一般民眾版

# 辨識網路詐騙學習手冊

MINISTRY OF EDUCATION 教育部

# 目錄

# 主題一 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1.通訊軟體／簡訊、2.網路交友與求職、3.網路釣魚、以及4.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。**

## 1. 通訊軟體／簡訊

通訊軟體、簡訊及電子郵件是非常重要且常用的功能，而且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。詐騙的類型主要可分為活動訊息、釣魚網站、危險連結等，以下針對各種類型，提供說明與案例參考。

### ● 活動訊息

詐騙歹徒擅長掌握人性弱點，常會以利益作為誘餌，利用網路便捷的特性，發送詐騙訊息，告知使用者獲得禮券、獎金、免費貼圖，如果使用者一時失察，禁不起誘惑，就可能誤信謊言，成為歹徒的肥羊。

**【案例參考】**

**適逢農曆七夕情人節，假冒Line免費貼圖下載的訊息：「七夕情人節限時免費下載，熊大來送愛！讓你情人節不孤單 https://cutt.ly/LINE-Love」，這類聲稱只要分享轉傳就可免費下載貼圖的詐騙訊息，實際上並非出自Line官方推出的活動。**

**提醒用戶收到這類帶有不明短網址的訊息，務必多加提高警覺，切勿點擊連結或填寫資料，以免個資遭外洩，也不要繼續轉傳才能遏止假訊息被持續散布。**

**【摘自自由時報2022/8/4】**

## ● 投資詐騙

網路投資詐騙的類型通常會結合Line群組，在社群平臺假冒名人或是藉由手機號碼加民眾入投資群組，透過噓寒問暖建立感情，營造溫馨關懷的人設，然後利用對方的信任，佯稱有高報酬的代操盤方案或是抽股票的方式，邀請民眾匯款到指定的帳戶，透過虛擬的投資平臺，讓受害者以為有高額獲利，不知不覺掉進詐騙歹徒的陷阱中，等到要領出時，會用各種理由要求再匯保證金，到最後血本無歸。

**【案例參考】**

**一名蔡姓女子瀏覽臉書，看到有關投資黃金的網頁廣告後主動留言詢問，歹徒立即回覆可先加入專業指導員Line好友，並傳送假投資網址要求蔡女點擊並註冊帳號加入會員，指示蔡女需先匯款到指定帳戶購買網站購物金，才能購得黃金。**

**初期蔡女帳戶顯示獲利數萬金額，而向客服人員申請提領獲利，但客服人員又表示需先繳納手續費才能進行提領，蔡女便依指示再度轉帳數筆匯款，直到蔡女帳戶金額顯示為零，才驚覺遭到詐騙。**

**刑事警察局表示，此類假投資詐騙初期會讓被害人投入小額本金並順利申請出金，使被害人放下戒心，等到被害人加碼投資後，便開始以需先扣稅或繳納手續費、保證金等各種理由拖延出金，後續網站或App即無預警關閉，讓被害人血本無歸，提醒民眾勿輕易相信來源不明的投資管道。**

**【摘自自由時報2023/3/13】**

### ● 危險連結

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：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訊息，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，惡意軟體便會在你不自覺的情況下下載並安裝在你的電腦（或行動裝置）中。

該惡意軟體可能會偷取你在裝置中儲存的個人資料，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，例如假借你的身分，跟好友借錢或購買遊戲點數。

**【案例參考】**

**有惡意人士冒用新竹市府名義，寄發有關「阿凡達2-水之道電影票免費索取」惡意郵件，企圖引誘不知情民眾下載點選惡意連結。**

**惡意人士刻意將寄件者Email網址尾碼改成g0v.tw（數字0）寄送，企圖讓民眾誤以為是由政府機關網址gov.tw（字母o）所發送郵件。此案例是欲引誘民眾登入假網頁以取得其帳密個資。**

**市府提醒，為防範社交工程郵件，建議「關閉信件預覽」、「關閉預載圖片」、「以純文字模式開啟信件」，並於開啟信件時先確認信件來源無誤後再開啟，以降低觸發釣魚信件開啟及點閱率。**

**若不慎已點選該郵件的連結或附件，電腦即有可能已經中毒或遭植入木馬，建議請專業資訊公司檢視電腦安全性。**

**【摘自聯合報2023/2/6】**

## 2. 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，更容易結交到志同道合的朋友。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。

但是我們要如何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。

### ● 交友App／通訊軟體

詐騙歹徒利用網路無遠弗屆且難以查證的特性，並且看準男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。由於網路具匿名性，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。

