用智慧型手機或平板電腦的族群，對自己或他人可能均會造成傷害。美國一名才 18 歲的少女沉迷臉書，連開車時都不忘向好友更新自己的狀態，就在今年一月，她一邊駕駛、一邊還在臉書上留言說「開車玩臉書實在好危險……」之後，竟然當場撞上了前方車輛身亡。

臉書沉迷就如網路沉迷或成癮一樣，不僅會影響視力、肌肉、頸部……等，對身體造成傷害，當在駕駛或從事其他工作時若同時也在上網或使用手機，也有可能對他人造成影響。此外還有心理層面的影響，根據美國心理學會(APA)對「網路成癮」之定義為，*因為過度使用網路，而對網路產生一種心理上的依賴，並且持續增加上網時間，無法克制使用網路的衝動。*

臺灣精神醫學會前任理事長陳正宗醫師也曾經在報導中指出，*若一天連續上網 7 個小時，連續 3 個月都出現同樣行為模式，離開網路會坐立不安、焦慮易怒，則屬於網路成癮之現象*。

數字會說話

上班族臉書行為排行榜

1	觀看朋友的動態
2	按讚或留言
3	在塗鴉牆上更新自己的最新動態
4	玩遊戲或心理測驗

上班族粉絲團喜好排行榜

1	食物類（餐廳、美食）
2	娛樂類
3	衣著服飾類

資料來源：360d 才庫人力資源顧問公司-「上班族臉書沉迷指數」調查 (2011/3/16)

青少年獲得新聞的管道

1	電視新聞
2	臉書上的朋友分享
3	主動瀏覽網站

資料來源：親子天下雜誌 30 期 – 2011 青少年閱讀力大調查 (2011/12)

根據挪威卑爾根大學（University of Bergen）所提供的臉書成癮量表，在以下的 6 個問題中，回答「常常」或「總是」的題目數有 4 題（含）以上，表示你可能有臉書成癮了[11]。

- ☐ 你老是掛念著臉書，或想著打開臉書
- ☐ 你對臉書的牽掛日益濃烈
- ☐ 你使用臉書是為了忘卻個人煩惱
- ☐ 你試過減少使用臉書，但卻失敗了
- ☐ 當無法使用臉書時，你會感到焦躁不安
- ☐ 你因為使用臉書過度，已經對工作或學習產生負面影響

以下是由柯俊銘心理師在 2010 年於聯合報所刊載的臉書成癮常見表現列表，提供給民眾參考與評估自己的臉書成癮傾向[43]。

- ☐ 剛起床或睡覺前，都要打開電腦連上去察看
- ☐ 每天瀏覽多次，若因故無法檢視，整個人就會沮喪或焦慮不安
- ☐ 玩到廢寢忘食，忽略現實生活中應盡責任，例如無心上班或做家事
- ☐ 在該網站結交朋友眾多，但半數以上根本沒見過或只碰過一次面
- ☐ 寧願連線上該網站發送郵件、簡訊給親友，卻不願用方便的電話連絡
- ☐ 在該網站找人哈啦的時間，遠比陪伴至親好友聊天或聚會的時間還多
- ☐ 即使已經下線，心中還是念念不忘，期盼能趕快再上去玩
- ☐ 設定手機或電子郵件即時通知，以便能掌握網站上的最新動態
- ☐ 當被詢問在臉書上做些什麼，會變得神經兮兮或防衛心重，甚至編織謊言
- ☐ 明明有配偶或異性伴侶，卻設定是單身狀態，發展虛無的網路戀情

❸ 社群網站安全使用五大要點

本節將針對上節所提到的安全風險，提出民眾安全使用社群網站服務的五大要點：

❸-1 著手隱私權設定
❸-2 三思後才 post 文
❸-3 不點選不明來路的連結
❸-4 回報垃圾郵件(SPAM)或設定黑名單
❸-5 避免臉書沉迷小撇步

❸-1 著手隱私權設定

隱私權設定是保護個人在社群網站隱私的最基礎步驟，其可讓您選擇哪些人可以閱讀與檢視有關您個人的資訊。部分社群網站預設的使用者隱私權設定為公開讓所有人看得到您的個人資料，但是大多數的網站都允許使用者可以進一步做調整與客製化其隱私權設定，使用者一定要調整自己的隱私權設定值，最小化可以取得您個人資料的對象。

