

常見詐騙案例犯罪手法及預防方式一覽表 102年9月

詐騙犯罪手法	預防方式
<p>(一) 少女時代來臺，再現網購門票假賣家!</p> <p>少女時代於102年7月份來臺開唱，門票在6月15日開賣，雖然平均票價高達3400元，仍在當日下午就銷售一空，沒買到票的歌迷不願錯失目睹偶像丰采的機會，轉往拍賣網站購票，卻遇上假賣家行騙。</p> <p>根據165反詐騙諮詢專線統計，102年6月16日至25日間共有11位被害人出面報案，平均每人損失為新臺幣(以下同)1萬餘元。33歲的臺中陳先生於6月15日晚間，在網拍平臺上看到有人販賣少女時代門票，並留下LINE的聯絡方式，陳先生於是透過LINE與對方聯絡，對方要求先行匯款，但陳先生擔心不妥，還是請對方在網拍平臺開一個拍賣頁面，按照程序下標後，於晚間9點匯款2萬2,000元至對方指定帳戶，但不到5個小時過後，就收到網拍平臺所寄出的簡訊，通知該匯款帳號有安全之虞，已遭到停權，請陳先生勿再匯款。陳先生趕緊透過LINE及電話與對方聯絡，但已音訊全無，爰報警處理。</p>	<p>警方呼籲，話題性商品常遭假賣家利用行騙，尤其外國團體來臺開演唱會的門票，更經常成為詐騙工具，歌迷於網路上購買此類型商品務必提高警覺。網路拍賣應慎選賣家，除觀察評價、賣場狀況外，宜利用輕鬆付等第三方付費機制，可提高保障，並切勿私下交易，以免投訴無門。有任何與詐騙相關之問題，歡迎撥打165反詐騙諮詢專線查詢。</p>

常見詐騙案例犯罪手法及預防方式一覽表 102年9月

詐騙犯罪手法	預防方式
<p>(二) 魔鬼藏在細節裡，假電郵騙取企業匯款，多家公司損失千萬</p> <p>詐騙集團將觸手伸向企業，日前接獲企業報案，有歹徒利用電子郵件地址相似度極高的假郵件，如 l 或 l、w 與 vv 或長串英文字母中多或少 1 個字母等方式，騙取企業或客戶變更匯款帳戶，輕鬆取得企業客戶的信任而匯款，俟客戶反映未收到貨款時方知受騙。根據 165 犯詐騙諮詢專線統計，102 年上半年計發生 7 件企業遭假冒電郵騙取匯款案件，總損失近 2,100 萬元，各企業、會計或國貿人員應多加小心。</p> <p>在臺中經營橡膠接著劑的 J 公司，今年 3 月公司電子郵件遭到入侵，之後遭歹徒以相似度極高的假電子郵件，通知德國客戶變更匯款銀行帳號，俟德國公司來電確認是否收到匯款，J 公司方知遭到詐騙。本案歹徒係利用電子郵件地址字體小不易辨別，以及數字 l 與英文 l 的細微差異，輕鬆騙取德國廠商匯款 900 萬元。</p>	<p>警方在此呼籲，企業應與客戶建立多元聯繫管道，如遇有變更匯款帳戶情事，應有專人做多重確認，並檢視電子郵件地址是否正確，切莫僅憑電子郵件即匯款。有任何與詐騙相關疑問，歡迎撥打 165 反詐騙諮詢專線查證。</p>

常見詐騙案例犯罪手法及預防方式一覽表 102 年 9 月

詐騙犯罪手法	預防方式
<p>(三) 買餐券換現金，小心債務整合陷阱</p> <p>年約 50 歲的基隆林小姐某日接到資產管理顧問公司黃小姐來電，詢問是否有貸款需求，可以協助整合債務，並且可以代為向銀行申請低利、高額的貸款，林小姐因向 4 家銀行積欠卡債約新臺幣（以下同）50 萬元，於是與對方相約出面瞭解詳情。黃小姐碰面後以複雜的計算公式告訴林小姐，可以協助將還款利率降到最低，每月只需要付 8,000 元即可，林小姐於是同意並簽署委託書。而後黃小姐又聲稱因為與王品業務熟識，可以用購買禮券的方式來換取現金救急，黃小姐於是又用已經積欠卡債的 4 張信用卡，購買上千張王品集團旗下之餐廳禮券，消費金額高達 68 萬元，而後黃小姐協助轉賣，竟然只有匯給林小姐 58 萬元，林小姐向黃小姐確認時，她才告知必須扣除代辦費用 10 萬元，林小姐質疑為何需要收取如此高額的代辦費用，亦未事先說明，同時又揹負更高額的卡債，氣得出面向警方報案。</p> <p>日前亦有檢警單位破獲詐騙集團，以債務整合名義向卡債族聲稱與債權銀行有特約關係，可協助降低利率還款，並事先收取勞務報酬費，而後被害人發現卡債並未降息才驚覺上當。</p>	<p>警方呼籲，辦理貸款時應直接向金融機構臨櫃詢問辦理，以瞭解自身權益，以及作業程序、內容及條件等重要訊息，切勿聽信不明來電簡訊或網路訊息，以免自身權益受損。另外，切勿聽信陌生人任何說辭而交付個人身分證、信用卡等重要證件，以免遭不法利用。面對詐騙變化球，請多加利用 165 反詐騙諮詢專線。</p>

常見詐騙案例犯罪手法及預防方式一覽表 102 年 9 月

詐騙犯罪手法	預防方式
<p>(四) 小心!假防毒軟體詐騙你的信用卡資料</p> <p>家住新北市的王同學今年 7 月在家使用電腦，因誤觸釣魚網站，導致電腦中毒，隨後頁面出現若要解除，需購買防毒軟體，王同學不疑有他，線上刷卡付費後，還是無法解除中毒，方覺遭到詐騙。由於電腦中毒後先顯示掃毒畫面，之後出現微軟公司的安全性警告以及網路無法執行，再來顯示假的掃毒結果及病毒來源等資料，即便使用者重新開機，電腦畫面顯示的是無法使用的藍底白字的說明畫面，或是假的微軟開機畫面，告知使用者須購買防毒軟體。歹徒以假冒微軟公司的圖像，加上使用者受騙付款後會收到假的解毒軟體及金鑰，更讓民眾無法分辨是否遭到詐騙。</p>	<p>警方呼籲民眾不要隨易點擊來路不明的電郵附件和網路連結，並熟悉自己電腦裡所使用的防毒軟體，包括廠牌名稱、病毒警示視窗，以及更新程式與病毒碼的方法，以及定期更新。如果跳出的警示視窗的廠牌標示，與所使用的防毒軟體不同，那就很有可能是假防毒軟體。此外，沒有一款防毒軟體會採用付費掃瞄及清理電腦的方式，請民眾勿輕易上當，有任何與詐騙相關疑問，歡迎撥打 165 反詐騙諮詢專線查證。</p>

~~以上資料摘錄自內政部警政署刑事警察局及 165 反詐騙網站~~