

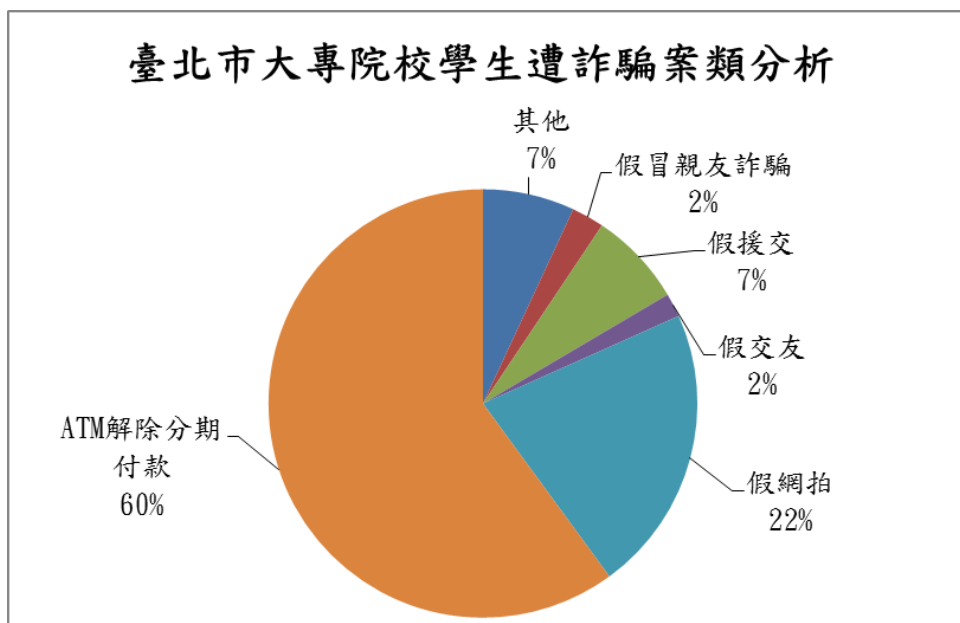
大專院校學生反詐騙宣導資料

壹、前言

近年來臺灣電子商務產業蓬勃發展，電子商務業者擁有大量會員個資及交易明細，卻未有完善的資安保護措施，導致民眾個資嚴重外洩，使得歹徒更有機會遂行詐騙。加上遊戲產業的蓬勃發展，也造成遊戲點數成為歹徒詐騙標的及洗錢管道，而大專院校學生因社會經驗及防詐騙意識不足，容易陷入歹徒所設詐騙情境。

貳、學生受騙案類統計

內政部警政署 165 反詐騙諮詢專線統計 106 年 1 月 1 日至 6 月 9 日詐騙被害資料，臺北市受理詐欺案件計 3,100 件，其中被害人為大專院校學生之案件計 448 件，占總數 14.45%。另大專院校學生遭詐騙最多案類為拍賣（購物）詐騙，計 366 件，占 81.70%，其中包含 ATM 解除分期付款案件計 269 件（73.5%）及假網拍詐騙計 97 件（26.5%）；次之為假援交、假交友詐騙，計 40 件；再次之為假冒親友詐騙（含猜猜我是誰、盜用 LINE 及網路帳號），計 11 件；其他案類（含假冒公務機關、信用卡盜刷等）計 31 件。



參、 學生常見詐騙手法及案例

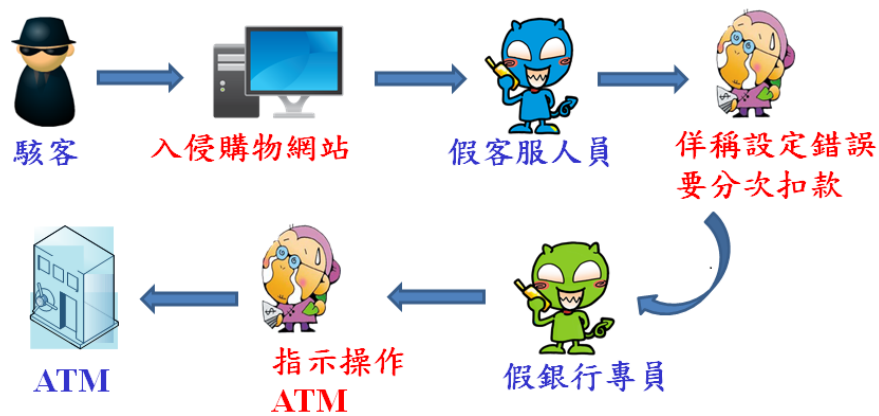
一、 解除分期付款詐騙

(一) 詐騙手法

詐騙歹徒取得網購(拍)交易個資後，竄改來電顯號假冒網購(拍)平臺客服人員，先與被害人核對交易資料以取信被害人，接著謊稱因人員作業疏失將該筆交易誤設為分期付款、誤刷重複訂購條碼或誤刷成經銷商條碼，將造成重複扣款，並詢問被害人的銀行帳戶，表示會請該銀行人員與被害人聯絡。