【案例參考】

蔚婷（化名）今年上半年因與男友分手、愛貓生病、催婚壓力等緣故，嘗試網路交友，下載交友軟體認識一名男子，對方自稱雙親來自臺灣，小時候移居中國大陸，目前擔任骨科醫生。二人很聊得來，交換Line也常通電話。

二人聊了三個月，以老公、老婆互稱。過了不久，男子打算回臺定居、開設診所，邀請蔚婷入金投資，男子表示只要入金40天，保證一定能回收本金加百分之八點四一美金利息。網站頁面設有投資專區、真人線上客服及投資明細等，儼然是個實際運作的網路銀行。

蔚婷前後匯款18次，匯款單上有11個不同銀行的帳戶，蔚婷曾問客服人員，為什麼是臺灣端的個人銀行帳戶？客服辯稱，這些帳戶是公司在臺灣的登記人，蔚婷不曉得為什麼自己當下會相信此說法。

投資的第39天，再一天就可以回收，蔚婷向系統客服表示要一次出清提領。客服告訴她，提領前必須先繳所得稅，加上蔚婷屬於境外人士，須繳納投資金額百分之十六的稅金，於是她還向家人借了數十萬元繳稅。

入金第42天，男子傳來訊息表示身不由己才行騙，語畢便刪除Line帳戶。蔚婷萬萬沒想到，積蓄化為帳面數據。

網路感情詐騙就是慫恿被害人投資，給予當事人可以一起走到未來的夢，最後卻煙消雲散。

【摘自聯合報2023/7/23】

### ● 盜用通訊／社群軟體帳號

即時通訊軟體、社群媒體，例如Line、Facebook、IG等，是一般人常見的溝通管道，這些應用程式可以讓線上的使用者進行聊天對話，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，並傳送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。有些詐騙歹徒則會假冒成親友發送訊息，要求幫忙購買遊戲點數，造成被害人金錢上的損失。

**【案例參考】**

**新竹縣竹北市近日發生多起國中生臉書帳號被盜用，盜用者冒名發訊息給臉書圈的同學，誘騙協助支付遊戲費用，未料詐騙集團利用話術騙走其它國中生帳號，取得臉書再繼續行騙，這兩天至少有4名竹北的國中生受害。**

**李姓家長指出，詐騙集團先盜用兒子同學的臉書，請兒子幫忙支付遊戲費用，還告訴對方「明天去學校會還錢。」因此她兒子就用電信的小額支付，還把驗證碼給詐騙集團使用，累積後竟高達2.9萬。後來詐騙集團利用話術，將她兒子蘋果帳號、臉書帳號等騙走，然後利用她兒子臉書，再騙取其他同學的錢。詢問兒子的同學後，才發現已有3位學生也被詐騙。**

**【摘自聯合報2023/5/4】**

### ● 網路求職

詐騙集團多以透過網路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。

甚至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，以高薪輕鬆免經驗的誘人條件，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。

**【案例參考】**

**柬埔寨詐騙案引起高度關注，現在傳出詐騙集團，把據點轉移到西亞和東歐的交界處「高加索地區」，同樣是用高薪、免經驗等話術，吸引民眾前往，這地區包含6個國家，也有治安跟戰爭問題，而外交部也證實，確實有臺灣人到當地求職，恐怕會受到人身和通信自由限制。**

**高加索地區包含俄羅斯及土耳其部分地區、亞美尼亞、喬治亞、伊朗等6個國家，不僅治安問題嚴重還有戰爭問題，而當地詐騙集團主要以大陸人為主，就是因為喬治亞開放大陸免簽。**

**GASO指出今年2月有民眾接到電話，對方自稱在人力銀行上看到履歷，介紹國外工作像博弈網站程式Net程式設計師等，還主動提供公司簡介主打免費供餐、生日禮金及績效獎金等。**

**為此外交部回應確實有國人受困在高加索地區，詐騙集團就是先前在東南亞的電信詐團，初期都會非常和善等到人過去了就開始限制人身和通信自由。**

**【摘自TVBS新聞網2023/6/7】**

## 3. 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。

### ● 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，然後用垃圾郵件或通訊軟體發送連結，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實際登入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，偽造相似的登入網站，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！

