

## 常見詐騙案例犯罪手法及預防方式一覽表 100 年 4 月

詐騙犯罪手法	預防方式
<p><b>(一) 外拍型錄要求提供商品？店家請小心防騙！</b></p> <p>丁同學於臺北地區一家專賣背包皮件連鎖店當工讀生，晚上 18 時接到自稱公司總經理來電，詢問店內最近業績狀況，然後表示正在附近外拍型錄，要丁同學把店裡幾款特定商品送過去拍攝，另以臨時須購買高價底片為由，要求丁同學攜帶現金 7,000 元一併交付。丁同學不疑有他，按照指示換穿公司制服，打包了 10 個包包及現金，火速送至鄰近路口。丁同學下班返家後，愈想愈奇怪，打電話向店長查證，才知遭到詐騙。</p>	<p>警方呼籲商家應加強教育員工，接獲類似電話，務必先與公司聯繫確認，如有任何疑問，最好立即撥打 165 反詐騙專線查證，以防受騙上當！</p>

常見詐騙案例犯罪手法及預防方式一覽表 100 年 4 月

詐騙犯罪手法	預防方式
<p><b>(二) 春吶音樂祭民宿一位難求，詐騙集團藉機行騙！</b></p> <p>臺中市鄭小姐(73 年次，服務業)為了春吶音樂祭訂房已經打了 10 通電話，向多家民宿及旅館聯繫皆碰壁，因此當搜尋到「四季庭園民宿、日租 990 (春吶尚有房間)」網頁時喜出望外，馬上依上面的手機號碼聯繫，得知尚有空房後，不但疏於查證就下訂，且立即外出將訂金 4,580 元匯入對方提供之帳戶。直到 3 日後，鄭小姐欲詢問民宿設施、地點、機車租賃等細節，再致電民宿業者，對方卻稱該手機門號已換新用戶，鄭小姐才知遭到詐騙。</p>	<p>警方呼籲網路預訂民宿，最好利用交通部觀光局或各縣市政府觀光局網站來搜尋經註冊認證的合法業者，才有保障，另在下訂匯款前，務必詢問交通位址、服務設施等細節內容，並透過其他管道查證，避免受騙。如有任何疑問，最好立即撥打 165 反詐騙專線查證。</p>

常見詐騙案例犯罪手法及預防方式一覽表 100 年 4 月

詐騙犯罪手法	預防方式
<p><b>(三) 歹徒佯稱以自動提款機解除分期付款方式，進行詐騙案例！</b></p> <p>臺中市謝小姐於今年 1 月間，於直銷公司網站訂購營養食品，使用信用卡線上付費，並順利收受貨物後，於 3 月底接獲自稱該公司人員來電表示當初匯款誤設分期付款，為保障其權益，將代為聯絡銀行協助取消分期付款約定，謝小姐隨即接到銀行客服人員來電，請其前往 ATM 按指示重新設定，最後發現被騙 59,956 元。</p> <p>新北市蔡小姐則於某公司直營分店購買化妝品，當場刷卡付款完成交易，於 2 個月後接獲自稱該公司人員來電，謊稱作業人員疏失記帳錯誤，導致誤設分期扣款轉帳約定，將造成蔡小姐連續按月扣款的損失，並請蔡小姐至 ATM 操作，以取消分期付款設定，實際上卻是詐騙蔡小姐將 29,978 元轉入詐騙人頭帳戶。</p>	<p>警方呼籲自動提(存)款機只有提(存)款或匯錢轉出的功能，無法設定或解除分期付款，只要聽到任何人指稱「至自動提(存)款機操作，以解除分期付款」說詞，必屬詐騙，千萬不可聽信操作。如有任何疑問，最好立即撥打 165 反詐騙專線查證。</p>

常見詐騙案例犯罪手法及預防方式一覽表 100 年 4 月

詐騙犯罪手法	預防方式
<p><b>(四) 即時通訊軟體詐騙手法簡介及防制！</b></p> <p>網路通訊發達，即時通訊及社群網站已融入日常生活中，人們已習慣以文字交談，對網路另一端帳號使用者是否為本人通常毫無警覺，詐欺集團看重此一特性，結合駭客盜取 MSN、Yahoo 即時通、Skype 及 Facebook 等網路通訊服務之帳號密碼，冒充該帳號身分針對通訊錄名單進行詐騙，從早期以借錢為由要求匯款之手法，隨著現今網路遊戲發展迅速，遊戲幣及遊戲寶物交易日趨方便，開始轉變成要求好友代買遊戲點數，騙取交易序號及密碼，再透過遊戲寶物交易平台快速洗錢獲取大量不法所得。</p> <p>綜觀此等詐騙手法，大多經由駭客散佈木馬程式及架設釣魚網站等不法手段，搜集大量帳號密碼賣給詐騙集團，經詐騙集團逐一檢視該帳號所申填相關資料及好友名單多寡，進行網路資料拼圖，過濾出詐騙成功可能性高之帳號，再進行修改相關認證資料及登入密碼，致使該帳號使用人無法登入，詐騙集團便利用這段期間偽冒該帳號者使用者身分進行詐騙。</p>	<p>警方呼籲使用電腦應有資安觀念，駭客常藉網路論壇、P2P 等管道散佈盜版軟體、文書檔案、PDF 檔案、影音檔等誘騙使用者下載讀取，藉此植入木馬程式，並透過電腦蠕蟲以電子郵件、即時通訊軟體散佈假登入頁面之釣魚網站或已遭入侵植入惡意程式碼之網頁連結，誘騙使用者點擊連結，因此使用者勿任意下載讀取來源不明之電腦檔案及開啟不明網頁連結，以減少帳號密碼遭盜取之風險。有任何疑問，最好立即撥打 165 反詐騙專線查證。</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~~