此外，也須注意的是，一些社群網站也會不定期地修正其隱私權聲明或隱私權設定方法，例如為了讓網站的某個新功能得以運作，必須降低使用者的安全設定，也建議您定期檢視自己的隱私權設定是否仍符合您的安全需求。

只接受認識對象的朋友邀請

盲目接受來自任何人的朋友邀請，只會讓自己的個人資料被更多陌生人知道而已，請試著逐一檢視您在臉書或噗浪朋友清單中的每一位朋友，清單中有幾位是您真正認識的人？ 只是點頭之交的又是哪幾位？ 連對方真實姓名都不清楚的又有哪些？請記得，您所加入的朋友都可以閱讀您自己填寫的個人資料，或者閱讀您更新在這些社群網站上的動態資訊與照片，每次更新資訊或照片時，請務必記得有您不熟識的人也在閱讀這些資訊。

若您覺得這樣的資訊揭露給這麼多陌生人並不適當，或者您發現某些已加入成為自己朋友的人常常給您奇怪的回應或有其他問題，您都可以利用社群網站提供的朋友移除方式，與對方切斷關係。

絕對不可公開在社群網站上的個人資訊

即使您透過隱私權設定篩選出哪些朋友可以看得到您所分享的資訊，仍要記得，這些朋友具備是否要將這些資訊轉寄出去的自由，而且您不容易針對這樣的自由進行管控。一般而言，絕對不要在您的社群網站個人資料檔案中分享以下資訊，或公開在任何的部落格中，即使您已經加密或限定只有少數人可以讀取您的個人資料：

- 家庭電話與地址
- 完整的生日（年、月、日）
- 身分證號碼
- 任何的密碼（社群網站、電子郵件、ATM 提款卡、網路銀行、電腦開機密碼……）
- 家庭的經濟狀況
- 信用卡號碼或銀行帳號資訊

除了自己控制公開的隱私資料外，也應該和您的社群網站朋友溝通尊重您的個人隱私，不要隨意公開與您有關的訊息或照片，例如請您的臉書朋友們不要為您打卡或加註標籤(tag)功能。若很難掌握朋友幫您進行 tag 的標示行為，也建議您在自己的隱私設定中，「勾選」標籤審查，可先行查看朋友在您發布的內容所貼上的標籤，再決定是否可以出現在臉書上，如下圖所示。

圖24.　審查臉書之標簽設定圖示

(圖像來源：facebook / 製圖：NII 產業發展協進會)

以臉書遊戲為例，當您決定要玩某個遊戲前，頁面上通常會跳出「授權請求」，請求您同意確認該應用程式將取得有關您的哪些個人資料，包括您的姓名、個人資料、用戶 ID、好友清單、聯絡方式、別人分享給您的資訊等項目，都是常見會授權提供給遊戲開發廠商的資訊。若您不確定您要分享個人資料的對象為誰，或不瞭解遊戲開發廠商可能會將您的個人資料運用在哪些用途，例如可能拿來做行銷廣告，甚至是會與其他第三方進行分享等，請不要輕易地同意該授權請求。

您可以在授權請求畫面中（如下圖）瞭解該應用程式或遊戲會取得哪些您的個人資訊，最下方灰色小字部分亦會提供該應用程式開發者將如何使用您的個人隱私資料的超連結，請您仔細閱讀後再決定是否參與，若有任何質疑，建議不要同意授權。