**【案例參考】**

**111年中元普渡前後，有網友在Facebook的「家樂福Carrefour商品網友真心話社團」發文提醒，原來Google的搜尋頁中第一個選項竟然是釣魚網頁，進入後會要填寫帳號、密碼及信用卡資料。仔細看會發現網址是w.tw.costcois.lol，和真正的家樂福官網網址明顯不同。**

**【摘自自由時報2022/8/4】**


圖/假網頁詐騙案例（資料來源：家樂福Carrefour商品網友真心話社團）

### ● 假粉絲專頁

許多知名人士創立粉絲專頁，吸引大量粉絲追蹤，詐騙集團便鎖定了粉絲專頁的高人氣。詐騙集團透過偽造臉書通知訊息竊取粉專的帳密，取得粉專的管理權或是建立一個相似的粉絲專頁，之後再透過辦理活動的方式，提供連結給民眾填寫個人資料，或是透過訊息聯絡要求匯款的方式進行詐騙。

**【案例參考】**

**有詐騙集團冒充知名寢具品牌法蝶公司，設置假臉書粉專及假網購頁面，竄改105年底新北市政府勞工局派員稽查法蝶公司歇業情形之電視新聞畫面，謊稱法蝶公司正在勞工局監督下低價出清庫存，吸引民眾購買；7月初更出現詐騙集團明目張膽設置假關務署臉書，竄改張貼臺北關標售公告，引誘民眾前往假造的私貨標售網站購物，所幸許多熱心民眾覺得可疑主動向新北市政府及關務署詢問反映，讓兩機關在官網發布公告澄清。**

**臉書購物詐騙的慣用手法之一就是竄改新聞報導與電視節目畫面，假造不實名人代言或好康資訊，使民眾誤以為有便宜可撿，藉此誘導民眾前往詐騙集團設置的一頁式網站消費。**

**【摘自新北市政府警察局土城分局2018/7/24】**

## 4. 網路交易

相對於傳統的實體購物環境，網路交易帶給消費者的好處包括：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及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，因此常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。

### ● 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。

近來也有不少歹徒偽裝成買家，要下單時告知無法交易，要求賣家掃 QR Code 或是點連結進假客服網站進行聯絡，會導引賣家透過網銀轉出帳戶金錢。

**【案例參考】**

**南韓女團BLACKPINK先前來臺開唱，出現不少黃牛哄抬價格賣票，而類似情況並不罕見。去年11月南韓團體Super Junior隊長當時在直播中就談到，臺灣的演唱會原只有2場，後來加開第3場，就是因為黃牛猖獗。**

**而行政院會2023年6日通過了文化創意產業發展法的部分條文修正，要嚴懲黃牛。文化部次長王時思回應，「只要超過票面的金額，或者是票的定價加價轉售就構成黃牛，另外用身分產生器這類的方式來做購票，或者是外掛的程式機器人掃票，這個也是現在主要黃牛票最、困擾的類型。」**

**草案中寫明，要遏止加價轉售藝文表演票券，其中也包含使用不當方式取得的行為，加價販售處票面金額10到50倍罰鍰；要是以外掛等不當方式取得票券，則是行政罰及刑罰併。**

**至於實名制是否入法，文化部評估認為現階段不強制立法，會持續輔導業者實施實名制，並建立合法的二手票券平台。另外這回修法也針對個人或事業單位，在投資影視音專案時能享有租稅優惠，希望持續壯大臺灣文創。**

**【摘自公視新聞網2023/4/6】**

### ● 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臺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，再假冒平臺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。

