2012

辨識網路詐騙學習手冊

教育部全民資安素養推廣計畫

出版日期： 101/06/20

辨識網路詐騙學習手冊

圖像來源：http://office.microsoft.com/

前言

依據國際電信聯盟(International Telecommunications Union, ITU)所公布之 2011 年最新統計數據，全球的上網人口數至 2011 年底已達 24 億，約佔全球 70 億人口總數的 35%[2]，可見網際網路的使用已相當普及。

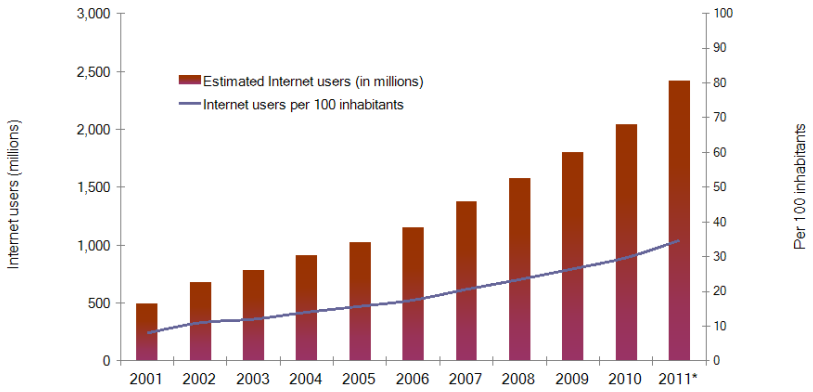


圖1.全球上網人口數統計

（資料來源：ITU World Telecommunication /ICT Indicators database[1]）

而我國的網路使用人數也和全球發展趨勢一致，逐年向上成長，根據資策會創新應用服務研究所 FIND 所公布，截至 2011 年 12 月底止，我國有線寬頻網路用戶數已達 526 萬，經常上網人口為 1,097 萬人（不含無線上網與行動上網人口）[3]。

Contents

參考 Social Media Today 於 2012 年 5 月 9 日所公布的最新調查統計數據，全球網路使用者經常使用的活動有哪些呢？約有 92%的網路使用者經常上網使用 email、其他主要的活動分別為使用搜尋引擎(92%)、健康或醫療資訊(83%)、與興趣相關的資訊(83%)、查詢地圖資訊(82%)、查詢氣象資訊(81%)、蒐集購物資訊(78%)、閱讀新聞(76%)、視聽娛樂(72%)及網路購物(71%)[4]。

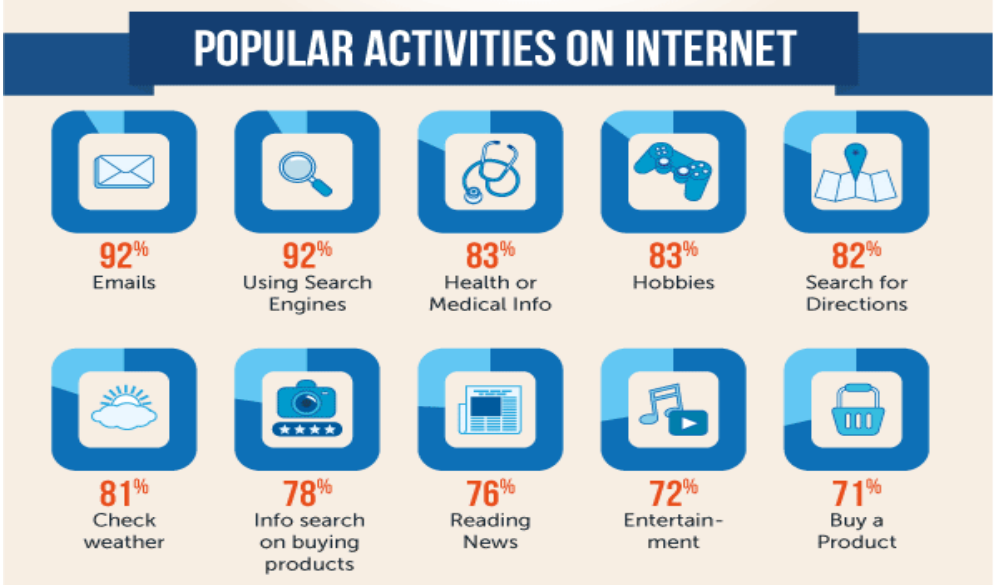


圖2.全球網路使用者經常使用的活動（資料來源：Social Media Today）

從事網路活動的時間分別為：社交網路(social networking)約佔 22%，其次為搜尋(21%)、閱讀內容(20%)、電子郵件或通訊(19%)、瀏覽影音多媒體網站(13%)，以及線上購物(5%)[4]。

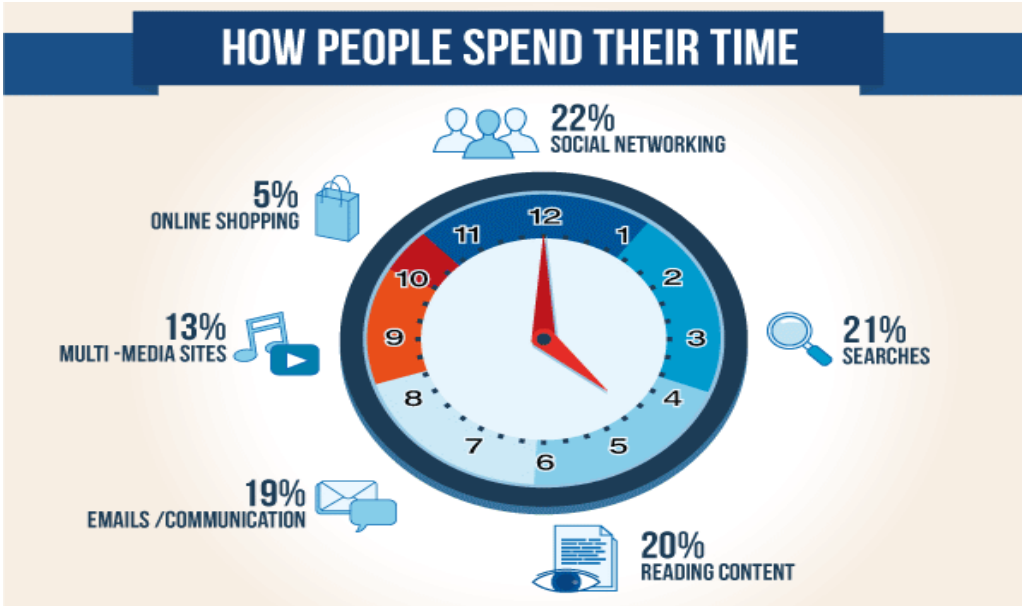


圖3.　網友從事各項活動的上網時間佔比（資料來源：Social Media Today）

從上述的相關數據不難看出，網際網路的使用人口迅速地增加，而民眾也越來越習慣將一些日常生活中的行為轉換至網路上來進行，比方說資料收集、新聞瀏覽、網路購物等。也由於網際網路的蓬勃發展，透過網路進行的詐騙活動也逐漸增加，且以更多樣化的類型與手法進行。

根據國際消費者聯盟 (National Consumers League, NCL)詐欺中心 2011 年網路詐欺統計[5]，名列前 10 名的詐騙類型如表 1 所列。

表1.　國際消費者聯盟 2011 年網路詐欺統計

排名	詐騙類型	排名	詐騙類型
1	網路購物詐騙 (36.12%)	6	網路交友 (2.16%)
2	假支票詐騙 (30.43%)	7	奈及利亞跨國詐騙 (1.60%)
3	免費抽獎和贈品(13.30%)	8	網路拍賣 (1.41%)
4	網路釣魚 (5.67%)	9	假冒親友借款 (0.97%)
5	信用貸款 (4.00%)	10	獎學金詐騙 (0.69%)

資料來源：國際消費者聯盟 (National Consumers League, NCL)詐欺中心

另一份由美國網路犯罪投訴中心 (Internet Crime Complaint Center, IC3) 所做的 2011 網路犯罪報告顯示，美國網路詐騙的投訴案例已經連續三年超過 30 萬件，網路詐騙損失金額估計約 4 億 8,530 萬美金。而最常見的前五大詐騙類型則為：假藉 FBI 名義的相關詐騙、竊取個人資料、預付款項詐騙、已付款但對方卻未交貨的購物詐騙、以及退款轉帳詐騙[6]。

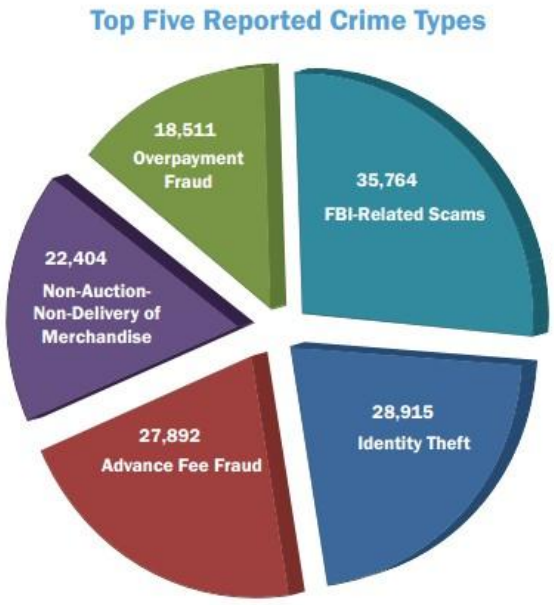


圖4.　2011 年美國最常見的前五大詐騙類型（資料來源：Internet Crime Complaint Center, IC3 ）

根據我國內政部警政署 101 年第 6 號（100 年詐欺案件概況）警政統計通報內容，100 年度詐欺案發生數共計 23,896 件，其中「網路詐欺」類案件有 1,706 件。

表2.　內政部警政署 100 年度詐欺案統計

犯罪方法	發生數				破獲率		0-17 歲被害人			
	本期（件）	結構比（%）	與上年同期比較		本期（件）	與上年同期比較（百分點）	本期（件）	結構比（%）	與上年同期比較	
			增減數（件）	增減率（%）					增減數（件）	增減率（%）
總計	23,896	100.00	- 4,598	- 16.14	75.59	- 11.30	1,124	100.00	272	31.92
電話、手機簡訊詐欺	6,784	28.39	- 1,699	- 20.03	73.19	- 16.71	212	18.86	30	16.48
詐騙款項	4,117	17.23	- 425	- 9.36	91.91	2.50	175	15.57	70	66.67
網路詐欺	4,053	16.96	- 1,706	- 29.62	53.96	- 29.93	408	36.30	129	46.24
假冒名義詐欺	3,391	14.19	- 348	- 9.31	77.50	- 5.86	147	13.08	30	25.64
偽稱買賣	1,797	7.52	- 366	- 16.92	80.36	- 13.26	95	8.45	24	33.80
拒付款項(賴帳)	1,301	5.44	39	3.09	83.70	1.85	25	2.22	4	19.05
詐騙帳號密碼	168	0.70	34	25.37	88.69	43.17	20	1.78	13	185.71
冒(盜)領現金	158	0.66	- 17	- 9.71	46.84	4.55	3	0.27	-	-
虛設行號	115	0.48	- 72	- 38.50	80.00	- 8.77	5	0.44	1	25.00
刊廣告(報章)詐欺	110	0.46	- 105	- 48.84	80.00	- 0.93	3	0.27	-	-
彩金詐欺	58	0.24	20	52.63	65.52	- 18.69	-	-	-	-
其他	1,844	7.72	47	2.62	82.75	- 4.01	31	2.76	- 29	- 48.33

註：1.破獲數含破積案。
2.詐騙款項包括設賭、介紹費、工資、舞資及飲食等。
3.其他類型詐欺主要包括投資詐欺、票據詐欺（空頭）、調包（金光黨）、佯稱代辦貸款、招會詐財、假貨押騙（售）、打工陷阱詐欺等。

資料來源：內政部警政署

而依據 165 全民防騙超連結 2012 年 6 月 4 日公布的最新結果，前 10 大詐騙類型排名如表 3 所列

表3.　165 全民防騙超連結十大詐騙類型統計

排名	詐騙類型	排名	詐騙類型
1	假冒機構（公務員）詐財	6	假投資
2	猜猜我是誰	7	假借個人資料外洩詐財
3	拍賣（購物）詐財	8	假借銀行貸款詐財
4	假推銷	9	假借催討欠款
5	騙取個人資料	10	假求職

資料來源：165 全民防騙超連結

許多詐騙行為在網路出現之前早就已經以多種不同的面貌存在，但是網際網路的發達與其他各種網路活動的盛行，也使得詐騙的類型更為多樣化。本學習手冊將介紹各種常見的網路詐騙管道及類型，包括電子郵件詐騙、網路交友與求職詐騙、網路釣魚詐騙、網路交易詐騙等等，說明這些網路詐騙的特點，並提醒民眾在預防類似詐騙案件應有的警覺；最後將介紹當民眾遇到網路詐騙時之求助方式，以及能夠透過哪些管道進行檢舉與報案。

圖像來源：http://office.microsoft.com/

主題 1. 常見的網路詐騙管道及類型

時有所聞的網路詐騙手法推陳出新，如何才能使自己免於成為這些詐騙行為下的受害者呢？網路詐騙的管道與可能的方式又有哪些呢？本章節將分別從 ❶ 電子郵件、❷ 網路交友與求職、❸ 網路釣魚、以及❹網路交易等四個次主題介紹常見的網路詐騙管道與類型，讓您避免落入詐騙集團的陷阱中。

❶ 電子郵件

根據行政院研考會「100 年個人/家戶數位機會調查報告」中的數據顯示，臺灣網路使用者曾使用的網路應用功能，使用比例最高的為收發 email，將近有九成的比率，可見電子郵件對於網路使用者而言，是一項非常重要且常用的功能，而且電子郵件具有低成本且可大量發送的特性，因此也成為網路詐騙最主要的管道與來源。電子郵件詐騙的類型主要可分為中獎通知、會員服務信件、危險連結等，以下針對各種類型，提供說明與案例參考。

❶-1 中獎通知

詐騙歹徒擅長掌握人性弱點，因此常會以中獎名義做為誘餌，利用網路平台的功能，發送電子郵件或是私人訊息，告知使用者獲得大筆獎金或是高額獎品，如果使用者一時失察，禁不起高額獎金和獎品的誘惑，就可能誤信謊言，成為詐騙歹徒到手的肥羊。

