

網路、「亡」路，詐騙我們的心



文/督導員郭欣怡

E世代的發達，網路讓我們生活、資訊便捷，但也因為隱匿的特性，而容易被人利用來做犯罪的工具，身為E世代的父母，我們不得不去了解及協助孩子避免發生網路詐騙的事件。

網路詐騙手法的心理動機：1、利用網路便利性。2、利用網路隱匿性。3、利用民眾同情心。4、抓住民眾好奇心。5、抓住民眾貪念心。

網路詐騙常見案例

《資料來源：165全民防騙超連結》

1、網路援交詐騙

詐騙常見用語～

- 女網友主動邀約見面。
- 見面前要去自動提款機。
- 以自動提款機匯援交費。
- 要辨識身分。
- 自動提款機操作錯誤
- 黑道分子恐嚇要配合更正錯誤。

2、購物個資外洩詐騙

詐騙常見用語～

- 核對網購商品、日期、金額。
- 通知帳戶設定錯誤，變成分期付款。
- 郵局或銀行來電協助解除設定。
- 要去自動提款機取消設定。

3、求職詐騙

詐騙常見用語～

- 網路刊登徵人廣告。
- 廣告只刊登行動電話。
- 電話中要求至車站、超商等公共場所面試。
- 要求交出金融卡或到自動提款機辦理薪資入帳。
- 要求先付保證金或裝置費。
- 要求申辦行動電話。

4、中獎、投資詐騙

詐騙常見用語～

- 網友在海外是六合彩、賽馬會、投資顧問公司職員！提供投資機會！
- 電話通知您已獲利，快去匯款贖回獲利！
- 海關查獲地下匯兌，要付關說費。

預防網路詐騙，家長可以協助少年安全上網方法：

- 1、透過中華電信申請上網時間管理服務，避免孩子過度使用電腦、沉迷網路遊戲。
- 2、透過中華電信申請色情守門員，可以防堵有害資訊，拒絕不良網站。
- 3、隨時留意孩子使用網路情形，教導孩子了解網路上存在的危險。
- 4、陪伴孩子一起面對被網路詐騙的不愉快經驗。
- 5、家長以身作則，正確使用網路。

建構安全網路之相關資源

◎網站

- | | |
|--------------|---|
| 165民防騙超連結 | http://www.165.gov.tw/index.aspx |
| HiNet健康上網 | http://hicare.hinet.net/index.html |
| iWIN網路內容防護機構 | http://www.win.org.tw/iwin/index.html |
| CAP白絲帶關懷協會 | http://www.cyberangel.org.tw/tw/ |

◎諮詢電話

- | | |
|-----------------|----------------|
| 反詐騙諮詢專線 | 165 |
| 白絲帶關懷協會家庭網安熱線電話 | (02) 3393-1885 |

看不見的陷阱

文/社工員傅翔立

小布前一陣子因為手機壞了，所以便上網想說有沒有便宜的二手機可以買，發現有一個賣家賣Iphone5空機64G只要9900元，對方說他是續約月租2000多元的費率，手機是0元，如果賣不出去就要送朋友，小布心想這價格也太便宜了，於是馬上用即時通跟他連絡。因為對方的評價是0，怕被騙，所以小布要求對方提供當初跟電信公司辦理的購買證明以及手機外盒的序號照片給小布，確認無誤就下標，不久後對方寄來了一張發票的照片，但沒日期，而且發票開立地點與商品網頁的地點不同，讓小布非常疑惑。正在思考是否下標的同時，突然收到拍賣網站寄來的信，說明賣家帳號已被停權，小布才驚覺對方是詐騙分子。這次經驗讓小布知道在網路上買太便宜的東西就有被詐騙的風險，還好小布還沒匯款付錢，不然就虧大了！

網路購物安全嗎？其實網路購物的安全程度跟一般的購物沒有兩樣，只是近幾年使用網路購物的比例逐漸上升，因此不肖人士自然就跟著多了起來。害人之心不可有，但防人之心不可無，知己知彼，百戰百勝，下面就讓我們來看看網路詐騙的實際情形與破解方式吧！

狀況一：網路拍賣的陷阱-這裡有隻手機好便宜!還不快來買。



一支高檔手機全新品只賣你6千元?天底下哪有這麼好的事啊!!