**【案例參考】**

**台北市刑事警察大隊表示，中秋節前夕詐騙集團時常利用話題，透過優惠「應景商品」來誘騙民眾購買，因此特地提出5點提醒民眾小心。**

**如北市刑警大隊指出，網路購物盛行，詐騙集團將月餅禮盒、烤肉組合等中秋節應景商品做優惠，誘騙民眾進入「一頁式廣告」購買，結果收到貨後才發現，和照片上看到的差了十萬八千里。**

**其次，解除分期付款，在官方網站或公認的三方平台購物也不一定安全，一旦網購的資料遭外洩，詐騙集團就會假扮成電商客服或銀行來電，先以外流資料取得信任，再以「操作錯誤」、「訂單誤植」等理由，要求民眾前往ATM解除分期付款或操作網路銀行。**

**北市刑警大隊也說，不只買家，現在連網路賣家也要小心，詐團會先佯稱商品無法下單，再以「未簽署保障協議」等話術，引導被害人掃描「QRcode」進入釣魚網站，藉機騙取個人資料。**

**第四是發送釣魚簡訊，若有收到「幫你訂購蛋黃酥」的訊息，還附上不明電話號碼或點擊釣魚連結，也可能會造成個資外洩以及信用卡遭盜刷。**

**第五則是「中秋免費Line貼圖」，台北刑警大隊說，每當國定假日，便會出現「領取免費貼圖」的訊息，提醒民眾先別急著點開，以免誤擊詐騙集團特別設計的假貼圖連結。**

**【摘自NOWnews今日新聞2023/9/29】**

### ● 一頁式廣告

一頁式廣告的特徵是網頁一頁到底，消費者只要順著瀏覽到網頁底端即可付款結帳。

詐騙集團會於臉書、Line及各大網路平臺購買廣告版面，假冒明星專家代言加持、截取正版廠商圖片或竄改新聞報導畫面等，將消費者引導至一頁式廣告網站。

這類網站的商品會以低於市場行情的價格促銷，強調「貨到付款」、「七天鑑賞期」等字眼取信於民眾，頁面裡也會有一面倒的正向評價，讓民眾誤以為真。等民眾收貨付款後才發現商品和廣告不符，或商品品質低劣、有明顯瑕疵，這時才發現一頁式廣告上寫的公司名稱、連絡電話等全是假的，遭到詐騙。

**【案例參考】**

**臺南1名70歲程姓婦人，在家上網看到一頁式賣車廣告，能以低價購到便宜進口車，程婦信以為真前往銀行提款，行員查覺有異通報警方。**

**程婦向警方說，她在家中上網時，她與一頁式賣車廣告的人員接洽，對方指示程婦僅需要提領現金100萬元，就能買到物超所值非常便宜的進口車，程婦打算購車給自己兒子使用，所以便至銀行臨櫃提款。**

**員警告知程婦典型的詐騙手法，說明一頁式網頁廣告，販賣來路不明汽車、價格落差太大，沒有銷售地址相當可疑，一頁式詐騙購物網站特徵其實一直在變，也會隨著時間進化，民眾應多加警覺，程婦遂打消提款念頭。**

**【摘自勁報2023/7/6】**

# 主題二　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。**

## 1. 通訊軟體／簡訊

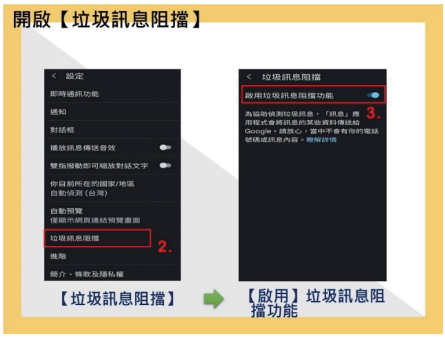
透過通訊軟體／簡訊進行網路詐騙行為，多數為有心人士假冒或偽裝身分，以友善、誘惑的內容誘騙民眾上鉤受騙，偽裝成各種活動、生活訊息設下陷阱，如夾帶惡意程式執行檔、內文中的惡意網頁超連結……等。為此，提供民眾面臨此類詐騙事件之基本防範措施如下：