圖25.　臉書應用程式授權請求示意

（圖像來源：Facebook/ 製圖：NII 產業發展協進會）

資安小專欄

提醒青少年謹慎填寫在社群網站上的個人資料

根據親子天下雜誌的「2011 年青少年閱讀力調查」結果，82%的國、高中學生擁有臉書帳號；國外的 Pew Internet Project 調查也顯示，有 50% 的青少年會透過社群網站結交新朋友，因此在社群網站的個人資料介紹上，會盡可能地仔細填寫，期望能夠藉此尋求志同道合的夥伴。建議家中有使用社群網站服務青少年的家長，須提醒青少年重新檢視自己公開的個人資料，並考量：

- 利用綽號取代真實姓名；
- 利用寵物、風景照、卡通人物等圖像來取代自己真實的大頭照；
- 在填寫個人資料時應盡可能填寫最少的欄位；
- 絕對不要留下家中的地址及電話。

❸-2 三思後才 post 文

無論您在社群網站上使用的是真實姓名、英文名字或綽號，或者您的隱私設定得非常嚴謹，接受朋友邀請與篩選朋友方面也十分謹慎，在任何的社群網站（包括臉書、部落格、微網誌、網路相簿或影音分享等），還是必須得有您是在公開場合發言的心理準備。因為您可能在某次疏忽下或者有其他考量情況下，必須加入一位不是很熟稔的朋友；或者當您的發言論點和您的某一位朋友的論點有非常大的差異時，當下朋友的情緒可能一時失控，因此在您不知情的狀況下，您的發言或分享的照片可能透過轉推、按讚、分享、爭論、轉寄等方式給傳播出去了，即使您在事後刪除發言或某張照片，但已經傳播出去的資訊，非常有可能仍然會存在於網路社群其他使用者的頁面中，甚至流傳在整個網際網路上。

像是先前國內有一名員警酒後開車之後，還在自己的臉書上炫耀自己酒駕沒有被抓包是因為自己都知道警察在哪裡臨檢的結果，其張貼的文字就被網友大量轉寄出去，造成該名員警被懲戒的結果。此外，有時您在社群網站上的評論或發言原本的意圖可能並不是想要侮辱某件事情或某個人，但是您的言論在不同人的解讀下，都有可能被斷章取義，或加油添醋後再傳播出去。

建議每一位社群網站使用者，在網路上發表言論或上傳照片、影片之前，都請再思考幾分鐘，若這段文字或影像公開在網路上時，會不會造成自己的麻煩？ 有沒有觸犯他人或自己的隱私？ 有沒有可能會對誰造成傷害？ 特別是以下類型的言論，務必更謹慎地思考公開與否。

- 歧視言論，包括針對女性、身障人士、弱勢團體、特定種族或某個族群等的不當發言；
- 批評某個宗教的言論；
- 激烈的政治言論；
- 謾罵與毀謗他人的言論；
- 洩漏公司機密的言論；
- 對公司的老闆或同事，或是對學校老師或同學的不滿或嘲弄言論；
- 損害公司形象的言論；
- 任何可能會對別人造成名譽受損的言論、照片或影片；
- 任何您覺得可能會讓人感到不舒服的相片；
- 避免分享過多資訊，包括全家出遊計畫或者隨時上臉書打卡，因為沒有人真的想知道您每分鐘出現在何地，除非是那些想闖空門的小偷；
- 幫朋友打卡與 tag 之前應先取得同意。

❸-3 不點選不明來路的連結

如同電子郵件的安全使用注意事項，社群網站上來自好友或任何應用程式張貼的貼文所附加的超連結，包括在自己或朋友的頁面中出現的、所參與的粉絲團頁面上出現的、或在聊天室中傳遞來的超連結，都要特別注意這些超連結的可靠性，儘量避免點選看起來怪怪的或來路不明的網址。

曾經發生過一個案例是，朋友會在您的臉書塗鴉牆上留言提到：「您被偷拍 Po 上網了！」，並提供一個超連結請您點選去看一張您被偷拍的照片。 一旦點選該超連結就會連到一個網頁，該頁面會要求使用者輸入其電子郵件地址，接著就顯示一隻猴子的照片，然後該網站會告訴使用者可以將這個「玩笑」再傳給其他好友。其實，該超連結頁面最主要的目的就是在蒐集使用者的電子郵件資訊。