防詐騙訣竅:

- 1.注意網路商品與一般市價是否相當，若差距過大則風險較多，切勿抱持貪小便宜的心態。
- 2.選擇有信譽的拍賣網站或購物網站，並瞭解賣方的信用、風評等，並注意網址是否為仿冒網站。
- 3.網路購物盡可能以貨到付款或見面交易為主，以確認貨真價實。

狀況二：LINE的友情請求-你可以幫我個忙嗎?



不過是上網買個東西，哪需要這麼多資料啊!!

防詐騙訣竅:

- 1.觀察好友的用詞語氣是否與平常有所不同。
- 2.不輕易出借手機傳遞訊息，以防小額付款詐騙。

狀況三：LINE的超連結陷阱-可以幫我投票嗎?



我怎麼都不知道你朋友如此多才多藝，想唬我沒這麼容易!!!!

防詐騙訣竅:

- 1.仔細觀察連結網址是否為熟知的網頁。
- 2.再三與朋友確認活動訊息的真偽，不隨意點入連結。

結語:

網路詐騙手法多樣，且受騙案例層出不窮，若是不小心，極有可能成為受害者，因此須時時保持警覺，才能享受網路帶來的便利生活。

我與少輔組的故事

文/少年木木

認識少輔組到現在已經好幾年了，我從國中開始接觸，因為自己不喜歡念書，人生又沒有什麼目標與方向，喜歡跟朋友在一起，就開始會有些偏差的行為，然後跟朋友一起出去打架，被警察抓到有案子，陸陸續續的進出少觀所三次。

說真的剛開始被他們輔導覺得很煩，總是覺得他們很囉唆，每個禮拜都會來學校輔導我，問我最近過的怎樣，有沒有出狀況，我都會覺得這些根本對我一點幫助都沒有，唯一覺得比較好的就是可以做一些測驗讓我知道自己是怎樣的人，有什麼人格特質，其他的我都是有點敷衍的帶過。

我一開始覺得在外面打架或惹事都沒什麼，反正被抓到就去法院開庭跟對方和解就沒事了，到了第一次被法官判收容到少觀護所一個多月，進去時還沒有想很多，直到媽媽大老遠的來看我，寄東西給我吃，那時我隔著玻璃看到媽媽，瞬間眼淚就流個不停，哭到話都說不太出來，只有跟媽媽道歉請她不用擔心，我會照顧自己，那時候真的好後悔，後悔自己為什麼要這樣讓家裡人擔心，以後我一定不會再讓他們擔心了！

出去後社工跟媽媽都有提醒我，要我記得在裡面所反省的，不要再進去了，但我還是漸漸的把在裡面反省的事給忘掉，繼續跟那些朋友玩在一起，朋友找我去打架，我也都僥倖的覺得自己不會這麼倒楣被抓到，結果還是被抓到了，就這樣我又進去了第二次，收容兩個月，這次出來

後知道自己再犯案子就不會是收容一兩個月，可能就是一兩年的感化教育，開始會告訴自己，什麼該做什麼不該做，但一樣都抱著僥倖的心態！

直到第三次被收容，自己知道可能會被判感化教育，又剛好在裡面過年，沒辦法回家和家人一起團聚，而且媽媽又剛好工作很忙一個月只能來看我一次，那時候的我心情都沒有很好，睡覺也都睡不好，這大概是我最低潮的時候吧，只有社工能夠每個禮拜來看我，那時我都把內心深處的話告訴社工，社工也慢慢的輔導我，讓我心情不會那麼差，我真的很感動她可以一直陪我度過那些日子。

媽媽和社工來看我時跟我說：「自己做錯要自己面對，要真的在裡面好好反省，想想自己的未來，不要好了傷疤就忘了痛，不能再一直僥倖的去做事情。」聽到這些話我才真的清楚知道，誰是真的對我有幫助，會在我需要幫助的時候陪伴我！在裡面我就告訴自己，如果我真的能夠出去，我一定不會再讓他們擔心，不會再浪費時間，要讓自己變成新的一個人，不會跟以前一樣！