### ● 設定阻絕垃圾簡訊


**IOS透過關閉iMessage功能 阻絕詐騙簡訊**

1. 單則簡訊封鎖、刪除與回報
2. 設定【不使用電子信箱接收iMessage】
3. 開啟【過濾未知的寄件人】功能
4. 關閉 iMessage 服務

圖/阻絕惱人詐騙簡訊（資料來源：內政部警政署165全民防騙網）

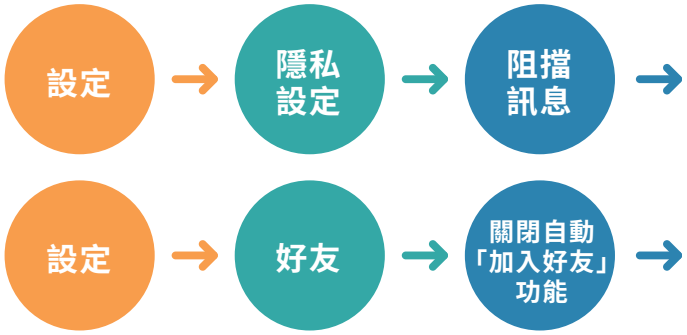



**安卓簡訊透過系統設定**

訊息 → 右上角設定 → 垃圾訊息阻擋 → 啟用

圖/阻絕惱人詐騙簡訊（資料來源：內政部警政署165全民防騙網）

## ● Line阻擋陌生訊息




非好友的訊息就看不到了。✓

不允許自動加入通訊錄裡的用戶，關閉「允許被加入好友」，禁止他人透過電話搜尋到你的LINE。✓

## ● 建立多重驗證機制

**Facebook**

1. 前往**帳號安全和登入設定**。
2. 向下捲動至**使用雙重驗證**，然後點擊**編輯**。
3. 選擇想要新增的帳號防護方式，並按照畫面上的指示操作。

在Facebook上設定雙重驗證時，系統會要求您從三種帳號防護方式中擇一設定：

- ✓ 在相容的裝置上點按**安全性金鑰**。
- ✓ 從**第三方驗證應用程式**取得登入碼。
- ✓ 從手機取得**簡訊（SMS）驗證碼**。

**Gmail**

1.開啟您的Google帳戶。
2.選取導覽面板上的**[安全性]**。
3.依序選取「登入 Google」底下的**[兩步驟驗證]**下一步**[開始使用]**。
4.按照畫面上的步驟操作。

值得注意的是，各種網路服務、程式介面中有關阻擋垃圾訊息、建立多重驗證機制等設定，其設定路徑經常隨著系統版本更新，一般而言系統及裝置都會定期進行自動更新，所以只要定時確保你的系統處於最新版本，基本上都可以找到相關設定！

## 2. 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。藉由網際網路「無國界」的特性，Twitter、Instagram、TikTok、Facebook、Email等等各式各樣的網路服務，都可以不受時間、地點的限制，讓世界各地的人得以交流，結交來自異國的朋友；但也由於網路「隱密」的特性，使得其中傳遞的訊息可能包含不真實的資訊，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，也常遇到一些網路求職陷阱，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：

### ● 網路交友之基本防範措施

**(1) 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。

**(2) 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。

**(3) 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。

### ● 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、治裝費用……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（https://gcis.nat.gov.tw/mainNew/）查詢該公司是否有合法登記。

### ● 網路釣魚

網路釣魚中所提供的超連結，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及檢查帳號，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，請注意網址是否為https（資訊加密協定）開頭，這能保障您在訊息的傳輸過程中具備一定程度的安全性。

## ● 網路交易

刑事警察局統計111年詐騙前三名其中假網拍和解除分期付款分佔一、三名，合計超過10,000多件，顯見網路交易詐騙仍居高不下，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，請民眾勿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、第三方支付或面交方式避免金錢損失

不論是賣家或買家，面交可以一手交錢一手交貨，當場確認物品及金額無誤後銀貨兩訖，是較有保障的方式，而尤其高單價的貨品，最好選擇標題所述的方式來進行交易，確保物品無虞，也能減少消費糾紛。此外亦提醒各位讀者面交時要注意自身安全。

### (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。

## 主題三　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。**

**在求職方面若遇詐騙可透過行政院勞工委員會服務專線1955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。**

## 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。

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全民防騙網」網站，民眾可以直接透過網站進行檢舉與報案。

民眾進入「165全民防騙網」網站後，可以根據實際的情況點選「我要檢舉」或「我要報案」，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。

而「165全民防騙網」除了提供線上檢舉與報案的服務之外，也提供許多豐富的資訊，如：高風險賣場、闢謠專區、反詐騙宣導、詐騙Line ID或境外帳戶之查詢等資料，讓民眾對於網路詐騙有更多的瞭解，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全民防騙網**
  網址：https://165.npa.gov.tw/

## 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之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「網路釣魚通報單一窗口」，現名為「釣魚網站通報」，此網頁可供填寫釣魚網站網址、行業類型，以及模仿對象位置等，再由專人統一受理通報與後續處理追蹤。

「釣魚網站通報」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。

民眾點入通報平臺後，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。

## iWIN網路內容防護機構

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）。

現今則改為「iWIN網路內容防護機構」網站（Institute of Watch Internet Network，https://i.win.org.tw）。

為了讓青少年及兒童有一個健康、安全的網路環境，「iWIN網路內容防護機構」網站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，民眾可以透過「iWIN網路內容防護機構」網站進行申訴。

線上申訴的類別分類分為：色情、暴力、恐怖、血腥、有害物品、其它違反有害兒少身心健康內容等六大類。

民眾若遇到相關有害兒少身心健康之網路內容，可透過「iWIN網路內容防護機構」網站進行申訴或通報，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臺服務提供者妥善處理，建立更為安全自由的網路空間。