【案例參考】

臺北一名吳姓民眾，在個人電子郵件信箱收到一則中獎通知，信中內容為「恭喜您的 ID 已被抽取為幸運用戶，將獲得本公司送出的驚喜獎品。請您登入活動網站：http://www.xxxxxxxxx.us 領取獎品，驗證碼：【*****】」，壹等獎（PDA 電腦價值 8,800 美金）幸運用戶須辦理保險金，要求前往銀行臨櫃或 ATM 轉帳 5,600 元，至其指定金融帳戶或是前往銀行辦理西聯匯款。」吳姓民眾不疑有他，相信自己幸運中大獎，主動撥打國際電話與對方聯繫，並依據對方指示，前往 ATM 轉帳 5,600 元後，就再也聯繫不上對方，才驚覺是遇上了詐騙。

資料來源：內政部警政署刑事警察局及 165 反詐騙網站

圖像來源：http://office.microsoft.com/

❶-2 會員服務信件

為了使用網站所提供更完整的服務內容，許多網路使用者都會主動註冊加入各種網站的會員，然而這樣的方式，也給了詐騙歹徒一個騙取網路使用者個人資料或是金錢的管道。通常詐騙歹徒會冒用網站管理者身分，向會員們發出通知信件，告知使用者會員帳號資料已過期需重新驗證，或是網站功能更新推出新的服務，請使用者回覆會員帳號和密碼，以便於提供或取消服務。如果使用者不留意，依照信件中的說明回傳帳號和密碼，就會被詐騙歹徒取得自己的資料，而歹徒可以利用取得的資料，登入會員功能頁面取得或修改使用者的註冊個人資料。

資安素養 A to Z

- e-mail spoofing
  欺騙性郵件

欺騙性郵件，主要以偽裝其發送位址為某知名公司、銀行或使用他人郵件位址發送信件，信件內容可能提及回覆個人資料或資料確認，以誘導使用者登入不明網站或回覆提供個人相關的重要資訊，偽裝者可以透過此手法獲得個人資料，以進行入侵個人電腦系統或盜領銀行帳戶等犯罪行為。欺騙性郵件有時也會為垃圾郵件的發送者所使用，引誘收件者打開郵件，以達到垃圾郵件發送的目的。

e-mail spoofing 的相關手法及防範守則，可參考本手冊主題 1 及主題 2 的「❶ 電子郵件」章節說明。

資料來源：i-Security 網站
www.i-security.tw

【案例參考】

寄件者：Google 電子信箱 <pesseea@gmail.com>

主旨：Gmail 信箱(會員)通知書

收件者：xxxxxxx@gmail.com

Gmail 會員您好：

歡迎您使用 Gmail 電子信箱，近年 Gmail 免費電子信箱遭大量濫用，Gmail 會員中心電子信箱服務中心將採收費制度，將可採月繳制及年繳制二種方式。

為重視各位會員使用之各項權利，即日起是否採收費制度及各會員資料重組與確認，將徵求各會員同意與否？為方便各會員回函答覆程序，會員收到 Gmail 會員中心電子信箱服務組寄發信後，填寫下方個人會員資料後，回覆給予 Gmail 會員中心電子信箱服務組確定即可。

不同意採收費制度的會員

Gmail 會員帳號：

Gmail 會員密碼：

同意採收費制度的會員

Gmail 會員帳號：

Gmail 會員密碼：

即日起 Gmail 會員中心將會統計各會員意見，是否收費與其標準，以公告方式告知各位會員。Gmail 會員中心感謝會員長期使用，如有照成不便之處，敬請見諒！

Gmail 會員中心電子信箱服務中心敬上

收件人若未提高警覺，依照寄件者的指示回信，
有心人士就能輕易地取得您的 email 帳號密碼

圖像來源：http://office.microsoft.com/

❶-3　危險連結

所謂的社交工程(Social Engineering)是以運用擬真並極具吸引力的方式，欺騙他人以獲得有用資訊的電子郵件中的危險連結，通常都會搭配一些目前最熱門的新聞時事或是特定假日、流行潮流等，例如：日本 311 大地震、世足賽、知名人士的死訊、耶誕假期、報稅季節、好萊塢熱門電影……等，詐騙歹徒藉由網路使用者的好奇心，可能會寄給你外表看起來很正常又很專業的電子郵件，信中告訴你必須點選某個超連結或下載附加檔案即可瀏覽相關內容，一旦你點選了超連結或下載檔案，惡意程式便會在你不自覺的情況下下載並安裝在你的電腦中。該惡意程式可能會偷取你在電腦中儲存的個人資料，或是側錄你在上網時所輸入的帳號與密碼，並透過網路把這些資訊傳送出去，歹徒即可利用這些個人資料來假冒你的身分，從事不法行為，例如假借你的名義濫發垃圾郵件，甚至破壞你的電腦設備。

圖像來源：http://office.microsoft.com/

【案例參考】

美國國土安全部（Department of Homeland Security）網路安全部門宣布，歹徒試圖利用巨星麥可傑克森過世的消息，發出垃圾郵件、釣魚攻擊和惡意程式進行詐騙。

該單位操作部門電腦安全緊急應變小組表示，這些電子郵件可能會以釣魚攻擊方式騙取網友的個人資料，或者含有惡意程式，或是連線到看似合法但含有惡意程式的網站。

此緊急應變小組亦呼籲網友在打開垃圾郵件時務必謹慎，且須確定防毒軟體已更新。

資料來源：中央社，2009 年 6 月 27 日

❷ 網路交友與求職

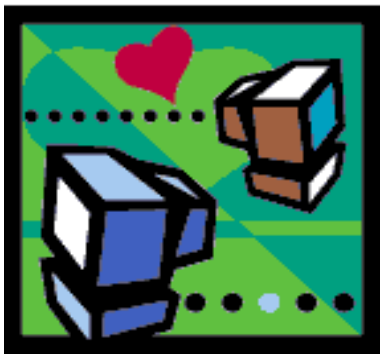
由於網路的普及與便利，愈來愈多人開始在網路上尋找朋友，相較於實體世界，在網際網路的國度中，更是容易結交彼此志同道合的朋友。網路上的溝通使得原本因陌生而產生的尷尬幾乎消失，也因訊息快速的傳遞縮短了有形、無形的距離。但是我們怎麼能夠瞭解在網路上和我們對話的人究竟是個什麼樣的人呢？是真心想要交朋友，還是打著交友的幌子行詐騙之實？因為網路交友而造成生命與金錢損失的新聞層出不窮，民眾實應提高注意，不要再誤入有心人士的圈套中。另外，網路發達的現代社會，民眾透過求職網站刊登履歷，也容易成為詐騙集團下手的目標。以下針對網路交友與求職時常見的詐騙類型，提供說明與案例參考。

圖像來源：http://office.microsoft.com/

❷-1 網路聊天室

詐騙歹徒利用網路無遠弗屆且難以查證的特性，看準宅男熟女渴求感情依靠的弱點，通常都先冒用帥哥美女的照片當作自己的個人照片，在網路聊天室出沒以物色詐騙對象。由於網路聊天室使用匿名交友，可以肆無忌憚地情意綿綿，也不需要對說的話負責，所以容易短時間就建立浪漫的情誼，網路的距離感、神秘感，以及存在想像空間，也讓人容易進入美麗和幻想的空間。

詐騙歹徒通常在與受害人建立一定的情感和信任之後，開始以各種理由向被害人提出金錢的需求，包括家中突然發生緊急情況急需用錢，或是利誘參與高報酬投資或邀約進行投機取巧中獎操作，以遂行詐騙。也有心懷不軌的人透過網路聊天室誘騙少女外出見面，然後進行援交或是奪取性命的社會案件發生。網路只是擴展交友圈的管道之一，無論如何網路戀情還是要回歸現實面，並謹慎防範網路詐騙，注意自身的安全。



圖像來源：http://office.microsoft.com/

【案例參考】

香港商人在網路聊天室認識自稱住在臺中市的女大學生「小可」，雙方相談甚歡、進一步互留電話。但小可突然接連多日未上線且失聯，港商心急如焚，連續多天嘗試上線後終於聯絡上，小可聲稱母親生病住院無心上網，且因心情不佳而關機。

港商得知後，立即表明要前往探視小可母親，隔天從香港搭機來台，渾然不知已掉入詐騙集團的陷阱；抵台後撥打手機給小可，小可在電話中聲淚俱下，誆稱母親癌症病情加重、已轉至臺北大醫院就醫，但特殊藥物很昂貴，需要籌措一筆龐大的醫藥費，不知如何是好。

港商同情小可遭遇，隨即詢問如何幫忙，小可留下帳號請港商至銀行存款機存款，日後有錢再歸還；港商不疑有他，馬上拿出 5 萬港幣兌換成台幣存入後，小可卻自此失聯，港商此時才驚覺遭騙而報警。

資料來源：自由時報，2012 年 6 月 3 日

❷-2　社群網站（Facebook、部落格）

1967 年心理學家史坦利．米爾格倫 (Stanley Milgram)研究提出「六度分隔理論」，也就是指世界上每 2 個陌生人，平均只要和 6 個人連繫就能連上關係，但是近年來社群網站的興起，尤其是 Facebook 的異軍突起，已經打破了「六度分隔理論」，經統計 Facebook 上的使用者，任何 2 個不同網絡的人，平均只要與 4.74 個人鏈結就能扯上關係，我們可以透過朋友的朋友，將彼此的關係線串連起來。而根據統計，至 2012 年 5 月底為止臺灣使用 Facebook 的人數已經將近 1,200 萬人，超越了其他社群網站和部落格的使用人數，也成為企業或是廣告最主要的行銷管道，當然網路詐騙歹徒也不會放過這個網路使用者這麼活躍的地方，網路詐騙也在透過 Facebook 使用者間的彼此分享散播出去。

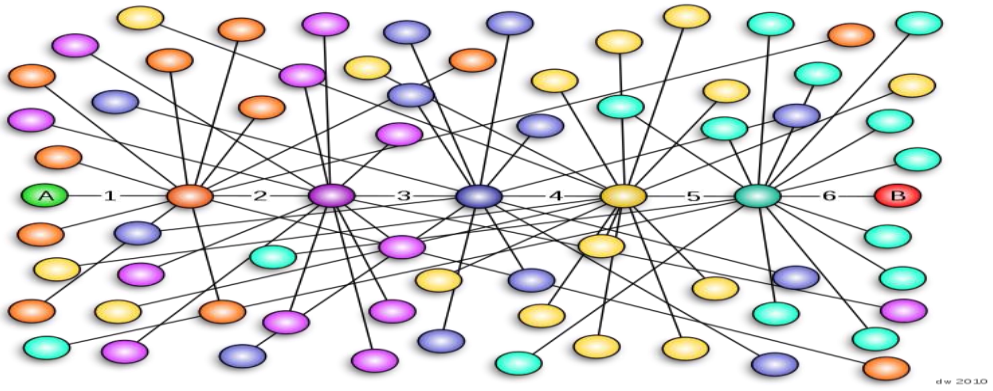


圖5.　六度分隔理論示意圖（圖像來源：http://en.wikipedia.org/）

【案例參考】

Facebook 使用者在塗鴉牆上瘋狂分享一則以「免費取得 Costco 禮物卡！（限時優惠）」標題的訊息連結，從圖 6 可看到這訊息還附有一張 Costco 現金卡的圖示，訊息表示「Costco 現正向所有 Facebook 用戶免費送出 100 元禮物卡！」，宣稱只要分享網頁的連結，並且留言，將可得到一張 Costco 價值 100 美元的禮物卡，許多網友認為撿到好康了，順手按了一個讚，然後系統要求使用者主動與所有 Facebook 友人分享這連結，之後用戶會收到已贏得這禮物卡的通知，並要求用戶填寫一份網上問卷，但事實上用戶永遠不會看到「已贏得」的獎品，而這則訊息經過證實也並非 Costco 官方發出，歹徒目的是為了要收集使用者的個人資料，並為某些網站帶來更多訪客。詐騙歹徒獲利的途徑主要是來自每份完成的問卷、每項購買的物品，以及每個被盜取資料的戶口所獲得的佣金歹徒並利用這些途徑來散發電腦病毒並盜取個人資料

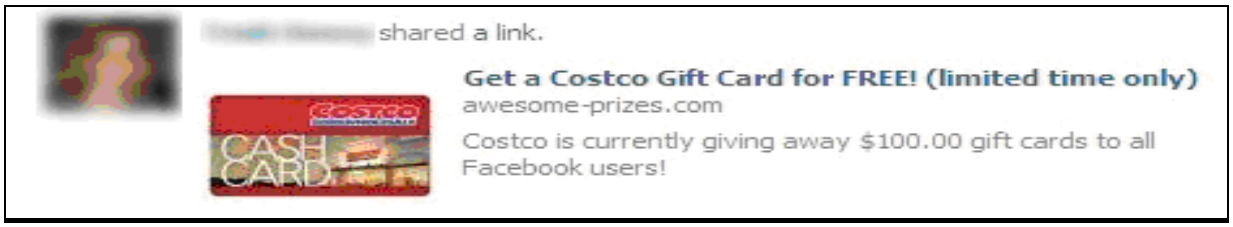


圖6.　Facebook 塗鴉牆詐騙案例（圖像來源：facebook）

❷-3　盜用通訊軟體帳號

常見的通訊軟體有微軟的 MSN、Yahoo 的即時通……等等，這些應用程式可以讓線上的使用者透過平台進行聊天對話，通常即時通訊軟體上都有一大串聯絡人的清單，詐騙歹徒會利用竊來的帳號和密碼登入上線，以往的詐騙手法通常是在離線狀態下，傳送一則內含奇怪網址的訊息給通訊軟體中的聯絡人，一旦不小心點選了，可能就會造成使用者的電腦被植入木馬程式，再藉以竊取或側錄使用者在網站上輸入的帳號密碼，或是成為發送病毒攻擊的跳板。而前陣子透過通訊軟體帳號進行的詐騙則是假冒親友發送訊息，要求幫忙購買遊戲點數的詐騙案件，造成被害人金錢上的損失。

圖像來源：http://office.microsoft.com/

【案例參考】

臺南縣汪小姐在家中上網，突然收到來自加拿大，已認識 8 年的大學同學「密她」，說在學校不方便出去，請他幫忙去超商買遊戲點數，再將密碼用即時通傳給他，久未見面的同學再度連絡，她感到特別開心，因此毫不猶豫的買了一張 3,000 元的點數卡，後來同學又說不夠，她再度去超商，共買了 32 張點數卡，花了 7 萬元。次日，她收到同學的留言，才知道同學的 MSN 帳號被盜用，且帳號、密碼都被修改，已經完全無法登入使用，造成歹徒趁此詐取遊戲點數，只是同學的通知還是晚了一步。