詐騙集團接著假冒銀行人員，要求被害人至附近 ATM 依指示操作解除設定，更甚者謊稱民眾解除設定動作太慢或操作錯誤，造成資料卡在系統內，要購買遊戲點數才能將資料洗出退款等，再次詐騙遊戲點數，造成民眾財產重大損失。

解除分期付款詐騙流程



(二) 案例

一名許姓大學生日前在「TAAZE 讀冊生活」購買數本新書，日前接到假冒 TAAZE 讀冊生活的客服人員來電，表示因為超商店員的疏失誤刷條碼，將許男的訂單刷成批發商的訂單，導致將會從許男的帳戶扣款 12 本書的費用，並要許男別擔心，銀行客服人員會協助操作解除設定。10 分鐘後，許男接獲自稱郵局客服人員的來電，要求許男至郵局操作解除 ATM 分期付款設定取消訂單，

在對方的指示下，許男從自己戶頭匯出 2 萬 9,985 元至對方提供的帳戶，直到查詢帳戶餘額時發現存款短少，才知道受騙，趕緊向警方報案。

(三) 防騙注意事項

- (1) 網路購物、訂票、訂房及銀行客服人員不會以電話通知帳戶設定錯誤變成 12 期分期付款。
- (2) ATM 沒有解除設定的功能，無法解除分期付款設定錯誤，遊戲點數卡亦無解除帳戶設定功能。千萬不要依陌生人指示操作 ATM 或購買遊戲點數，以免受騙。
- (3) 歹徒會以篡改電話號碼技術，將來電竄改為公務機關、網拍公司或是銀行客服人員電話，如果看到字頭為「+」，後面為區域號碼的來電（如+02、+2、+8862xxxxxxxx），就是從國外打來的篡改電話，要特別注意。

二、假網拍詐騙

(一) 詐騙手法

詐騙歹徒於網拍平臺或臉書社團，假意出售低於行情價的商品，如高單價 3C 電子產品(智慧型手機、數位相機)、熱門商品(如演唱會門票、限量球鞋)等，誘使網友購買。

當買家與假賣家聯繫後，詐騙集團會要求用 FB 或 LINE 私下連繫交易事宜，並提供銀行帳號催促買家儘快匯款，待買家匯款後旋即關閉 FB、LINE 帳號，讓被害人求助無門。

(二) 案例

藝人 Hebe 田馥甄巡迴演唱會門票開賣秒殺，24 歲張女沒搶到票，只好在臉書「演唱會讓票、換票、求票」社團貼文求票。隔天早上，收到化名「小琳」的臉友私訊表示願意以原價 3 張票共 1 萬 2600 元讓給張女，只要先匯款再憑序號自行去超商取票即可。雙方用 LINE 談妥，張女隨即依約將票款全數匯給對方，對方也傳來取票序號和身分證號碼，張女趕到附近的超商取票，

沒想到超商機台竟連連出現號碼錯誤的訊息，無法領票，對方也人間蒸發，才驚覺上當。

(三) 防騙注意事項

- (1) 網路上低於市價太多的商品可能有詐，若賣家要求使用 FB 或 LINE 私下交易，要特別提高警覺。
- (2) 網路購物最好使用有提供第三方支付的交易平臺、選擇評家良好、有實體店面的賣家，或堅持面交，以保障自身財產安全。

三、 假援交詐騙

(一) 詐騙手法

詐騙集團假冒年輕貌美女生，透過社群網站、交友軟體尋找被害人，加入 LINE 好友後，謊稱有兼職援交，並以遊戲點數取代現金交易可規避警方查緝、要先繳交保證金等說詞，要求被害人購買遊戲點數。被害人如拒絕或不從時，則由另一自稱是黑道兄弟恐嚇被害人，稱握有被害人資料將對其不利，造成被害人心理恐懼而依其指示照辦。