除了家人，對我最有幫助的就是社工了，她從沒有放棄過我，一直在幫助我教了我很多事，也陪我度過人生低潮的時候，真的很感謝她，讓我能夠改變自己，如果國中沒有被輔導的話，我可能現在還在感化院裡面生活呢！

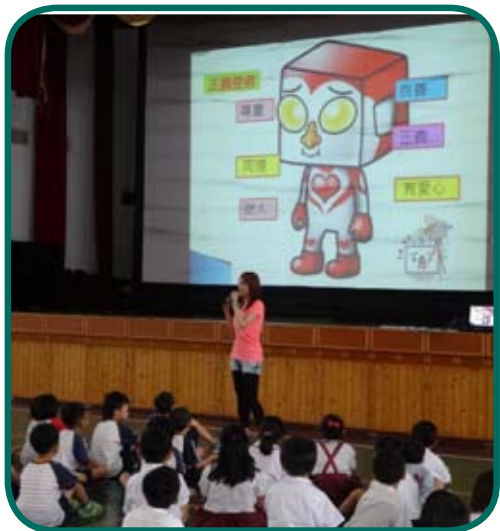
校園宣導 活動花絮



10/7北投少輔組泉源國小進行同儕衝突與傷害事件之預防宣導，學生十分活潑且反應熱烈。



10/30士林少輔組蘭雅國小校園宣導正確兩性關係與交友應注意事項，讓學生瞭解健康性別關係、性騷擾認識與自我保護。



9/29大同少輔組大橋國小校園宣導，透過活潑生動的簡報與宣導短片播放，增強學生如何避免同儕衝突(傷害)事件之知能，引起學生共鳴，反應熱烈，宣導成效佳。



9/30中山少輔組大佳國小校園宣導，透過動畫協助學生認識網路霸凌及可能觸犯的法律，再以真實的新聞案件加深學生印象，反應熱烈，頗受好評。

遊戲點數小額付費，騙徒施詐術，帳單父母付

文/松山分局少年事件防制官魏光廷

江太太的兒子現就讀國小五年級，平時在家喜歡玩橘子遊戲公司推出的網路遊戲，單純玩網路遊戲，沒想到竟會落入騙徒的圈套。

日前江太太發現家中室內電信帳單多了9筆購買遊戲點數消費，總計要繳4500元，追問兒子後才發現，是被網友以「外掛免費」誑騙，將家中電話及父母資料都告知網友。

某日江小弟在家中上網玩「爆爆王」，由網友指引進入聊天室，以取得「外掛免費」為由，要他告知住家電話號碼及母親身分證字號，聰明的江小弟跑到媽媽房間查看戶口名簿，沒多久歹徒回復一組6位數認證碼，江小弟誤以為這就是獲得免費外掛的憑證，經誘導使用自家電話撥打0800-085735，進入「中華電信免付費認證專線」輸入認證碼，對方又以認證失敗，就這樣反覆操作9次，遊戲點數全進了歹徒的網路帳戶，遭詐騙損失新臺幣4500元。

現今進入網路世代，網路遊戲勢不可擋，歹徒利用「市話小額付費」的簡易便捷，看準孩子對遊戲點數取得、購買方式並不清楚，也無法預料輕易告知父母親的電話及身分資料會有如此後果，歹徒只要以免費外掛程式誘惑，就很容易掉進詐騙陷阱。

警方提醒，民眾應妥慎保管個人資料，更要注意家裡的孩子，並告知詐騙手法，以避免遭詐騙青少年朋友涉世未深，甚至基於好奇而容易落入詐騙圈套，「冷靜」、「查證」、「報警」是防詐騙的不二法門。