臺北市陳小姐也是上網遇到歹徒假冒的朋友，讓她先買了 5 張 1,000 元的點數卡，歹徒以第一次的要求做試探，見她並未警覺異狀，便再度提出要求，但第二次的購買張數與金額都增加許多，當歹徒要求再買 15 張點數卡時，她曾問朋友要如何拿錢給她，對方就要了她的銀行帳號，說次日即可將錢匯入帳戶內，她花了 2 萬元。2 小時後，她接到朋友電話，說好友在「臉書」留言版提到帳戶遭盜用，只是這也是遲來的通知，因為她已將遊戲點數密碼告訴歹徒，無法挽回被騙損失。

圖像來源：http://office.microsoft.com/

資料來源：內政部警政署刑事警察局，2010 年 5 月 24 日

❷-4 網路求職

過去詐騙集團多以透過報紙徵才廣告吸引求職者上門，再以辦理薪資轉帳之名義，誘騙被害人交付存摺、提款卡並告知密碼，使被害人帳號淪為詐騙人頭帳戶。而今網路發達，民眾上網至人力銀行刊登求職履歷，詐騙集團只要以虛設的公司行號名義取得企業帳號登入，即可透過人力銀行每天寄發的履歷配對隨機挑選詐騙對象，或是在網站上刊登職缺，等候主動投遞履歷的求職者上門，然後藉由面試邀約的名義進行詐騙

圖像來源：http://office.microsoft.com/

【案例參考】

張姓男子等人組成詐騙集團，先在求職網站上假冒美國「拉斯維加斯威尼斯飯店」、「奧蘭多海洋公園」名義刊登徵才廣告，招募「園區中文導覽解說員」、「公關人員」、「中式餐飲服務助理」等工作。吸引許多不知情且懷抱前往美國工作夢想的大陸民眾上網應徵工作填寫履歷後，便由詐騙集團成員分別扮演第一線管理部專員，對求職者進行簡單的訪談並安排面試。

詐騙集團假冒「美國金沙集團亞洲區人事部經理」向求職者謊稱通過面試，並以該公司需先負擔求職者機票、簽證、住宿等費用，為預防求職者抱持遊玩心態或藉此機會出國，造成公司損失等理由，請求職者準備護照，而且帳戶內需有 40 萬人民幣額度的財力證明，同時要辦理 U 盾（用以識別使用者身分的電子憑證）及網路轉帳，方便領取公司薪資。

當求職者依照指示插入 U 盾並進入該公司提供的「假官網」網頁進行驗證，打開驗證程式時，已遭植入木馬程式，歹徒便從遠端網路透過轉帳功能將求職者帳戶內的金錢轉出並提領一空。

詐騙對象為大陸地區民眾，被害人多半有高學歷、英語能力佳，懷有美國夢的年輕男女，粗估該集團詐騙至少獲利新台幣 1,000 萬元以上。

資料來源：中央社，2012 年 5 月 9 日

❸ 網路釣魚

網路釣魚 (phishing)通常是一種誘騙電腦使用者透過電子郵件訊息或網站提供個人或財務資訊的手段。一般詐騙集團使用網路釣魚的誘騙手段都是從電子郵件訊息開始，假冒知名單位，如銀行、信用卡公司或聲譽良好的線上商家，或是用類似的網址發出看似正式的通知。在電子郵件訊息中，收件者會被引導至詐騙網站，並在其中被要求提供個人資訊，再透過核對資料的過程中竊取使用者的個人資料與密碼，然後用此資訊來進行身分盜用。

❸-1 使用與官網相似的網址與頁面

通常詐騙集團仿冒知名公司網站，架設神似的假網頁，然後用垃圾郵件或即時通訊發送連結，告知網站服務更新或是使用者資料更正等通知，要求網路使用者點選信件中的網址連結，進行個人資料更新，當您按下該連結後，您將會被轉介至一個與銀行網頁設計極為相似之網站，其實詐騙集團就是透過這樣的方式盜取使用者的帳號密碼，再利用這些資料獲取不當利益。
之前曾有詐騙集團利用作業系統的漏洞，偽造相似的銀行網站（如圖 7 及圖 8 所示）如果使用者沒有仔細對照，很容易在沒有察覺的情況下，就輸入帳號密碼登入頁面，卻不知個人資料已經在不知不覺中被詐騙集團所側錄擷取了！

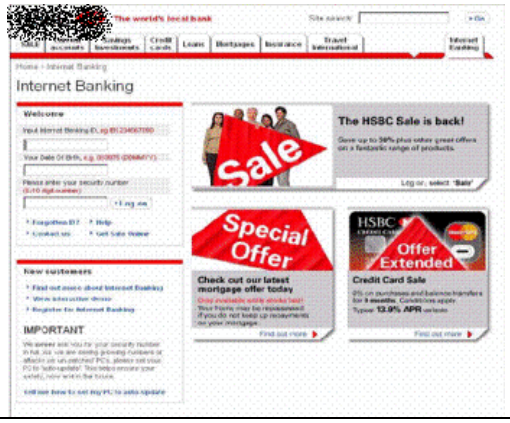


圖7. 詐騙集團偽造某銀行的釣魚網頁（假網頁）
（圖像來源：ettoday 新聞）

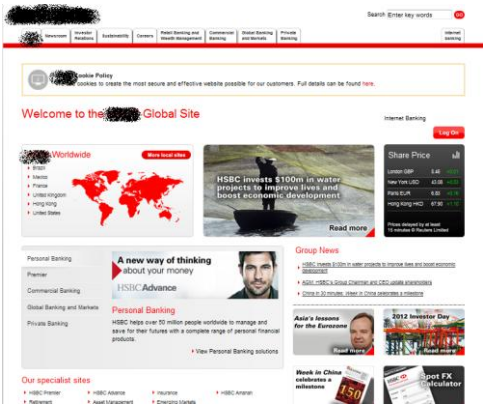


圖8. 左圖銀行的官方網頁（真網頁）
（圖像來源：http://www.hsbc.com）

【案例參考】

玩家們引頸期待十年的動作角色扮演遊戲《暗黑破壞神 3》，一開賣便引發搶購，更發生遊戲人數過多，無法登入亞洲伺服器的狀況。同時許多玩家紛紛試圖從網路下載遊戲，「diablo 3」成為網路搜尋熱門關鍵字。然而愈熱門的話題，愈容易被駭客所利用，目前已有資訊安全廠商發現，駭客利用暗黑 3 來騙取使用者個人資訊的情形。

以關鍵字串「diablo 3 free download （暗黑破壞神 3 免費下載）」進行搜尋，可發現近九千筆相關網址，趨勢科技發現，目前至少已有兩個排行較為前面的搜尋結果被駭客黑帽化，植入詐騙問卷調查頁面。

一旦點選此網址後，會被引導至一個看似暗黑破壞神 3 的下載頁面，點選下載鈕將被導往特定的問卷網頁。進入網站後，網友將被要求按照網頁指示下載暗黑破壞神 3。然而在下載過程中，該網頁會強迫網友分享連結於 Facebook 個人頁面，即便網友完成所有程序，仍無法成功下載免費版暗黑破壞神 3，反而被導向另一個不知名的問卷網頁。

資料來源：中時電子報，2012 年 5 月 24 日

圖9. 點選左圖的免費下載網頁後將導向右圖的問卷網頁，誘騙使用者填寫個資
（圖像來源：趨勢科技網頁）

【案例參考】

臺北林小姐於 6 月 30 日下午收到黎姓友人傳來的即時通訊息，訊息中提供一個網址連結，請林小姐瀏覽部落格衝人氣，林小姐點選連結後，隨即跳出一個與微軟官方網站非常相似的網頁，上面已有林小姐的即時通帳號，僅要求輸入密碼，林小姐以為是網路不穩定自動登出，未有質疑即輸入密碼，但網頁卻顯示密碼錯誤，林小姐此時開始起疑，因此再點選一次該連結，出現的依舊是該疑似官方網站，而非朋友所稱的部落格，但因當時即時通依然可以使用，便未有進一步處理。翌日一早林小姐發現，黎姓友人在臉書上發布自己的即時通帳號密碼遭盜，沒多久林小姐的即時通亦被登出且無法登入，而林小姐的朋友則陸續接到冒用訊息，要求協助購買 1 千至 2 千元不等的大陸手機儲值卡。其中有朋友已透過大陸同事代買並將帳號密碼提供給對方，幸而林小姐即時提醒，請大陸友人搶在歹徒之前立即兌換儲值卡，而免於損失。

資料來源：中央社，2011 年 7 月 10 日

❸-2　網路抽獎廣告連結

網路上有各式各樣的廣告，不管它看起來有多漂亮、多吸引人，或是看起來很像是一個合法的活動，只要是點入後跳出請你輸入個人資料的網頁，都請不要輕易輸入你的資料。通常這類的連結都是以抽獎為名義，跳出一個視窗告訴網路使用者獲得樂透獎金、3G 智慧型手機，甚至是綠卡申請機會，這都是詐騙集團或行銷公司利用網路使用者貪小便宜的弱點，一旦使用者點選了這些廣告，將會連結到其他的網址，可能會請你填寫個人資料，或是輸入手機號碼，之後就會接到詐騙集團的電話要求支付相關申請費用，或是每個月的手機電話費帳單莫名多出了簡訊傳送費用。

【案例參考】

美國每年提供 5 萬名移民名額，讓符合條件的民眾參加抽籤。然而卻有詐騙集團假冒美國國務院名義，以電子郵件謊稱民眾抽中，詐騙高額手續費，美國在台協會特別發出聲明，提醒民眾千萬不要上當；AIT 發言人表示，美國每年提供 5 萬張移民簽證，給包括台灣在內符合條件的各國人士抽籤，過程完全免費，也不需透過他人協助，只有真正抽到、需到 AIT 面試時才需付費。

許多詐騙網站冒充美國政府網站，謊稱須先付錢，以便「完成」抽籤移民簽證登記表格。AIT 表示，負責抽籤移民的肯塔基領事中心不會收取抽籤移民任何費用，且一律以「郵寄信件」通知中籤者，絕不會以 email 通知，並會提供如何進行下一步的相關程序；美國政府也沒有授權任何其他機構或公司通知中選的抽籤移民申請人。

資料來源：大紀元，2011 年 2 月 24 日

圖10.　美國在台協會公告的「抽籤移民簽證詐騙警告」（圖像來源：http://www.ait.org.tw）

❹　網路交易

相對於傳統的購物環境，透過網路交易帶給了消費者的好處包括：更多的選擇、更多產品資訊、較低的價格及隨時隨地可向全球的網路商店進行購物，透過網際網路，消費者不需出門，便可向全世界的電子商務業者購買各式各樣的商品及服務。但也由於網路交易無法親眼看見摸到想要購買的商品，也不像傳統購物一樣屬於一手交錢一手交貨銀貨兩訖的交易方式，因此也被詐騙歹徒利用來作為騙取網路使用者金錢的管道。以下針對網路交易時常見的詐騙類型，提供說明與案例參考。

❹-1　網路拍賣

在拍賣網站上，不法人士會以低於市價行情的價格販售高單價商品，如：最新款智慧型手機、平板電腦、筆記型電腦，或是最新上市且很難買得到的限量款球鞋，以及一票難求的入場券等，讓受害者以為撿到便宜，開心地下標購買並完成轉帳匯款，結果非但沒有收到商品，賣方也不知去向，又或者是收到的商品根本就是個山寨版的冒牌貨。

【案例參考】

西洋流行樂壇天后 Lady Gaga 世界巡迴演唱會於臺北演出時，演唱會門票售價從 1,800 元至 1 萬 2,800 元不等，堪稱價值不斐，因此低價位門票很早就銷售一空，許多粉絲為一親偶像芳澤，不惜透過網路拍賣另覓門票，

被害人蔡小姐在拍賣網站找到一位賣家，聲稱有演唱會 1,800 元門票 6 張，每張含運費要價 2,300 元，雖然比官方售票定價貴了些許，但剛好符合一群朋友共 6 人隨行的需求，因此被害人隨即下訂該 6 張門票，並於結標後依賣家指示匯款 1 萬 3,800 元，惟遲遲未收到門票，被害人起疑上網查詢才發現賣家已被停權，始知上當受騙，向警察機關報案。

資料來源：NOWnews，2012 年 5 月 14 日

❹-2 網路購物

網路購物的詐騙方式，通常為詐騙集團以駭客入侵方式進入購物網站平台與賣家的訂單或出貨系統，竊取買家個人資料與交易明細資料，再假冒平台或商家客服人員以電話聯絡，聲稱因刷卡時誤勾選為分期付款，將會造成被害人銀行帳戶每月被自動扣款，營造出讓被害人擔心錢財不保之情境，誘騙被害人至 ATM 解除分期付款設定。被害人因擔心財物損失，且又不知如何操作提款機，一邊以手機聽從歹徒指示、一邊按鍵，輸入所謂的代碼，該代碼其實是「匯款金額」與「歹徒帳號」，直到轉帳交易成功，帳戶內的存款被轉走，才發現被騙。

圖像來源：http://office.microsoft.com/

資安素養 A to Z

- pharming 網址轉嫁

網路犯罪集團所利用的網路釣魚手法之一。在網路使用者瀏覽網站時，利用修改 DNS（域名系統）的技術，改變使用者欲連接的網站位址，將使用者連接到假的網站，引誘使用者瀏覽假的網站並進一步進行犯罪行為。

有關釣魚網站的相關手法及防範守則，可參考本手冊主題 1 及主題 2 的「❸ 網路釣魚」章節說明。

資料來源：i-Security 網站 www.i-security.tw

【案例參考】

苗栗縣李小姐上網購買一個 1,500 元的電腦桌後，於 12 月初接到網路商家來電告知，因公司員工作業程序出錯，致使李女信用卡誤設分期付款，將按月扣款。隨後李女接到自稱銀行客服人員來電，並聽從指示外出至 ATM 轉帳匯出兩筆金額共計 4 萬餘元。惟後李女立刻發現帳戶存款減少並提出質疑，對方辯解此係李女操作錯誤所致，且已造成其個人金融帳戶無法關閉，相關財資恐有公諸於網路而遭駭客盜取之虞，請她將存款轉帳至中華郵政公司之公正帳戶以供監管，李女遂陸續轉匯了 15 萬元至歹徒人頭帳戶。

翌日歹徒假冒中華郵政員工致電李女，聲稱她的帳戶財資仍無法關閉，公司已轉請金融監督管理委員會尋求解決之道，但金管會看了帳號紀錄資訊，懷疑李女有作內線交易，要凍結申報她的帳戶，請她領取 420 萬元交付，作為金融保險。李女依照指示分兩次提領現金 220 萬及 200 萬元，於住家附近面交給假冒法務部書記官之歹徒。之後李女愈想愈覺怪異，經打電話詢問銀行，始驚覺自己被詐騙了 439 萬餘元！