請參照本手冊有關 ❷-5 辨識釣魚郵件五大重點、以及❷-4 謹慎開啟電子郵件的附夾檔案等章節之說明。

❸-4 回報垃圾郵件(SPAM)或設定黑名單

許多社群網站都有針對濫發垃圾訊息者提供回報或設定黑名單的功能，適當地回報與設定，可降低您的版面被垃圾訊息「洗版」及收到具有惡意程式垃圾訊息的機會。下圖以臉書為例，說明如何舉報垃圾郵件。

圖26.　如何在臉書舉報垃圾訊息示意圖

（圖像來源：Facebook / 製圖：NII 產業發展協進會）

❸-5 避免臉書沉迷小撇步

針對避免臉書沉迷，以下截錄柯俊銘心理師在 2010 年 4 月份於聯合報所刊載的臉書成癮因應建議[43]。

● 當旁人提醒應適可而止，或因使用太過惹來麻煩，主觀已感到困擾時，應正視問題，坦承有改善必要，主動學習自主管理。
● 取消臉書上的朋友動態更新透過電子郵件或手機簡訊即時通知之設定。
● 每天使用臉書最多不超過 2 次，且每次以半小時為限，必要時可以在電腦旁裝設計時器或鬧鐘，做為警示用。
● 使用臉書不妨將重點擺在瀏覽朋友有無新聞發布與回應上，盡量少玩遊戲、心理測驗。
● 臉書一旦使用完畢，應馬上登出離開該網站，避免一直維持在登入狀態。
● 與其總在朋友的塗鴉牆留言，試著改用電話聯絡或面對面邀約的方式。
● 辦公時若感到疲累，起身動一動，喝杯水、飲料或找同事聊聊天，別把剩餘精力花在臉書上。
● 平時培養其他休閒嗜好。
● 若有心脫離臉書一陣子，關閉帳號或請信得過的親友代為更改密碼都是不錯的方法。
● 若上述政策都不管用，依然強迫性地想去玩，請盡快尋求心理衛生專業，如精神科醫師、心理師等協助。

參考資料

[1] Alexa Internet Website, http://www.alexa.com/

[2] ETtoday 新聞雲，病毒也「林來瘋」 郵件暗藏惡意程式 ，2012 年 3 月

[3] Inside，從趙志勳事件談起–如何避免社交媒體不當發言的負面效應，2011 年 3 月 16 日

[4] ITU, World Telecommunication/ICT Indicators Database 2011 (15th Edition), December 2011