親愛的讀者們：

看完本期的內容後，是否對於網路詐騙有更進一步的認識與了解！為了讓自己更清楚吸收多少，來個隨堂測驗吧！答案公布在第四版的右上角喔！

- () (1) 網路詐騙，沒那麼衰!! 絕對不會輪到我。
- () (2) 朋友傳LINE叫我協助代收簡訊、匯款，不需要查證趕快幫朋友的忙。
- () (3) 遇到不明的「+」字頭電話，需要小心謹慎、不輕易給予個人資料。
- () (4) 為避免手機小額付款詐騙手法，可向電信公司取消小額付款功能。
- () (5) 如遇疑似詐騙可撥打165求證。

大考驗

下期預告

用電腦、手機上網已經成為你不可或缺的习惯之一嗎？

你知道許多看似沒有傷害的留言，卻已經構成網路霸凌的行為嗎？

敬請期待下期少輔簡訊！



本期主題：

網路資訊安全與素養

主題摘要

1版 專家專欄

導讀
網路詐騙現況與預防策略

2版 親職專欄

網路、「亡」路，詐騙我們的心

3版 少年交流區

看不見的陷阱

4版 社區交流道

我與少輔組的故事
遊戲點數小額付費，騙徒施詐術，帳單父母付
校園宣導 活動花絮

中華郵政第1085號執照登記為雜誌交寄

2014年12月5號出版/月刊

發行人：黃昇勇
出版：臺北市政府警察局少年警察隊
地址：11080臺北市信義區信義路5段180號
網址：http://jad.tcpd.gov.tw
電話：(02) 2346-7585
主編：吳春沂
副主編：楊岱錚
編輯：簡世珪、汪志皇、鄧進華
顧問：陳永富
編輯小組：薛惠玲、郭欣怡、傅翔立、張頌琦



「為什麼匯款後賣家遲遲沒有寄送貨品啊??」、「怎麼莫名其妙，上個月的電話帳單多了一千多??」、「怎麼平常不會玩線上遊戲的媽媽，傳line要我幫他收簡訊認證碼呢?」這是近來的新興詐騙手法，無論是傳統的ATM轉帳、簡訊，到線上的網拍、電子郵件、Line、網址連結…等，透過手機、網路不斷傳送訊息，很容易讓懵懂無知的少年、一般民眾，不疑有他立即點選惡意網址、匯款、協助收認證碼。

網路詐騙之所以逐年攀升，就在於詐騙者藉由網路的普遍化、人手一機的盛行，以通訊軟體盜用熟識友人、家人帳號、偽裝拍賣網站賣家、遊戲軟體網址連結，卸除一般民眾心防。成年人有時也會被這樣的詐騙手法給迷惑而受騙，更遑論是未成年的孩子們。由於網路詐騙除了盜取個人身分資料、金錢外，還會藉由個人通訊軟體、手機通訊錄延伸至家人、好友，也讓其他人也遭受詐騙、身受其害，不但本身資料被盜用，也連帶盜用他人的身分資料，形成一連串的詐騙網路事件。

因此，本期邀請專家學者165專線組長論述網路詐騙的常見手法與預防策略；松山分局少防官，提供您小額付款的詐騙手法及預防方式；案例事件分析，透過本組社工員及少年被詐騙經驗分享，及提供家長如何與少年談防堵詐騙。內容精采，若您對於網路詐騙仍有許多擔憂與不了解，請跟著我們的腳步，一起看下去…

「網路詐騙現況與預防策略」

文/165反詐騙專線組長傅陣原

電信網路詐欺案件，俗稱網路詐騙，自89年起因網際網路日益發達，故情況趨於惡化，形成嚴重的治安問題，為因應此狀況，政府自92年起，除陸續推動多項警政偵防、金融管理及電信監理策略外，亦於93年4月26日設置「165反詐騙諮詢專線」，作為全民反詐騙主要樞紐，隨時掌握詐騙犯罪手法與模式，研擬對應策略，與跨部會合作建構反詐騙聯防網絡，獲致一定成效。根據統計，今年上網人口已多達1700萬人，隨著無線上網涵蓋率及智慧型手機的普及，資訊及通訊正式進入數位匯流時代，資訊流、物流、金流均已匯集於網路，招致犯罪者覬覦，開始轉向結合網路進行各類詐騙，問題有日益升高的現象。