# 主題四 防範網路詐騙的六個小撇步

**在本手冊的最末，我們將提供各位讀者以下6個防範網路詐騙的小撇步，請大家時時自我提醒與警惕，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

各式付費App尤其網路遊戲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或先享受付費服務，之後點數費用可以再連同手機帳單一起支付。

提醒遊戲玩家以及各位網路使用者，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消費。

## 2. 小心求證

當朋友以通訊軟體方式傳來訊息要向你借錢或請你幫忙買東西時，一定要用其他的方式再次求證，例如直接打電話詢問朋友，不要輕易地就答應對方的要求。如果只是網路上的好友，就算是談及愛情，也要留意是否可能遭到愛情詐騙。

## 3. 下載安裝前請三思

各種App或軟體也可能暗藏有詐騙的陷阱，在你決定下載App之前，請先確認它的存取權限，注意是否有不清楚的說明，也要多留意評論，如果評分過低，或存取權限不合理，像記帳App要求存取通訊錄、文書App要求定位、通話權限，甚至是要求輸入信用卡資料的，都要謹慎考慮是否使用。

## 4. 不隨意點選連結

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、通訊軟體訊息、社群平臺留言等處。

## 5. 設定安全的密碼

設定高強度的密碼以確保帳號安全，不要為了方便，把自己的所有網路服務都設定為同一組帳號與密碼！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。

## 6. 設定多重驗證機制

設定手機、Email帳戶的多重驗證機制，不管是什麼帳號，利用多重驗證機制多加一份保障，避免密碼被破解後帳號就被盜走。

## 參考資料

于郁金（2023，7月6日）。**南警戳破一頁式廣告詐騙　婦買車險遭詐騙100 萬**。勁報。https://news.owlting.com/articles/400806

王駿杰（2023，2月6日）。**竹市府遭冒用名義寄發惡意郵件　已報警呼籲民眾小心**。聯合新聞網。https://udn.com/news/story/7320/6953835

江昀蔓（2023，6月7日）。**詐團據點轉「高加索地區」　自願前往人數增。TVBS新聞網**。https://news.tvbs.com.tw/world/2145150

國家發展委員會（2020）。**109年數位發展調查報告**。https://ws.ndc.gov-.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJh-dG9yLzEwL2NrZmlsZS80M2FmZmM1Zi04NmU1LTQyYjEtOWQ3YS04ZTA1YTcyZGVmZjIucGRm&n=MTA55bm05pW45L2N55m85bGV6Kq%2f5p%2bl5aCx5ZGKKOWFrOWRiueJiCkucGRm&icon=.pdf

國家發展委員會（2021）。**110年國家數位發展研究報告**。https://ws.ndc.gov.tw/001/book/109-Digital/index.html#anchor-1

許國楨（2012，6月3日）。**假援交詐財　　工程師性沖沖存款**。自由時報。https://news.ltn.com.tw/news/society/paper/588836

郭政芬（2023，5月4日）。**竹北多起國中生被詐騙！家長急報案「同學都遭殃」**。聯合新聞網。https://udn.com/news/story/7320/7142649

新北市政府警察局土城分局（2018，7月24日）。**臉書出現政府機關假粉專！警呼籲網購族慎防詐騙**。https://www.tucheng.police.ntpc.gov-.tw/cp-530-48016-19.html

新北市政府警察局中和分局（2012，5月22日）。**解除分期付款詐騙手法又翻新，網購1,500元電腦桌被騙439萬！**。https://www.zhonghe.police.ntpc.gov.tw/cp-2450-5185-13.html

臺北市政府警察局中山分局（2015，5月10日）。**網購卡卡演唱會門票被騙，週來發生8件案例**。https://cs.police.gov.taipei/News_Content.aspx?n=661C9AFEA7BCE977&sms=78D644F2755ACCAA&s=6992373EB3ABAD4C

劉惠琴（2022，8月4日）。**LINE七夕情人節「熊大來送愛」免費下載貼圖是假的！2招破解詐騙手法**。自由時報。https://3c.ltn.com.tw/news/50458

鄭景議（2023，3月13日）。**分享假投資詐騙「養套殺」案例　刑事局：保證獲利絕對假**。自由時報。https://news.ltn.com.tw/news/society/breakingnews/4238298

警政署刑事警察局（2022，11月30日）。**警政統計通報（111年第48週）**。警政署統計室。https://www.npa.gov.tw/ch/app/data/list?module=wg057&id=2218&page=1&pageSize=15