資料來源：內政部警政署刑事警察局，2012 年 1 月 3 日

❹-3　網路投資（股票、博奕）

網路投資詐騙的類型通常會結合網路交友的模式，詐騙歹徒通常都會先在網路聊天室或是相關的部落格網站發表專業的理財投資文章，先建立與受害者之間的信賴，或是以貌美的照片博取異性網友好感，藉網路傳情建立感情基礎，然後利用對方的信任，佯稱有親友是網路博奕活動的操盤者，假藉共同投資理財、一圓夢想的溫情攻勢，讓受害者往往無法抵擋投資的盛情邀約，不知不覺掉進詐騙歹徒的陷阱中。

【案例參考】

蔡姓男子以不同暱稱，在一些理財網站、部格格或網站聊天室，宣稱可代客買賣期貨商品，客戶只要先把網路下單密碼及期貨電子交易帳號、憑證交給他即可，事先不用支付任何費用，一旦獲利，才會從中抽取佣金，由於事先不需交付任何金錢，不少網友因此委託其代為買賣期貨商品。

但蔡騙取網友的交易帳號、密碼後，故意選擇一些不活絡期貨商品作為交易標的，以自己的期貨交易帳號低買高賣、被害人的期貨交易帳號高買低賣方式來對沖交易期貨商品，造成自己賺到錢，被害人卻因而虧損的情況，等被害人察覺自己帳戶虧損時，因不知對方真實身分，無法聯絡到對方，致求償無門。短短半年內詐得 2 百多萬元，至少有 20 位網友受害。

資料來源：自由時報，2012 年 3 月 27 日

主題 2. 避免網路詐騙防範守則

在主題 1 當中，我們已向各位讀者介紹了常見的網路詐騙管道及類型，因應目前眾多的網路詐騙手法，民眾應該以何種方式來防範與因應呢？本節內容將從操作面與實務面來說明一般應具備之基本認知及防範措施，避免民眾遭遇網路詐騙事件，並降低損害的發生。

❶ 電子郵件

透過電子郵件進行網路詐騙行為，多數為有心人士假冒或偽裝身分，以友善、誘惑的內容誘騙民眾上勾受騙，藉由設下電子郵件攻擊的陷阱，如夾帶惡意程式執行檔、內文中的惡意網頁超連結、HTML 郵件隱藏遠端下載…等。為此，提供民眾面臨電子郵件詐騙事件之基本防範措施如下：

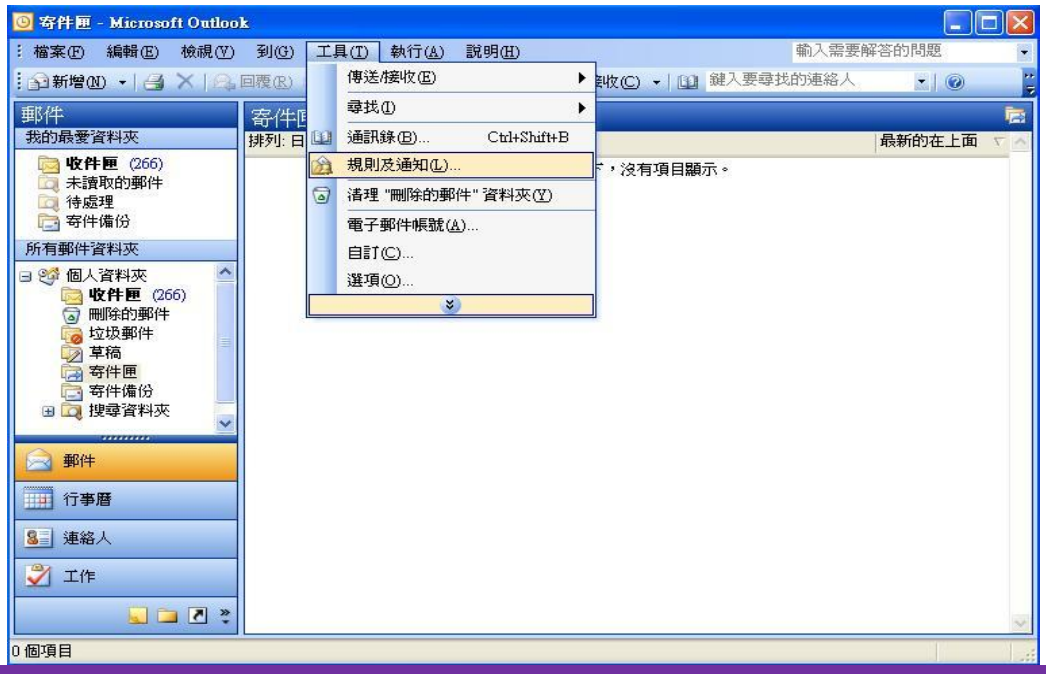
❶-1 設定阻絕垃圾郵件

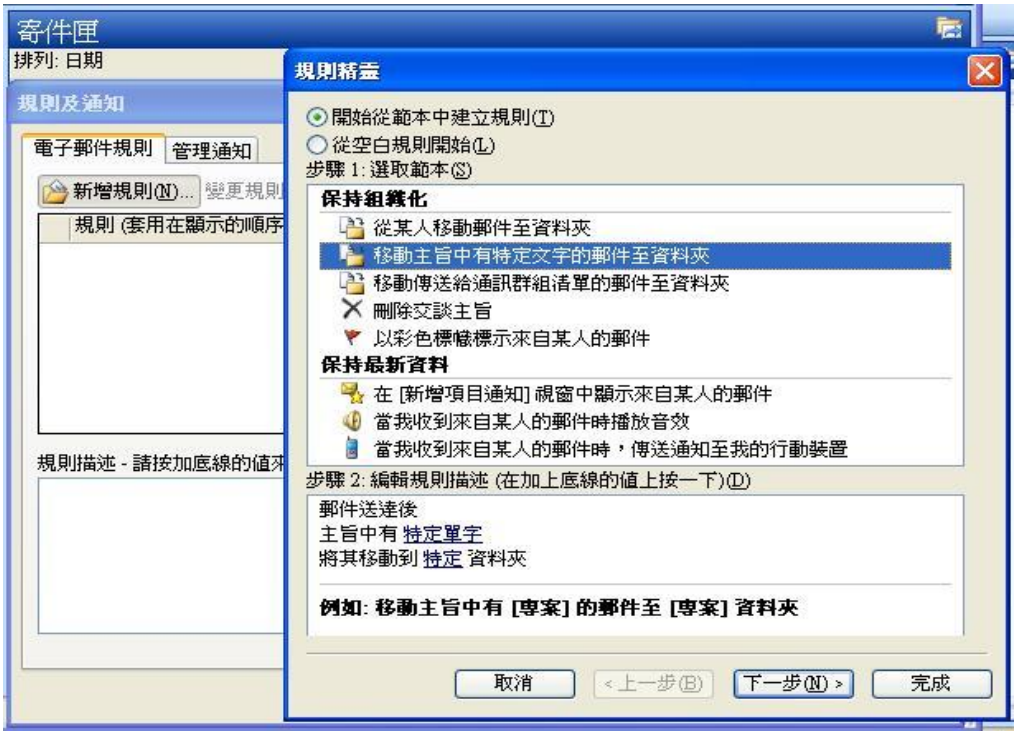
目前大多數的郵件軟體或是網頁郵件 (Webmail)，都已有相關的設定功能，只要稍加設定就能夠減少大部分的垃圾郵件，甚至系統可以主動為您將疑似垃圾郵件的信件予以隔離，再由使用者主動檢視確認是否為垃圾郵件後再行刪除。

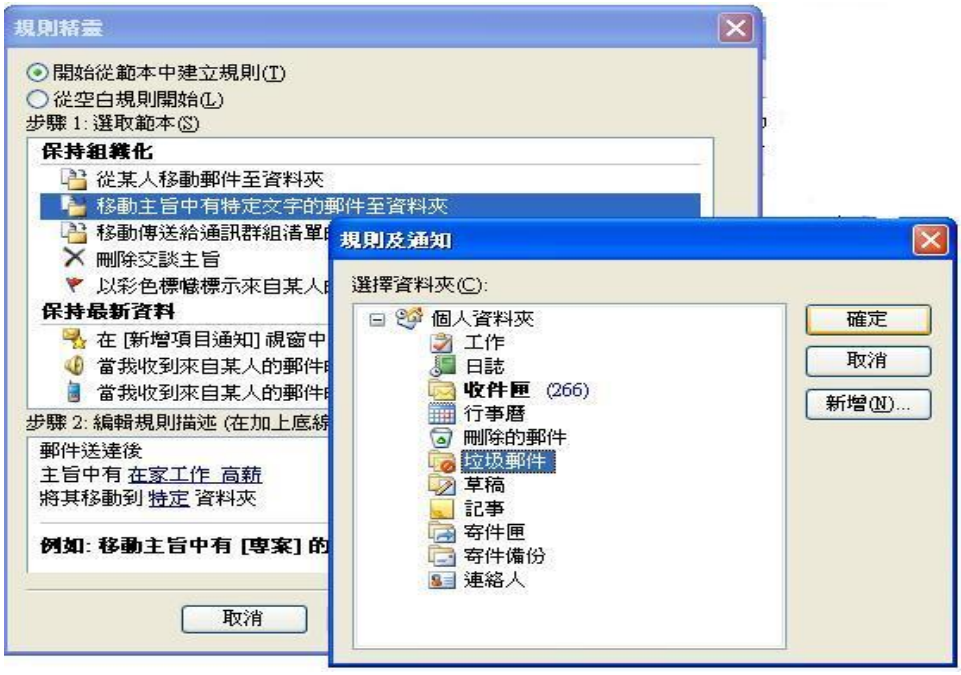
有關垃圾郵件的阻絕設定，以下使用常見的郵件軟體 Outlook 及 Outlook Express 分別進行說明：

(1) 以 Outlook 設定為例（註：不同版本的 Outlook 選單的位置可能會不同）：

- 選取【工具】/【規則及通知】/【規則精靈】
- 設定相關的郵件規則或是關鍵字，將含有此規則或關鍵字的信件移至【垃圾郵件】資料夾

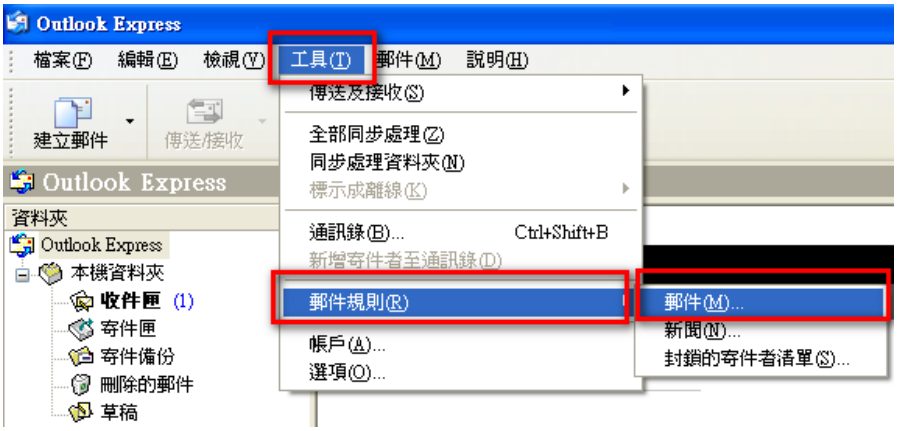


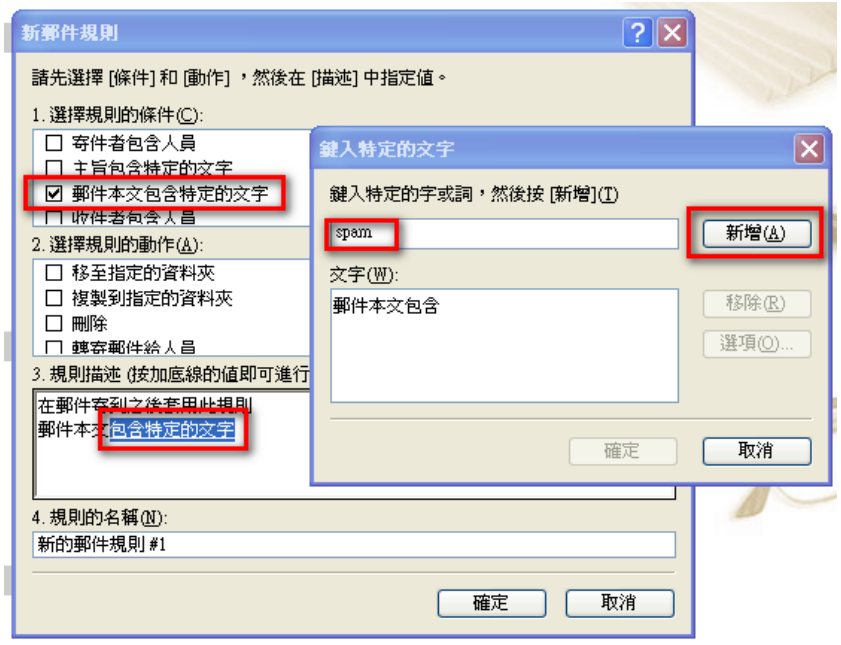


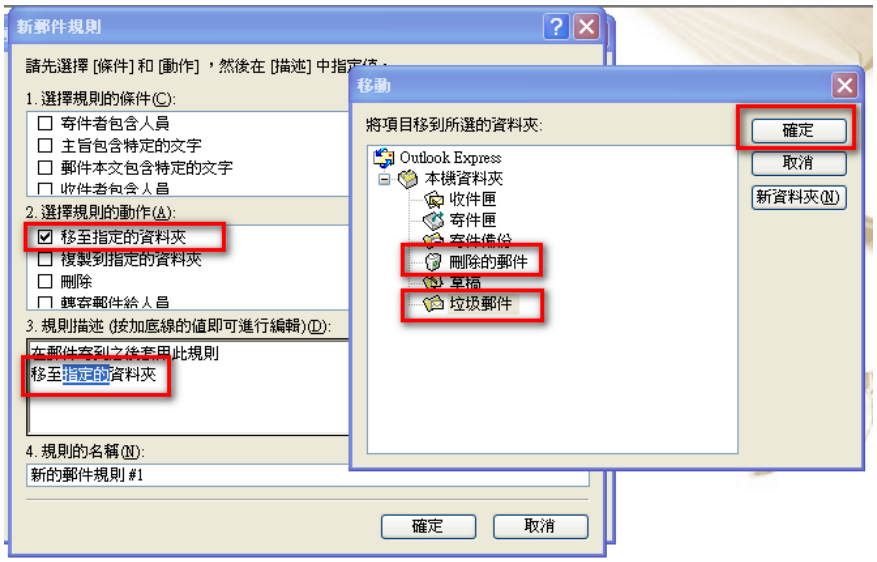


(2) 以 Outlook Express 設定為例：

- 選取【工具】/【郵件規則】/【郵件】
- 設定相關的郵件規則或是關鍵字勾選【郵件本文包含特定的文字】/ 點選設定【鍵入特定的文字】/ 按下【新增】
- 將含有此規則或關鍵字的信件移至特定資料夾勾選【移至指定的資料夾】/ 點選設定設定【特定的資料夾】（如：刪除的郵件或垃圾郵件）/ 按下【新增】