壹、為預防受騙，對現今多元的詐騙手法則不可不知，目前常見的網路詐騙手法分述如下：

一、手機惡意連結犯罪手法

詐騙集團將惡意程式載於某特定網站，以隨機發送或盜取之帳號發送好友群組連結供被害人點選，點選連結後，會主動或要求下載惡意程式至手機內，此時遭嵌入惡意程式之手機會自動上傳手機資訊至詐騙集團設立之伺服器。

二、常見之LINE詐騙手法

駭客入侵好友LINE帳號取得通訊錄後，發出大量APP簡訊進行詐騙，以手機小額付費詐騙最多，或要求好友點選簡訊所夾帶之惡意網址(常為goo.gl縮址)使手機中毒後，駭客自遠端伺服器操控手機完成小額付費，詐取遊戲點數;至超商購買遊戲點數;或收取網路賣家手機註冊認證碼，等認證通過，歹徒即會展開網拍詐騙。

三、網拍詐欺

詐騙集團利用人頭電話認證註冊網路賣家帳號，或入侵LINE與手機，要求群組好友用手機撥打語音電話或收取認證碼，通過手機身份認證完成賣家註冊入侵賣家帳號，繼而以低價商品吸引買家購買，被害人匯款(轉帳)後，於約定期間未能收到貨後才驚覺被騙。

四、其他與遊戲點數有關的詐騙手法

- (一) 色情應召：歹徒假冒援交妹與被害人聊天約定進行性交易，要被害人先付保證金，並謊稱擔心警察人員釣魚，現已由遊戲點數取代現金交易，詐騙被害人至超商購買遊戲點數。
- (二) 猜猜我是誰：歹徒假冒超商的工程人員，謊稱要測試機台，詐騙店員操作如I-BON等機台，列出購買遊戲點數的帳單並進行掃描過卡後，將卡號提供，進而詐得遊戲點數。

貳、建議因應防制策略:

一、對於竄改電話提高警覺性：

迄今詐騙電話均由國外多層跳板輾轉至台灣居多。遇前面出現「+」字頭，後面為區域號碼的，即為國際篡改電話(如+02、+2、+8862xxxxxxx及不顯號)來電，多半均屬詐騙電話。接獲網購交易問題電話時，應主動尋求正確管道或撥打165專線查詢之觀念，而非僅依電話號碼相同即一味盲從電話指示操作。

二、LINE自我保護

- (一) LINE使用者，可開啟「隱私設定」中「阻擋訊息」的功能，開啟後，不論是廣告訊息或詐騙訊息都可有效防範。
- (二) 取消LINE「我的帳號」中「允許自其他裝置登入」，避免駭客取得的帳密後從電腦登入。
- (三) 非LINE好友傳送訊息時，注意是否有不明連結，該訊息上方有「您尚未將本用戶加入好友名單內」警告，判斷是否為名單內好友。
- (四) 不要點選訊息中的短網址連結(goo.gl、bit.ly等等)或IP連結，可先向發送訊息的朋友查證。
- (五) 向電信公司取消小額付款功能。
- (六) 不要下載來源不明或非官方認證應用程式，應在Google Play平台下載。
- (七) 下載應用程式時，應查看星等級數、使用者評論、APP的功能及介紹、「APP存取權限」和開發者的其他APP，以免下載惡意程式。
- (八) 取消勾選「設定」內的「安全性」中「未知的來源」，該功能若開啟，會同意來源不明的應用程式安裝在手機中，容易造成手機安全危害。
- (九) 如遇疑似詐騙可立即撥打165求證。

參、結語：

身為網路世代的一份子，我們必須知道網路世界無遠弗屆，縮短人與人溝通的距離，伴隨電子商務的快速成長，帶動線上金融支付龐大需求，進行購物交流的可能也將趨於頻繁，為免遭不法人士利用網路進行各種新型態的智慧型犯罪，資安防護雖為第一道關卡，但用戶自身的帳號密碼保護及深化預防網路犯罪的相關知能更為重要，多一分用心，少一分風險的承擔。