(二) 案例

一名張男張姓男大生在網路交友平台認識名為「嬌嬌」的網友，與「嬌嬌」互加 LINE 成為好友後，嬌嬌訴說家裡欠高利貸，需靠援交還債，如果不嫌棄她，「願意在一起」，張男得知她援交

價碼兩小時 3 千元，決定花錢捧場，盼她早日脫離火坑，嬌嬌卻說「公司擔心警方查緝」，要求張男至超商購買遊戲點數，再將序號、密碼傳給她。

不久，張男接到自稱「小吳」的男子來電表示，3 千元收到了，但怕是警方釣魚，要求再買 1 萬元當保證金，此時嬌嬌不斷以噓寒問暖等溫情攻勢，張男盛情難卻，前後共買 2 萬元遊戲點數，沒想到小吳又傳恐嚇訊息再要 1 萬元，靠打工當生活費的張男身上沒錢了，將此事告知朋友，才知遇詐，趕緊到派出所報案。

(三) 防騙注意事項

- (1) 交友網站或通訊軟體的照片、人名很容易虛擬造假，不應輕信。
- (2) 網友交往談及金錢，可能有詐，切勿依對方指示購買遊戲點數或匯款，以免遭詐。

四、盜用 LINE 帳號及假親友詐騙

(一) 詐騙手法

(1) 歹徒以亂槍打鳥方式撥打詐騙電話，冒充被害人親友，再以受傷住院、資金週轉、欠債等理由，要求被害人匯款到指定帳戶。此外，詐騙集團也常利用盜用 LINE 帳號後，再假冒親友傳送借錢訊息詐騙。

(2) 詐騙集團盜用 LINE 三步驟：

- 【步驟 1】：先入侵朋友 A 的 臉書或其他通訊軟體帳號，以朋友名義詢問您的電話號碼。
- 【步驟 2】：當您提供電話號碼後，詐騙集團利用電腦「手機註冊新帳號」輸入您提供的手機號碼，此時 LINE 會發一封簡訊認證碼到您的手機。
- 【步驟 3】：歹徒誣稱他的 LINE 重新登入，須請朋友代收「驗證碼」提供給他，當你將簡訊中的四位數驗證碼提

供後，歹徒即成功盜用 LINE，並廣發訊息向您的親朋好友借錢。

(二) 案例

劉女士月初接獲自稱友人鄭小姐的來電，對方聲稱買新手機換了號碼，要劉女士重新加 LINE 好友。隔日，對方再度來電，稱兒子投資急需用錢，希望劉女士幫忙匯錢到指定帳戶，劉女士不疑有他，照著對方 LINE 傳送過來的帳號匯了 68 萬元，匯款後才想到打電話到鄭小姐的公司求證，驚覺受騙。

(三) 防騙注意事項

- (1) 接到久未連絡的親友電話或訊息，聲稱換了電話號碼、有急需用需要借錢等，都應提高警覺。
- (2) 遇到親友用電話或 LINE 借錢的情況，可以故意說錯的事情或名字測試對方，或以親友原本的電話或其他管道詳加查證，並直接約見面，以免受騙。
- (3) 為避免 LINE 帳號被盜用，應注重以下資訊安全：
 - 1、google 密碼不要使用傻瓜密碼，並設定兩階段認證，以免通訊錄資料外洩。
 - 2、LINE 開啟「阻擋訊息」功能，阻擋非好友的廣告及詐騙訊息。
 - 3、LINE 關閉「公開 ID」功能，避免遭陌生人亂加入好友。
 - 4、LINE 關閉「允許其他裝置登入」功能，避免駭客從電腦登入您的帳號。
 - 5、LINE 公司經由簡訊所傳送的四位數驗證碼為自身帳號密碼，如同任何帳號密碼一樣重要，不應幫人代收且不可告知任何人，以免帳號遭盜用。

肆、 結論

近年來網路詐騙犯罪快速發展而更趨複雜，在校學生平日忙於課業，較少接收到外界資訊，且使用網路購物、交友的頻率高，容易落入詐騙集團佈下的網路詐騙陷阱。

內政部警政署於 103 年建立「165 防詐騙宣導」LINE 官方帳號、「165 反詐騙宣導」FB 粉絲專頁，本局亦於 103 年建立「反詐騙小金剛」FB 粉絲專頁，即時更新的常見的詐騙案例及防範之道，以提升民眾反詐騙意識，歡迎學校師生隨時上網瀏覽。此外，詐騙手法日新月異，建議學生應養成看新聞的習慣，以隨時獲知反詐騙新知，保障自身財產安全。