Outlook Express
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
建立郵件
傳送/接收
傳送及接收(S)
全部同步處理(Z)
同步處理資料夾(N)
標示成離線(K)
通訊錄(B)... Ctrl+Shift+B
新增寄件者至通訊錄(D)
郵件規則(R)
帳戶(A)...
選項(O)...
郵件(M)...
新聞(N)...
封鎖的寄件者清單(S)...
資料夾
Outlook Express
本機資料夾
收件匣 (1)
寄件匣
寄件備份
刪除的郵件
草稿


新郵件規則
請先選擇 [條件] 和 [動作]，然後在 [描述] 中指定值。
1. 選擇規則的條件(C):
寄件者包含人員
主旨包含特定的文字
郵件本文包含特定的文字
2. 選擇規則的動作(A):
移至指定的資料夾
複製到指定的資料夾
刪除
3. 規則描述 (按加底線的值即可進行
在郵件寄到之後套用此規則
郵件本文包含特定的文字
4. 規則的名稱(N):
新的郵件規則 #1
確定
取消
鍵入特定的文字
鍵入特定的字或詞，然後按 [新增](T)
spam
新增(A)
文字(W):
郵件本文包含
移除(R)
選項(O)...
確定
取消


新郵件規則
請先選擇 [條件] 和 [動作]，然後在 [描述] 中指定值。
1. 選擇規則的條件(C):
寄件者包含人員
主旨包含特定的文字
郵件本文包含特定的文字
2. 選擇規則的動作(A):
移至指定的資料夾
複製到指定的資料夾
刪除
3. 規則描述 (按加底線的值即可進行編輯)(D):
在郵件寄到之後套用此規則
移至指定的資料夾
4. 規則的名稱(N):
新的郵件規則 #1
確定
取消
移動
將項目移到所選的資料夾:
Outlook Express
本機資料夾
收件匣
寄件匣
寄件備份
刪除的郵件
草稿
垃圾郵件
確定
取消
新資料夾(N)

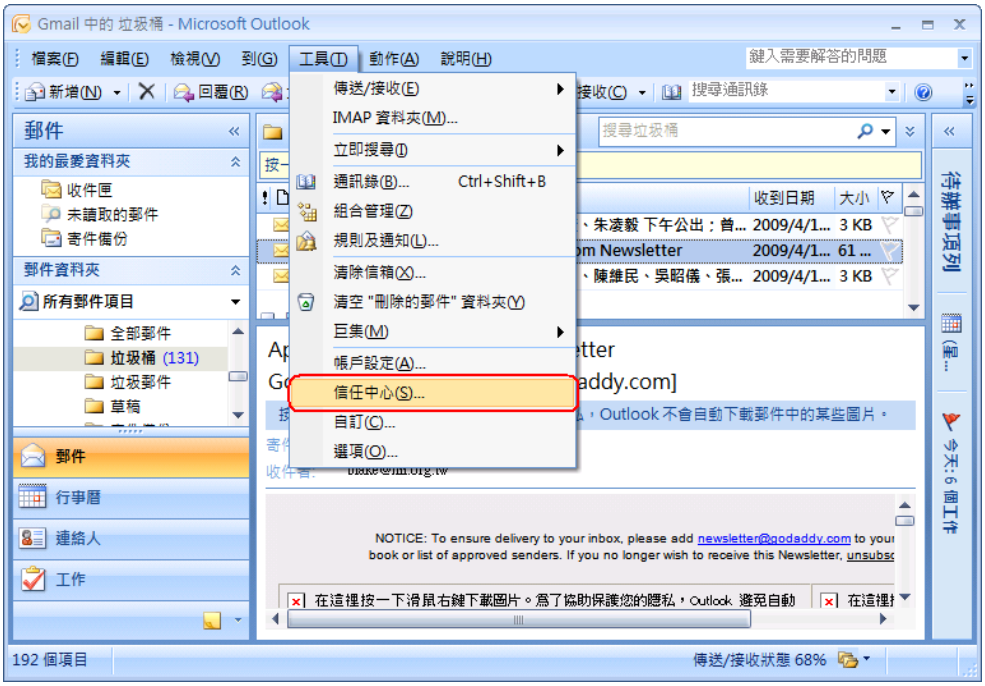
❶-2　關閉自動下載圖片

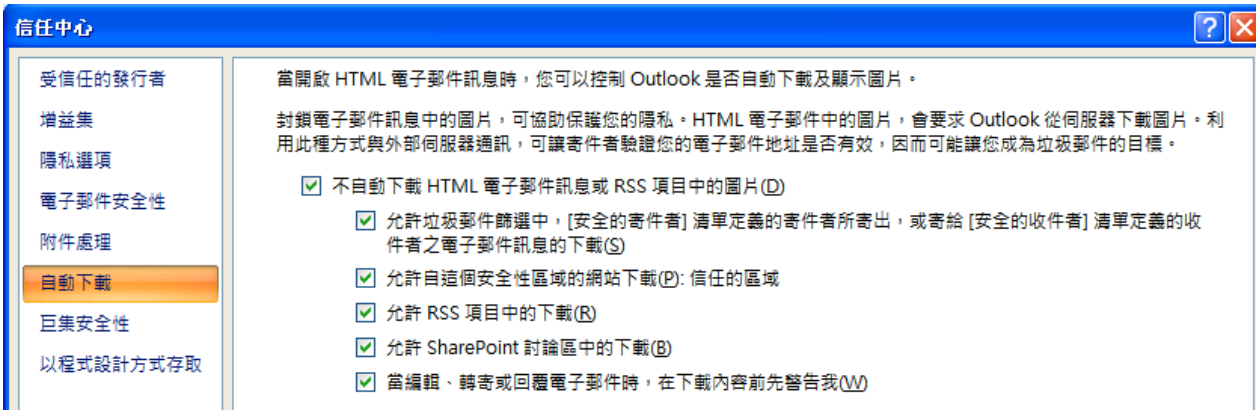
隨著 HTML 格式電子郵件的普遍，電子郵件的內容也日趨多樣化，但也給了病毒透過電子郵件來傳播的機會，最安全的方法就是將電子郵件的檢視設為純文字，但它會讓電子郵件的檢視失去了多采多姿的內容，較為折衷的方式就是關閉圖片自動下載功能。

關閉圖片自動下載的功能設定，以下使用常見的郵件軟體 Outlook 及 Outlook Express 來分別進行說明：

(1) 以 Outlook 設定為例（註：不同版本的 Outlook 選單的位置可能會不同）：

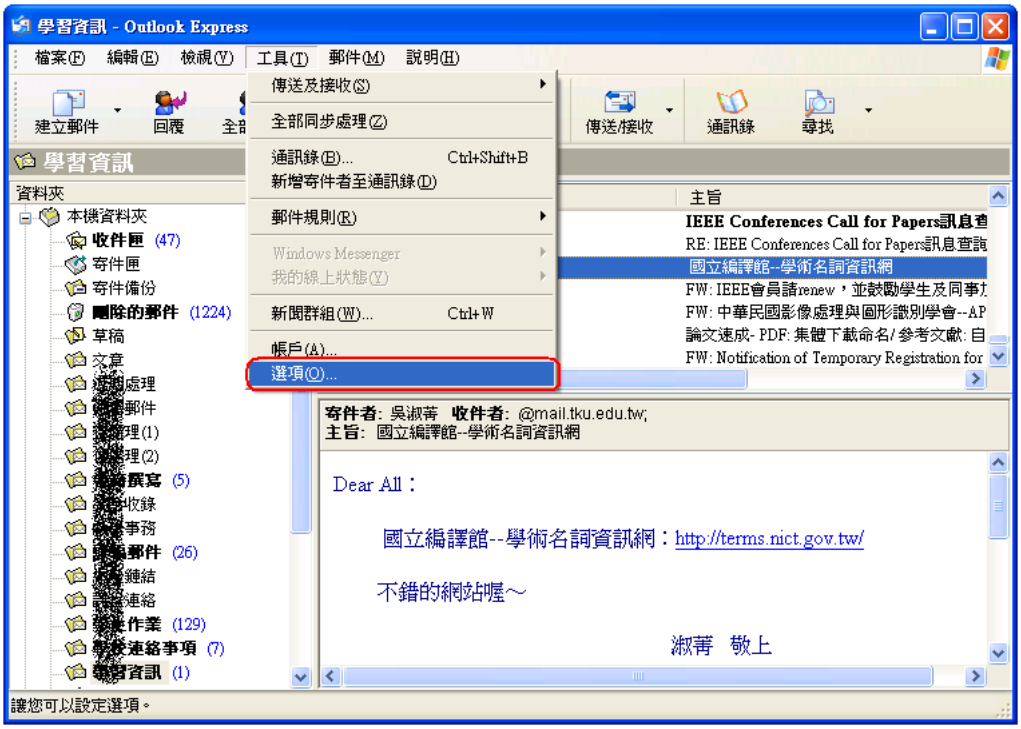
- 選取【工具】/【信任中心】/【信任中心設定】/【自動下載】
- 勾選【不自動下載 HTML 電子郵件訊息或 RSS 項目中的圖片】

