

常見詐騙案例犯罪手法及預防方式一覽表 103年2月

詐騙犯罪手法	預防方式
<p><b>(一) 手機接獲不明簡訊連結，請小心誤觸!</b></p> <p>邇來 165 反詐騙諮詢專線接獲民眾檢舉或報案，於手機接獲不明簡訊，內文有提供連結，一旦點選即開始安裝應用程式或下載檔案，甚至有被害人因此遭小額付費扣款，請民眾務必提高警覺。</p> <p>桃園的吳先生於 8 月份接獲手機簡訊，內容是：「是吳○○么？老同學來看我現在的相片能想起來我是誰嗎^^ 安卓手機這裡看 <a href="http://photo.appphoto.net/">http://photo.appphoto.net/</a>」。吳先生好奇心驅使下，點選連結後，便依照網頁指示下載檔名為.apk 的手機應用軟體，之後螢幕就跑出一些人物照片，但不到一個小時後，竟接獲電信公司傳來的小額付費簡訊通知，才驚覺受騙上當，損失金額新臺幣 6,000 元整。經點選簡訊內所提供之網頁連結後，網頁上聲稱為方便下載，該程式未上傳至 google play 應用市場，並於網頁中指導如何修改手機設定，實則是讓民眾取消手機的安全設定，以下載未經官方審核的手機應用程式。</p> <p>除上開案例外，另有 3 位民眾亦於同一個月內接獲「○○○被偷拍的是你嗎？<a href="http://199.101.117.21/index.php">http://199.101.117.21/index.php</a>」的不明簡訊，其中一位民眾於點選後出現色情照片，嚇得趕緊將手機關機，此舉讓該應用程式無法繼續執行，事後向電信公司查詢，所幸未遭小額付費扣款。</p>	<p>雖然簡訊文字使用大陸用語，國內民眾不易上當，但因簡訊內容開頭稱呼是手機持有人之姓名，造成被害人誤信為友人所傳而降低戒心，進而點選連結而下載不當檔案或程式。警方呼籲，沒有上架於 google play 應用市場 (android 系統) 的手機應用程式未經安全審核，風險極高，切勿下載使用，如誤觸下載則不要執行並盡速移除。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 103 年 2 月

詐騙犯罪手法	預防方式
<p><b>(二) 電子郵件辦案詐騙手法再現，請小心誤上當！</b></p> <p>今年初 165 接獲 6 通檢舉電話，均是民眾收到以臺北市政府警察局為名義發出的電子郵件，除要求收件者配合辦案外，還有附加檔案。上個月又有民眾接獲相似的電子郵件，請民眾務必提高警覺，切勿點選附加檔，以免誤中木馬病毒。</p> <p>臺北的吳先生於上個月接到一封主旨為「吳○○調查函—臺北市政府警察局」的電子郵件，寄件者署名陳安銘警員，郵件內容則是經濟詐騙事件成立通知書，全文以公文書方式呈現，內容如下：「近日接一市民到我警局舉報壹宗經濟詐騙案件，警方已經就這宗案件進行調查，…請和我們保持聯絡（應為絡），9 月 2 日前請回覆郵件，以便邀請妳返回警局作進一步查詢…，請協助我們調查，以免帶來不必要的麻煩。詐騙事件成立，請查照附件詳情。」吳先生看到 email 內容一度以為真得是警察局發出的正式公文，趕緊去電臺北市政府警察局查證，市警局告知該發文字號並非警察局所發出的公文，而後再向 165 確認是詐騙手法後，才放心地將信件刪除。</p> <p>今年初已有 6 位民眾反映接獲假警察辦案之電子郵件，上個月又再度現蹤，歹徒疑似掌握當事人姓名及電子郵件帳號，以假檢警方式進行詐騙，且郵件還另有附加檔案，恐挾帶病毒，以攻擊收件者的電腦，竊取更多個人資料。</p>	<p>警方呼籲，檢警單位辦案，會以掛號或警察親送的方式送達正式公文書，絕不會以傳真或電子郵件處理，另外，不輕易開電子郵件附加檔、不隨意點選網站連結，是資訊安全的重要原則，有任何與詐騙相關的疑問，歡迎撥打 165 反詐騙諮詢專線查證。</p>

~~以上資料摘錄自新北市新莊區公所-新北公告~~