[5] Josh Smith, Free iPad 3 on Facebook? Don’ t Get Scammed, 03/01/2012

[6] Radicati Group, E-mail Statistics Report 2012-2016, April 10 2012

[7] StaySafeOnline.org, Privacy Tips for Social Networking

[8] Symantec, Internet Security Threat Report: 2011 Trends Volume 17, April 2012

[9] Symantec, Symantec Intelligence Report: February 2012, February 2012

[10] TrendLabs Malware Blog, “IQ Test” Spam Proliferating via Instant Messages

[11] University of Bergen: New Research about Facebook Addiction

[12] Vic Hargrave, 10 Social Networking Tips for Parents, April 30 2011

[13] WebSense, Websense 2012 Threat Report

[14] Wikipedia http://www.wikipedia.org/

[15] 于文強，E-mail 電子郵件行銷的善與惡，2008 年 5 月 28 日

[16] 中央社，冒經建會名義釣魚郵件 勿開啟，2012 年 1 月 5 日

[17] 中廣新聞網，「釣魚網頁」假華航之名 小心上當，2011 年 11 月 18 日

[18] 今日新聞網，駭客假冒蔡英文名義 大量寄發釣魚信件，2011 年 7 月 8 日

[19] 天下雜誌，信件小幫手，Outlook 工具輕鬆整理篇

[20] 世界新聞網，沉迷臉書 兒子浴缸淹死，2011 年 1 月 15 日

[21] 卡巴斯基實驗室新聞中心，2012 年 1 月垃圾郵件關鍵詞：愛情、政治、體育，2012 年 2 月

[22] 江雅綺，社群網站臉書（facebook）與隱私權保護，2011 年 10 月 31 日，收錄於教育部人權教育諮詢暨資源中心

[23] 自由時報，「詐」到市議會 假傳票夾帶木馬病毒，2012 年 2 月 1 日

[24] 自由時報，恩師 email 求援? 講師上當，2009 年 9 月 12 日

[25] 行政院研考會，100 年個人/家戶數位機會調查報告，2011 年 9 月

[26] 行政院研考會，電子郵件安全參考指引 V.2，2009 年 3 月

[27] 呂宗翰，企業的 Anti-SPAM 大作戰（上），2009 年 7 月 11 日，收錄於網路資訊雜誌

[28] 李全興，從趙志勳事件談起–如何避免社交媒體不當發言的負面效應，2011 年 3 月 16 日， 本文收錄於 Inside 部落格

[29] 旺 e 報，太沉迷 少女開車 po 臉書撞死，2012 年 3 月 7 日

[30] 林佳明，e-mail 社交工程及防護

[31] 曹乙帆，社交行銷第一步 解構社交網路，2011 年 9 月 6 日，收錄於網路資訊雜誌

[32] 郭勝明，有線電視頻寬上網資訊安全管理系統之探討 - 以台中市有電視業者為例(上)，企業與資訊安全十月號電子報，2011 年 10 月

[33] 硬底子達人網，駭客也瘋 New iPad！臉書成網路釣魚與垃圾郵件攻擊誘餌，2012 年 3 月

[34] 華南銀行，網路銀行操作安全小秘訣手冊

[35] 微軟 Office 支援中心，識別虛假電子郵件和網路釣魚騙術

[36] 微軟官方網站，Windows 7 說明和使用方法

[37] 新頭殼，惡意程式攻擊手機 瘋貼何梅尼人形板，2012 年 3 月 2 日

[38] 資訊與電腦第 282 期

[39] 資策會，2011 年 12 月底止台灣上網人口，2012 年 3 月

[40] 臺灣網路資訊中心，寬頻網路使用調查報告，2011 年 7 月

[41] 聯合報，男切腹照護理師貼臉書 罰錢並停業，2011 年 7 月 14 日

[42] 聯合新聞網，PO 文辱罵客家人 高三女道歉，2012 年 5 月 16 日

[43] 聯合新聞網，還掛在「臉書」嗎？小心成癮，2010 年 4 月 23 日

[44] Openfind, Internet Threats Trend Report, April 2012

[45] Commtouch, Internet Threats Trend Report, January 2012

[46] iThome, FBI 警告：飯店上網小心中毒, 2012 年 5 月 11 日

[47] Visa，電子郵件詐騙參考範例

[48] Get Safe Online, Stop unwanted email

[49] Checkfacebook 網站，http://www.checkfacebook.com

網路服務平台安全

出 版 者　教育部

發 行 者　蔣偉寧　教育部部長

召 集 人　吳國維　財團法人中華民國國家資訊基本建設產業發展協進會執行長

　　梁理旋　財團法人中華民國國家資訊基本建設產業發展協進會協理

指導委員　何榮桂　教育部電算中心主任

　　韓善民　教育部電算中心副主任

　　楊文星　教育部電算中心高級管理師

　　苗宗忻　教育部電算中心資訊管理組組長

　　劉玉珍　教育部電算中心資訊管理組程式設計師

審查委員　李宗薇　國立臺北教育大學教育傳播與資訊研究所教授

　　郭秋田　國立空中大學 管理與資訊學系助理教授

　　賴守全　銘傳大學 電腦與通訊工程學系助理教授

撰稿人員　梁理旋　財團法人中華民國國家資訊基本建設產業發展協進會協理

承辦單位　財團法人中華民國國家資訊基本建設產業發展協進會

出版日期　民國 101 年 06 月

此手冊內容係對特定議題所提供之學習教材，僅供各界參考，非本部相關政策。