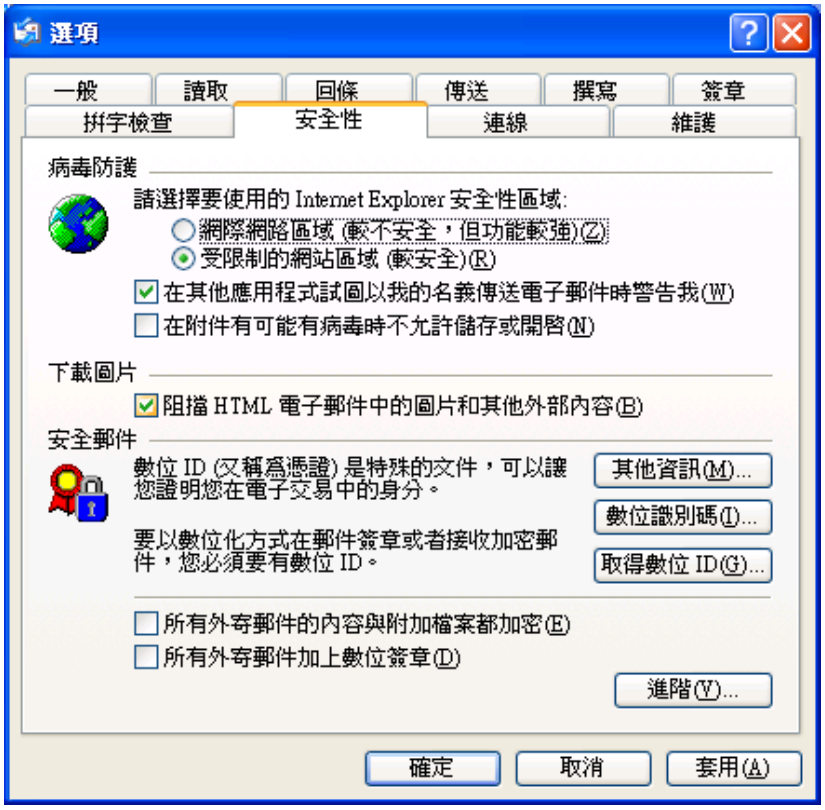




(2) 以 Outlook Express 設定為例：

- 選取【工具】/【選項】/【安全性】
- 勾選【阻擋 HTML 電子郵件中的圖片和其他外部內容】





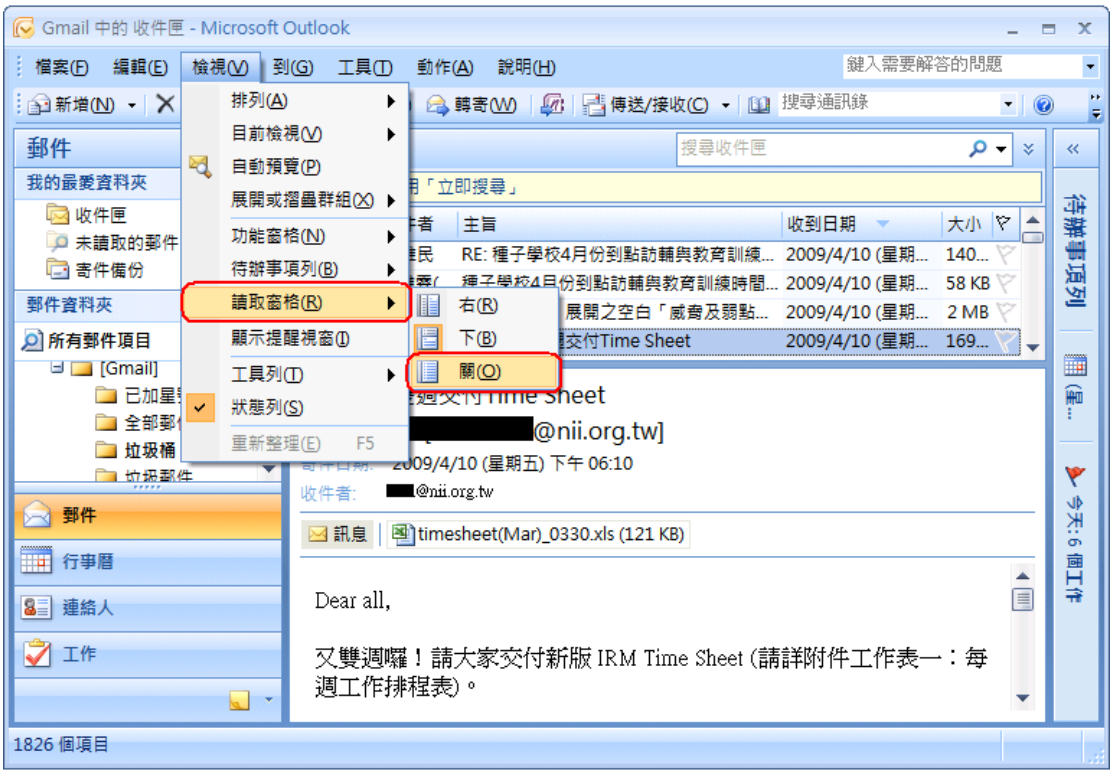
❶-3 關閉預覽視窗

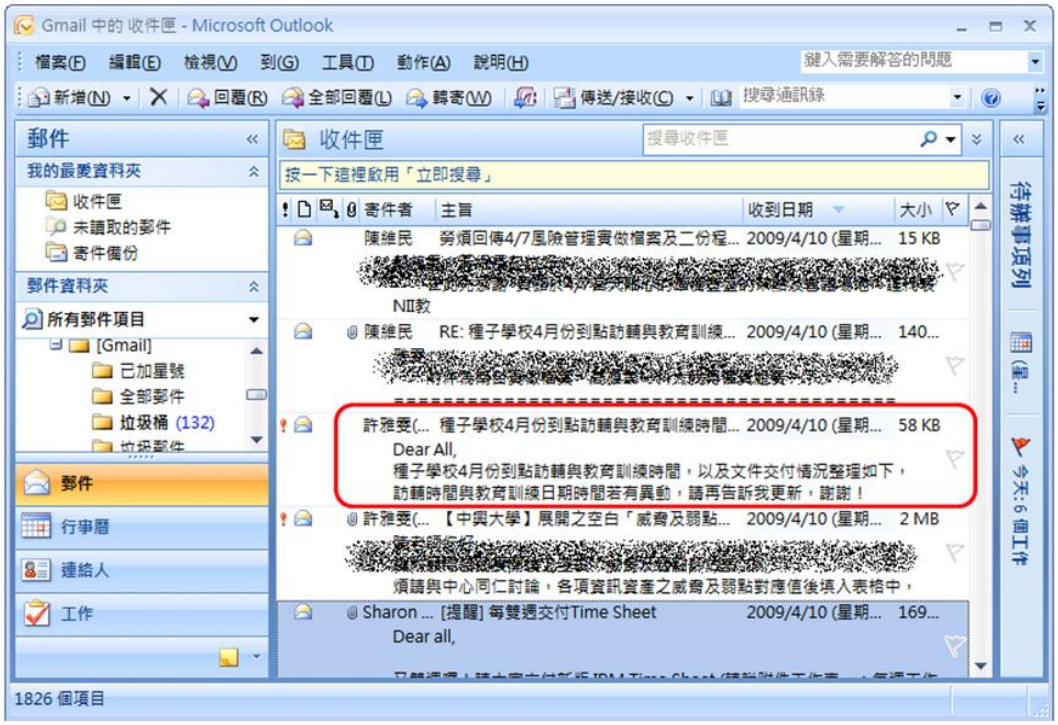
郵件軟體的預覽功能提供使用者較為方便的瀏覽方式，但是病毒也可能利用郵件軟體的閱讀及預覽功能達到傳播病毒的目的，使用者不需要執行電子郵件中的附加檔案，只要預覽帶有病毒的信件，就會使電腦受到病毒感染，因此建議最好可以將郵件軟體的預覽功能關閉，以避免不經意開啟惡意電子郵件。

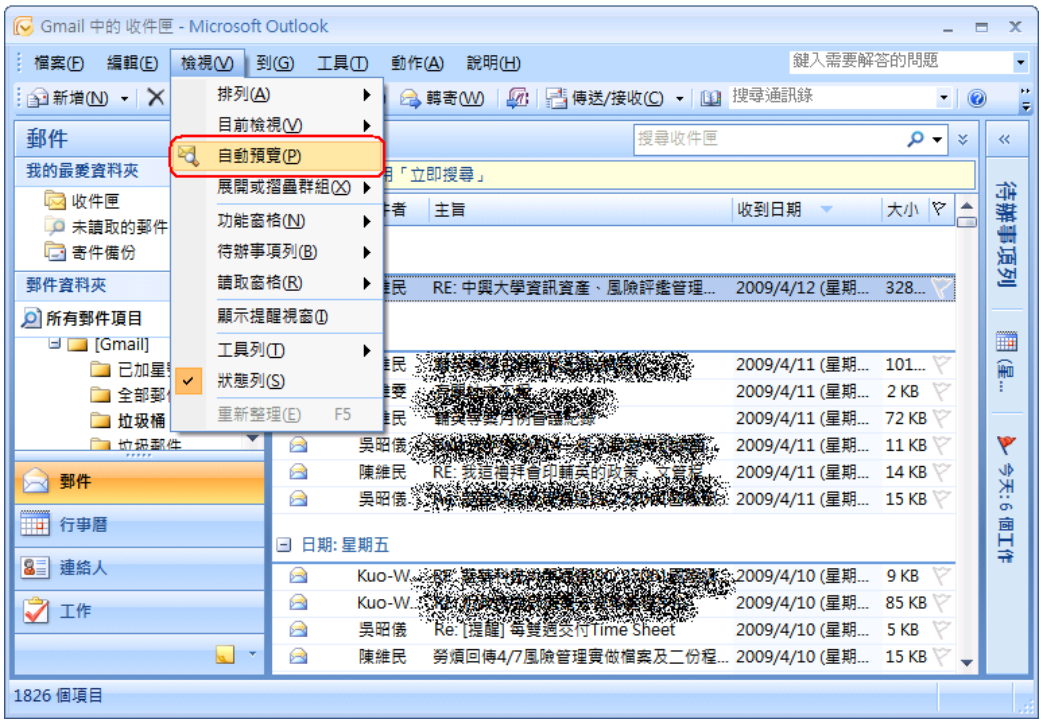
關閉郵件預覽視窗的功能設定，以下使用常見的郵件軟體 Outlook 及 Outlook Express 來分別進行說明：

(1) 以 Outlook 設定為例（註：不同版本的 Outlook 選單的位置可能會不同）：

- 選取【檢視】/【讀取窗格】
- 選擇【關閉】
- 或
- 選取【檢視】/【自動預覽】
- 點選即【關閉】，再點選則【開啟】

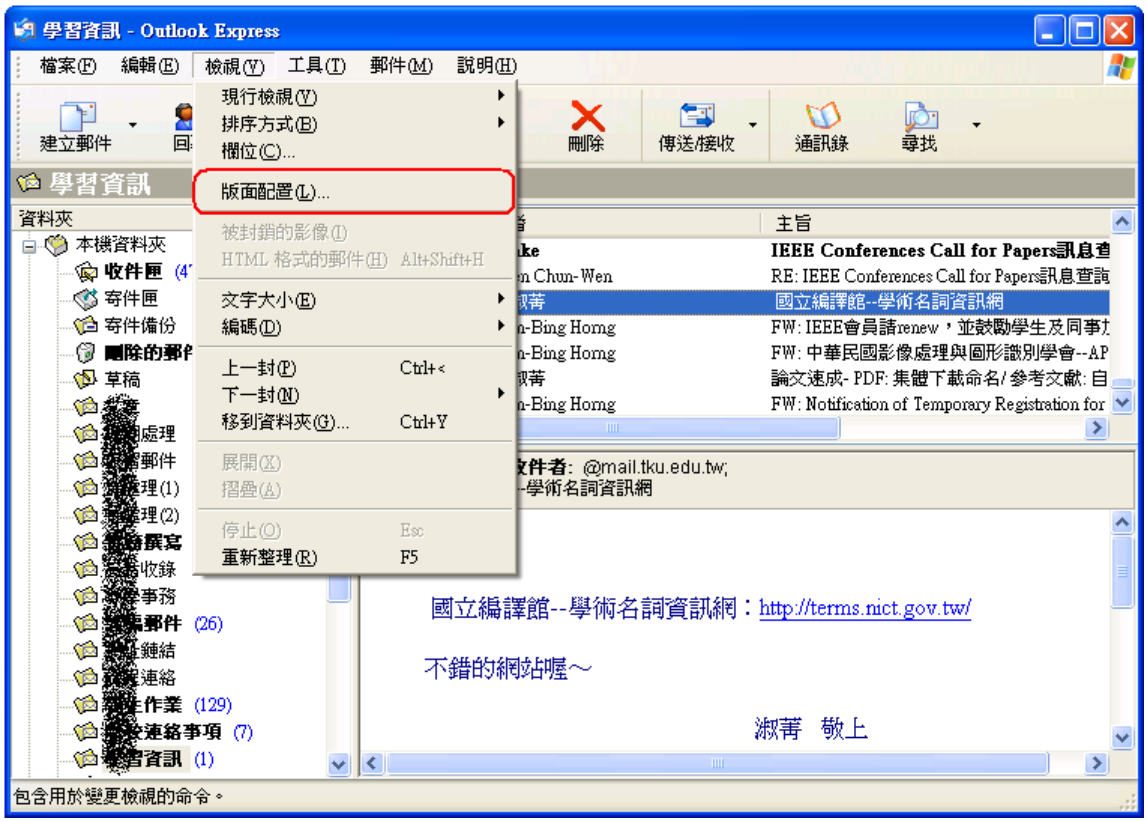


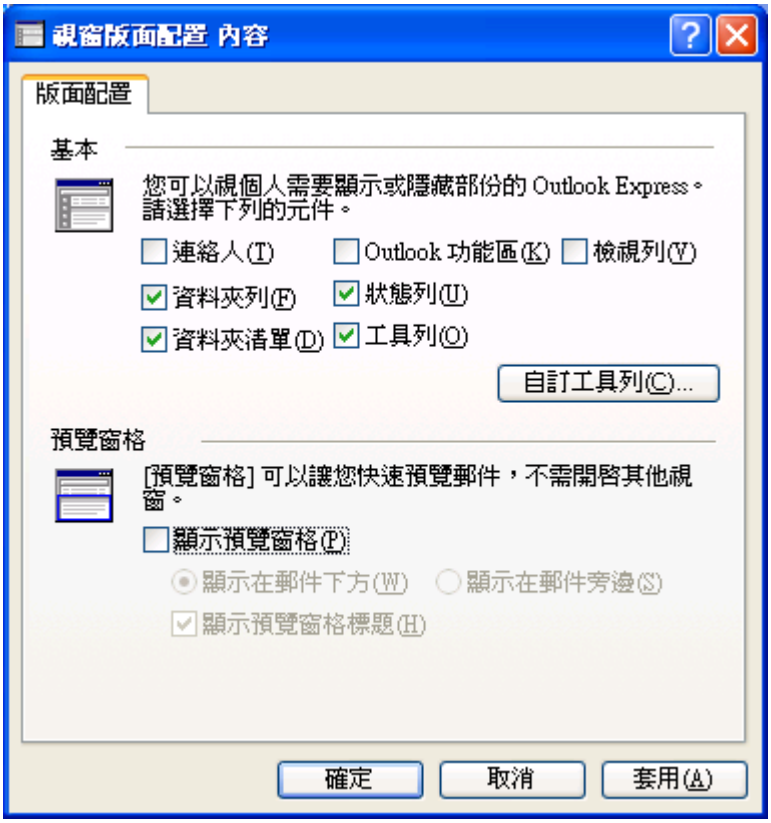




(2) 以 Outlook Express 設定為例：

- 選取【檢視】/【版面配置】
- 不勾選【顯示預覽窗格】


學習資訊 - Outlook Express
檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)
現行檢視(Y)
排序方式(B)
欄位(C)...
版面配置(L)...
被封鎖的影像(I)
HTML 格式的郵件(H) Alt+Shift+H
文字大小(E)
編碼(D)
上一封(P) Ctrl+<
下一封(N)
移到資料夾(G)... Ctrl+Y
展開(X)
摺疊(A)
停止(O) Esc
重新整理(R) F5
建立郵件
刪除
傳送/接收
通訊錄
尋找
學習資訊
資料夾
本機資料夾
收件匣
寄件匣
寄件備份
草稿
主旨
IEEE Conferences Call for Papers訊息查
RE: IEEE Conferences Call for Papers訊息查詢
國立編譯館--學術名詞資訊網
FW: IEEE會員請renew，並鼓勵學生及同事
FW: 中華民國影像處理與圖形識別學會--AP
論文速成- PDF: 集體下載命名/參考文獻: 自
FW: Notification of Temporary Registration for
@mail.tku.edu.tw;
-學術名詞資訊網
國立編譯館--學術名詞資訊網：http://terms.nict.gov.tw/
不錯的網站喔～
淑菁 敬上
包含用於變更檢視的命令。


視窗版面配置 內容
版面配置
基本
您可以視個人需要顯示或隱藏部份的 Outlook Express。請選擇下列的元件。
連絡人(T)
Outlook 功能區(K)
檢視列(V)
資料夾列(F)
狀態列(U)
資料夾清單(D)
工具列(O)
自訂工具列(C)...
預覽窗格
[預覽窗格] 可以讓您快速預覽郵件，不需開啓其他視窗。
顯示預覽窗格(P)
顯示在郵件下方(W)
顯示在郵件旁邊(S)
顯示預覽窗格標題(H)
確定
取消
套用(A)

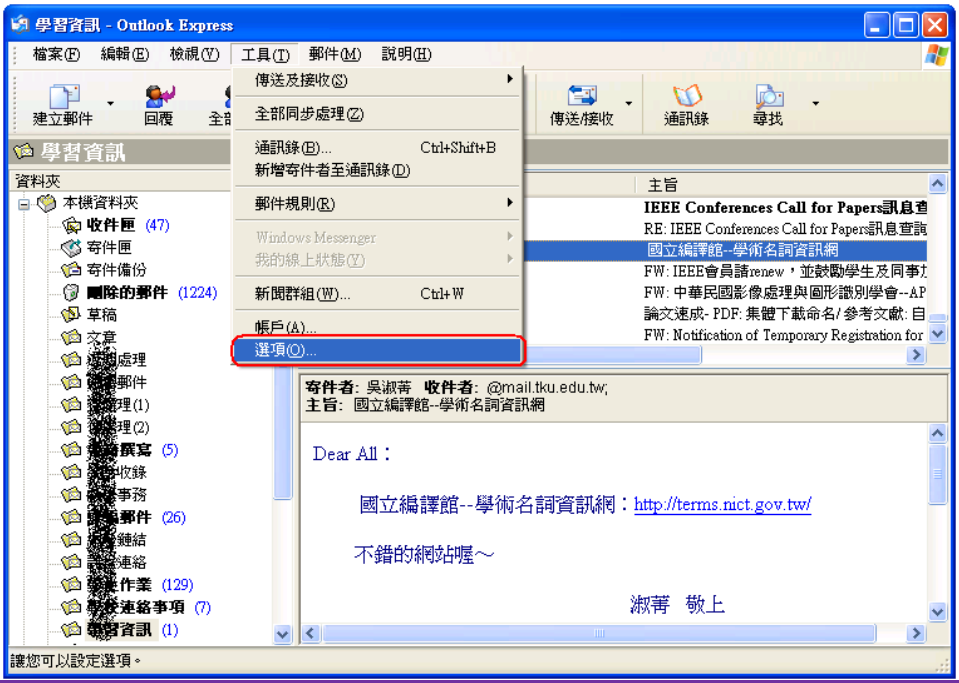
❶-4　設定以純文字格式讀取郵件

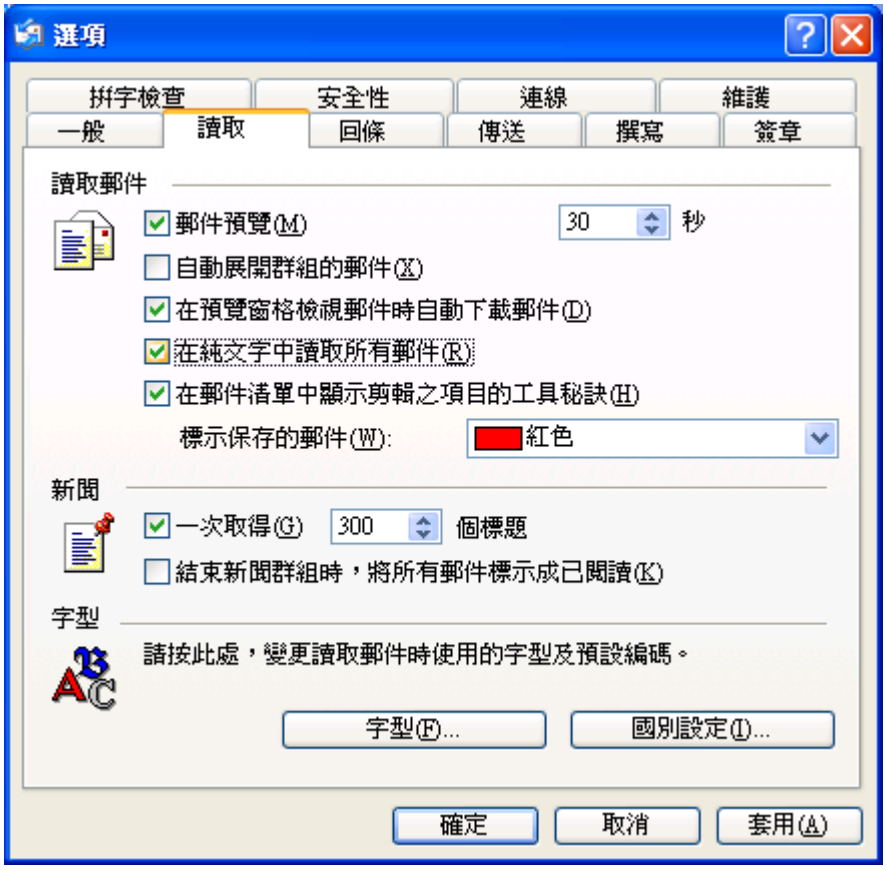
為了避免駭客或有心人士透過電子郵件，以超連結或圖片的方式暗藏惡意程式或散播病毒造成電腦的損害，建議最好以純文字的方式來閱讀或編輯電子郵件。

以純文字格式讀取郵件的功能設定，以下使用常見的郵件軟體 Outlook 及 Outlook Express 來分別進行說明：

(1) 以 Outlook 設定為例（註：不同版本的 Outlook 選單的位置可能會不同）：

(2) 以 Outlook Express 設定為例：





❷ 網路交友與求職

網際網路的進步以及資訊設施的發達，使得人與人之間的互動有了嶄新的發展，社交網路成為時下最夯的人際關係橋樑。然而網際網路「無國界」的特性，像是藉由 ICQ、聊天室、BBS、email、Facebook 等，不受時間、地點的限制，都可以讓世界各地的人聊天，結交來自異國的朋友，但由於網路「隱密」的特性，使得其中傳遞的訊息不真實的可能性極高，也為網路交友帶來陷阱。另外，多數民眾透過求職網站刊登履歷，常見的網路求職陷阱，像是不實求職廣告、工作內容與權利義務交代不清、求職前簽約及繳交費用……等，讓求職民眾防不勝防。以下針對網路交友與求職提供相關之基本防範措施：

❷-1 網路交友之基本防範措施：

(1) 慎選聊天室與網站

務必挑選正派經營、無色情暴力的聊天室，以免危害自己的身心健康。

(2) 慎防個人資料及隱私外洩

在雙方尚未熟識之前，切勿輕易透露個人資料，如：家裡的電話號碼及住址……等，以避免被對方騷擾的可能，也不要將個人的照片任意寄出，或藉由網路散布照片；如果網友傳送任何猥褻或令人覺得不舒服的訊息，千萬不可回應。

(3) 嚴禁金錢借貸或交易

一切開銷以各自負擔為原則，不佔對方便宜，也不搶著結帳，若對方開口借錢，應婉拒或轉移話題。

(4) 避免單獨赴約

如非得和網友見面，應以參加多人網聚較佳，最好要有同伴或其他友人同行，且約在人多、安全的公眾場合，並與家人保持聯繫；赴約時可以隨身攜帶防身物品，例如：防狼噴霧器、哨子……等，或是平常就學習一些防身術，一旦發現對方言行不一致，或察覺有異狀時，應冷靜地儘速離開。

❷-2 網路求職詐騙基本防範措施：

以下彙整 5 項網路求職詐騙基本防範措施予各位讀者參考：

(1) 審慎評估各類求才廣告或求才訊息。

(2) 拒絕接受非法工作。

(3) 勿繳交任何的費用及證件。

(4) 不簽署任何文件、契約。

(5) 讓家人知道面試的時間、地點和公司名稱。

消保會亦強調，一般業者並不會要求民眾在開始工作前即繳交任何費用，若業者要求民眾於工作前預先繳交材料費、工作訓練費用、置裝費用……等，求職者應提高警覺，或可於求職前先至經濟部商業司網站(http://gcis.nat.gov.tw/pub/cmpy/cmpyInfoListAction.do)查詢該公司是否有合法登記。

❷-3 網路釣魚：

通常釣魚電子郵件中所提供的超連結，其網址會與你實際所前往的網站不同。乍看下為知名公司網址，但其中的字母可能經過增減或更換，例如，www.microsoft.com 可能會變成 www.micosoft.com 或 www.mircosoft.com，因此而受騙的民眾輕則帳號被盜用，重則因個人金融資料外洩而損失慘重。以下針對網路釣魚提供相關之基本防範措施：

(1) 對於詢問您個人資料的郵件提高警覺

當您收到詢問您相關敏感資訊的信件要提高警覺，尤其含有對外超連結的信件。這些資訊包含：使用者名稱、帳號、密碼等，通常具有一定規模的企業、銀行，都不會透過 email 的方式詢問您相關的個人資訊，也不要將帳號和密碼以電子郵件的方式傳送給其他人。

(2) 不要隨意點選郵件中的網址連結

將日常經常使用的網站加入「我的最愛」書籤，透過書籤連結至正確的網站，或是開啟新的瀏覽器視窗直接輸入網址，若相關活動為真，應該能在官方網站上找到對應的活動訊息，避免誤連詐騙歹徒所設立的假網頁。

(3) 打電話向客服人員確認

若要確認信件中的訊息或是連結是否為真，除了至官方網站上查詢之外，也可以透過官方的服務電話或是郵件地址確認，電話號碼最好透過查號台查詢，或是日常交易單據上所印資料（如：銀行帳單），以確保所聯繫的電話與服務人員之真實性。

(4) 勿貪小便宜點選好康連結

「天下沒有白吃的午餐」，對於「免費優惠」、「好康大放送」……等吸引您的抽獎廣告，一旦點閱進入網頁，若要求您輸入敏感性資料來換取任何優惠或利益時，務必留意此網站之真實性，並且留意所同意留下的資料是否會對自己造成任何的不利或困擾。

(5) 定期檢查交易紀錄與網站帳號

對於重要的交易網站應經常瀏覽檢查帳號，並留意您的交易紀錄，如收到信用卡和銀行帳戶的交易紀錄時，請確認是否有任何未經授權的收費。若遲遲未收到帳單，請打電話至信用卡公司或銀行，確認帳單地址和帳戶餘額是否正確。

(6) 透過加密的網頁功能傳送個人資料

若網頁要求輸入任何敏感性資料，注意網址是否為 https（資訊加密協定）開頭，或是在瀏覽器頁面出現黃色鎖匙圖示（如圖 11~圖 13 所示，鎖匙標示的位置可能因為不同瀏覽器或不同版本而有差異，請各位讀者留意），這並非萬無一失，但能保證訊息在傳輸過程中某種程度的安全性。

圖11. 黃色鎖匙圖示標示位置（以 Internet Explorer 瀏覽器為例）

（圖像來源：教育部全民資安素養網 / 製圖：NII 產業發展協進會）

圖12.　黃色鎖匙圖示標示位置（以 Firefox 瀏覽器為例）

（圖像來源：教育部全民資安素養網 / 製圖：NII 產業發展協進會）

圖13.　黃色鎖匙圖示標示位置（以 Google Chrome 瀏覽器為例）

（圖像來源：教育部全民資安素養網 / 製圖：NII 產業發展協進會）

❷-4 網路交易：

刑事警察局統計 101 年 1 至 3 月份，詐騙集團以駭客手法入侵購物網站平台與賣家的訂單或出貨系統，竊取買家個人資料與交易明細資料，再假冒平台或商家以分期錯誤等方式為由，誘騙被害人至 ATM 解除分期付款設定，並依其指示轉帳而被騙，遭被害之前五大商家受害案件即逾 605 件，平均每月發生 201 件，詐騙金額累計超過 3,100 萬元。為避免網路交易時遭到詐騙，以下提供網路交易相關之基本防範措施：

(1) 勿至 ATM 解除分期付款設定

詐騙集團常以刷卡時誤設分期付款為由，向被害人謊稱如不配合至 ATM 解除可能會持續按月扣款；事實上，ATM 只有轉帳及提款功能，並無法解除設定刷卡分期付款，請民眾誤落入詐騙集團的陷阱中。

(2) 選擇有信譽之商家或賣家進行交易

選擇有信譽的交易對象，仔細瞭解對方的信用風評，如賣場資訊、評價紀錄或利用問與答的機制，於詢問時留意賣家專業度，可瞭解賣家是否真心投入、認真經營。賣家若將網路開店視為長期經營，勢必會重視客戶反應及商品品質，也可從賣家出貨速度、回應問題速度，決定未來是否再向這位賣家購買商品。此外，好評價給的時間點也要注意，例如：下午 4 點才剛結標的交易，買家 5 點就給好評價說已收到商品，這就有可能是賣家「自家人」所給的造假評價。

(3) 儘量選擇貨到付款或面交方式避免金錢損失

不論是賣家或買家，堅持面交，一手交錢一手交貨，當場確認物品及金額無誤後才能銀貨兩訖。尤其是單價高的貨品，最好以貨到付款或面交方式進行交易，但提醒各位讀者面交時亦要注意自身安全。

(4) 勿貪小便宜

不要貪小便宜，低於市價太多的東西往往有瑕疵，甚或可能是竊盜集團藉機銷贓，下標時要多加考量，另外，賣家若是使用原廠或其他賣場的商品圖片，極有可能其手上並沒有實體商品可供拍照，這類的情形也要多加小心。

(5) 撥打「165 反詐騙專線」詢問

網路賣家遇有不正確入帳情形，可迅速撥打 165，尋求警方協助聯繫相關銀行，以進一步釐清入帳來源，避免成為詐欺人頭戶。接到疑似詐騙電話或遇到疑似詐騙情境，謹記「防詐騙三要訣」：冷靜、查證、報警，儘速撥打 165 反詐騙諮詢專線電話查證，或撥打 110 求助，以免受害。

主題 3. 網路詐騙求助站

網路詐騙手法日新月異，倘若您不小心遇到網路詐騙時，應立即向警方報案，除了可請相關單位協助查證亦可聯繫網路警察追捕歹徒，以期即時阻斷各種可能的傷害與損失。在求職方面若欲詐騙可透過行政院勞工委員會服務專線 0800-085-151 尋求協助，網路購物或交易的糾紛可向行政院消費者保護委員會投訴，除此之外，亦可透過以下的管道進行通報或請求提供相關的協助。

❶ 165 反詐騙諮詢專線與網站

內政部警政署為提升全民反詐騙意識，加強預防詐欺犯罪，於民國 93 年 4 月 26 日成立「0800-018110 反詐騙諮詢專線」，建立民眾諮詢詐騙問題之管道。為了方便民眾有效牢記，內政部警政署向交通部爭取「165」特殊號碼，並正式更名為「165 反詐騙諮詢專線」，同時增派警力，提供民眾線上即時協助與受理報案，不論手機或市話，只要撥打「165」即可由專人說明並研判是否為詐騙事件。

圖14.　165 反詐騙諮詢專線（圖像來源：http://165.gov.tw）

原先 165 專線主要是針對民眾接到不明的可疑電話時，可以透過專線人員的協助，先行判斷是否為詐騙集團的欺騙伎倆，並提供相關的諮詢與服務，但由於近來網路活動的盛行與發達，詐騙集團的犯罪手法已不只侷限於電話詐騙，更擴展到網路上的交易或透過網路來欺騙民眾，因此內政部警政署也成立了「165 全民防騙超連結」網站，民眾可以直接透過網站進行檢舉與報案。

民眾進入「165 全民防騙超連結」網站後，可以根據實際的情況點選「我要檢舉」、「我要報案」或「案件查詢」，線上填寫相關的聯絡資訊與詐騙的形式與內容，資料送出後將由專人進行聯繫並提供必要的協助。

圖15.　165 全民防騙超連結（圖像來源：http://165.gov.tw/case_report.aspx）

而「165 全民防騙超連結」網站，除了提供線上檢舉與報案和案件查詢的服務之外，也提供許多豐富的資訊，如：詐騙小叮嚀、詐欺預防寶典、財損排名、詐騙排名、宣傳素材等資料，讓民眾對於網路詐騙有更深入的瞭解，避免成為詐騙集團下手的對象。

- **165 反詐騙諮詢專線**
  服務電話：手機或市話直接撥打「165」

- **165 全民防騙超連結**
  網址：http://165.gov.tw/

❷ 網路釣魚通報窗口

有鑑於網路釣魚手法持續進化，影響範圍日益擴大，網路釣客心態已經從單純好玩、有趣並藉此炫耀自己能力，轉而利用盜取的個資與詐騙集團勾結合作，利用各種管道取得被害人信任，並據此進行詐騙取財，造成個人或社會上巨大的經濟損失。因此在民國 99 年 7 月由台灣電腦網路危機處理暨協調中心 (Taiwan Computer Emergency Response Team/Coordination Center，簡稱 TWCERT/CC)成立「台灣反網路釣魚網站工作小組」，針對網路釣魚相關議題進行研究與討論，期許可集結各單位的資安事件處理能量，共同研商出打擊網路釣魚行為所造成潛在危害的具體可行方案。

為能統一處理網路釣魚資安事件的通報與後續處理追蹤，TWCERT/CC 於民國 99 年 10 月建立了「網路釣魚通報窗口」，統一處理網路釣魚資安事件的通報與後續處理追蹤。

圖16.　網路釣魚通報窗口（圖像來源：http://www.apnow.tw/）

「網路釣魚通報窗口」結合運用了政府相關的資訊整合平臺，如：政府資安資訊分享與分析中心（Government- Information Sharing and Analysis Center, G-ISAC）、教育學術資訊分享與分析中心（Academy- Information Sharing and Analysis Center, A-ISAC）、國家通訊傳播委員會資訊分享及分析中心 (National Communications Commission- Information Sharing and Analysis Center, NCC-ISAC)的資安能量，以迅速分享網路釣魚相關資訊，快速地協助處理並提供技術支援的後盾。

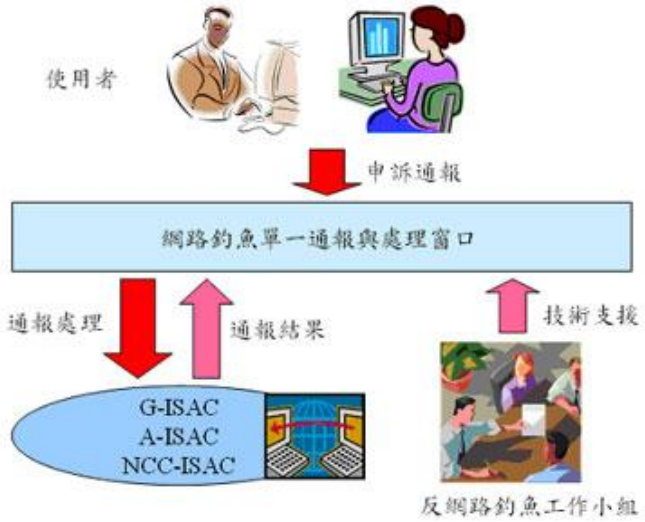


圖17.　網路釣魚通報窗口與其他單位之間的關係圖（圖像來源：http://www.apnow.tw/）

民眾點入通報平台後，使用者可以根據不同的類型進行通報，如：發現網路釣魚網站、收到網路釣魚信件，網站被植入釣魚網頁，若無法判別是否為網路釣魚網站，則可以透過其他類別進行通報，由專業的處理人員進行分析；線上通報後，單一窗口透過系統自動給予各個案件一個處理工作單號，後續可透過「通報查詢」功能，輸入工作單號查詢處理進度。

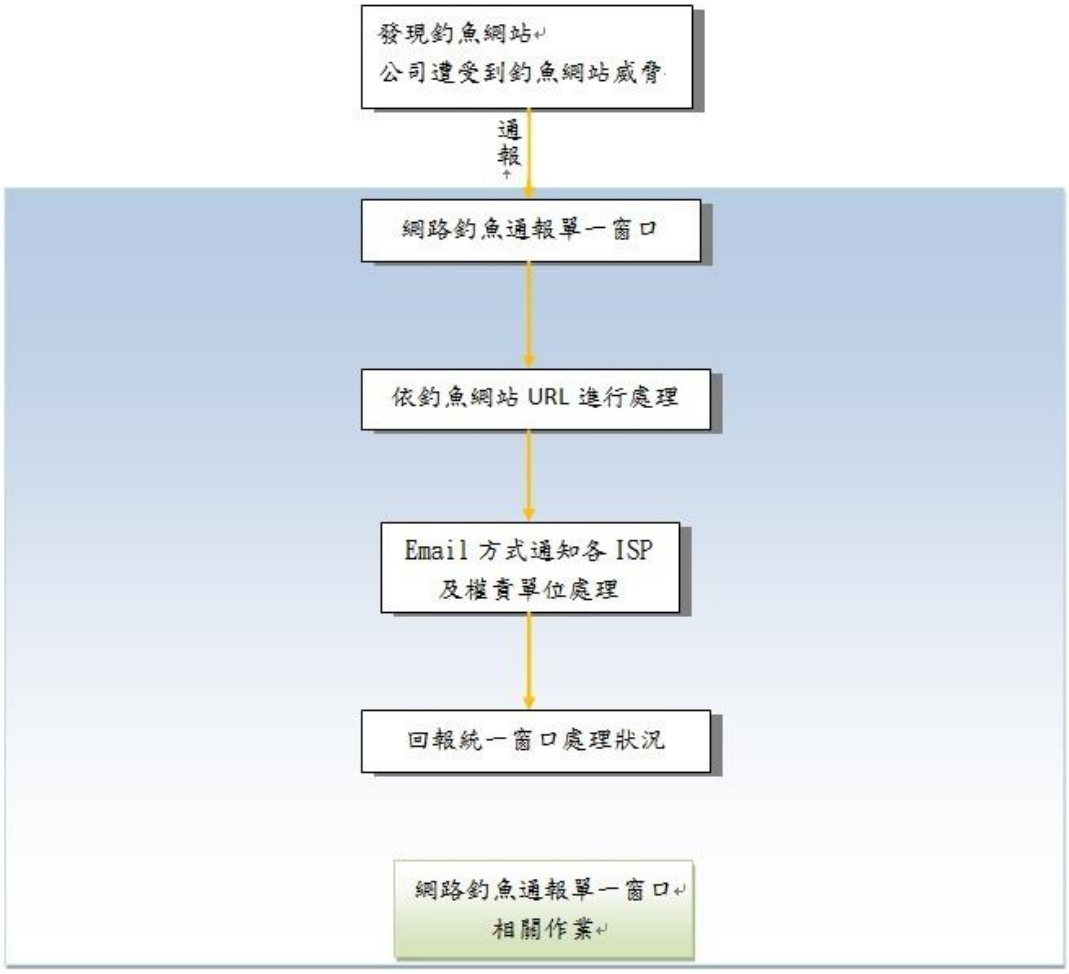


圖18.　網路釣魚事件通報流程圖（圖像來源：http://www.apnow.tw/）

❸ WIN 網路贏家單 e 窗口

網際網路發展愈普及，衍生的網路內容問題愈增多，為確保民眾網路內容安全問題能快速獲得處理及解答，以提升民眾對政府信賴，由「國家通訊傳播委員會」督導下，於民國 99 年 8 月 2 日成立「受理民眾申訴及通報網路內容問題單一窗口」，簡稱「WIN 網路贏家單 e 窗口」 (Watch Internet Network)。

圖19. WIN 網路贏家單 e 窗口（圖像來源：https://www.win.org.tw ）

為了讓青少年及兒童有一個健康、安全的網路環境，「WIN 網路贏家單 e 窗口」目前著重受理會對兒少身心發展有影響的網路內容，包括猥褻、裸露、血腥、暴力等文字、圖片、影音，以及其他涉及犯罪的內容，民眾可透過「WIN 網路贏家單 e 窗口」進行申訴。線上申訴的類別分類分為：網路色情類、網路詐騙/竊盜類、網路賭博類、毒品及藥物濫用類、網路暴力類、不當語言類、其他類（如：垃圾郵件），其中有關網路詐騙/竊盜類的項目包含：

- 網路詐欺：網路上虛設行號、販賣不實商品、釣魚網站、聊天室等詐騙錢財。
- 電腦病毒及網路竊盜：以不法之方式入侵他人電腦竊取、毀壞資料或以阻斷服務之方法癱瘓商務網站。
- 侵害版權、著作權、個資：未經授權網路販賣盜版媒體、使用他人的著作物。

民眾若遇到相關的網路詐騙/竊盜情事時，可透過「WIN 網路贏家單 e 窗口」進行申訴或通報，透過單一窗口電子信箱作業系統，將申訴案件轉請相關權責機關或網路平台服務提供者妥善處理，建立更為安全自由的網路空間。

申訴流程作業：

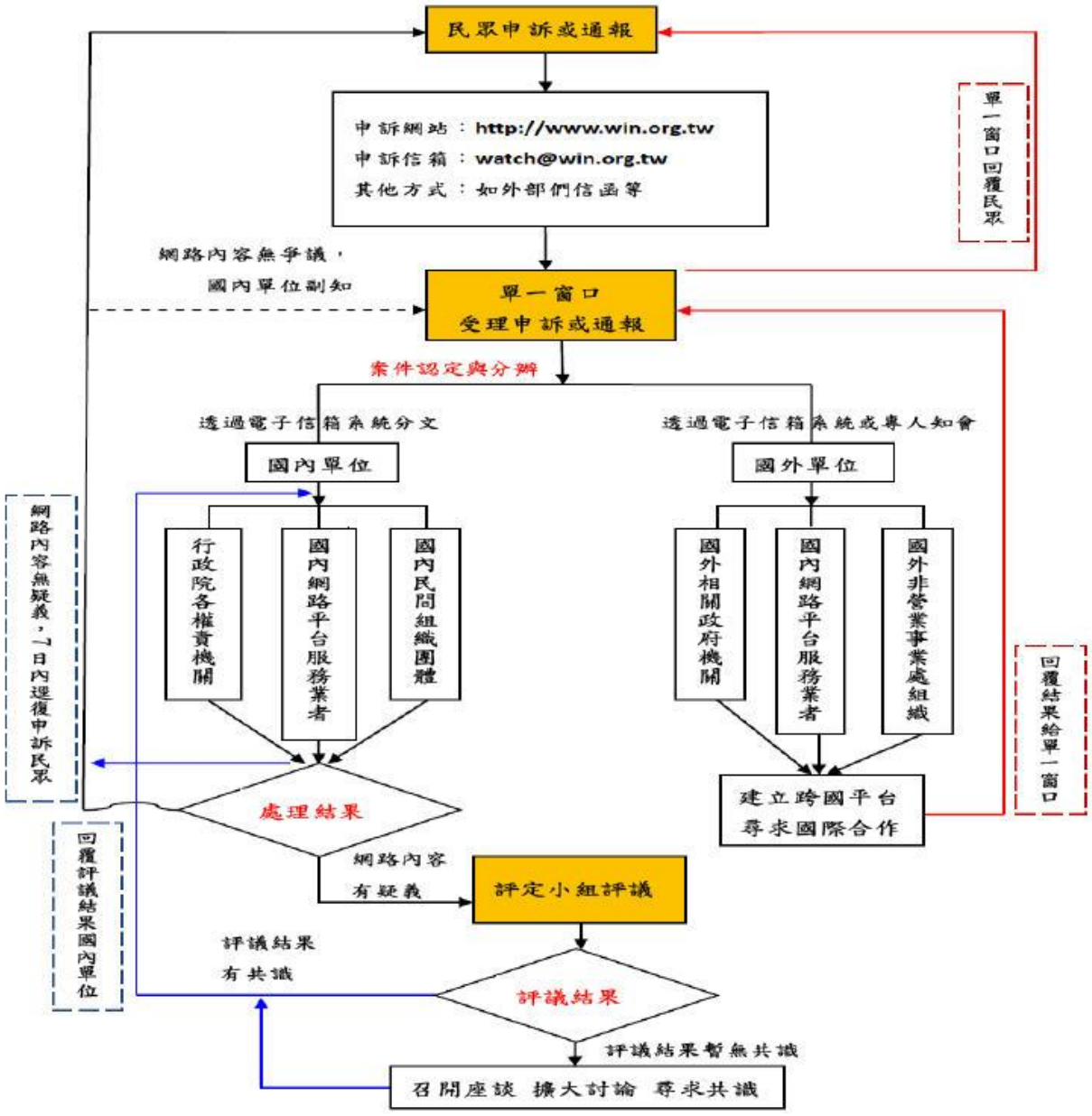


圖20.　WIN 網路贏家單 e 窗口申訴流程作業示意圖（圖像來源：https://www.win.org.tw ）

防範網路詐騙的五個小撇步

在本手冊的最末，我們將提供各位讀者以下五個防範網路詐騙的小撇步，請大家時時自我提醒，相信必能有助於你我遠離網路詐騙！

(1) **不輕易透露個人資料**：網路遊戲公司普遍都有和電信業者合作小額付款機制，讓用戶可以方便地用手機號碼購買遊戲點數，然後點數費用可以連同手機帳單費用一起支付。提醒遊戲玩家，不要貪小便宜或輕信網友，而把自己的手機號碼、身分證字號等資訊提供給他人，以免遭到歹徒利用，使用你的手機號碼小額付款來買點數。

(2) **小心求證**：當朋友以即時通方式傳來訊息要向你借錢或請你幫忙買東西時，一定要用即時通以外的其他方式再次求證，例如直接打電話詢問朋友，不要輕易地就答應對方的要求。

(3) **按下滑鼠前請三思**：臉書或噗浪等社群網路服務中也可能暗藏有詐騙的陷阱，像是臉書遊戲或應用程式已經發生暗藏木馬程式的案例。在你決定點選臉書上的超連結或要玩某個小遊戲之前，請再想想是否真的很必要，或者上網查一查別人是否有類似的受騙經驗。

(4) **不隨意點選網頁連結**：不任意下載讀取來源不明之電腦檔案及開啟不明網頁連結，以減少下載惡意程式與帳號密碼遭盜取之風險。這些惡意超連結可能出現在電子郵件、即時通訊息內、臉書塗鴉牆、聊天室或留言版等處。

(5) **設定安全的密碼**：設定安全網路服務密碼，不要為了方便，把自己的所有網路服務都設定同一組帳號與密碼！因為這樣就如同提供歹徒一個最方便的方式取得並盜用與假冒你所有的網路身分。

圖像來源：http://office.microsoft.com/

參考資料

[1] World Telecommunication/ICT Indicators Database, International Telecommunication Union

[2] The World in2011 ICT FACTS AND FIGURES, International Telecommunication Union

[3] 資策會 FIND「我國網際網路用戶數調查」

[4] How People Spend Their Time Online, Social Media Today

[5] Top Scams of 2011, NCL'S FRAUD CENTER

[6] 2011 Internet Crime Report, Internet Crime Complaint Center

[7] 台灣反網路釣魚通報機制與平台介紹 台灣反網路釣魚工作小組主席 林順傑

辨識網路詐騙

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　許雅雯　財團法人中華民國國家資訊基本建設產業發展協進會副理

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。