

網路及線上遊戲常見的詐騙手法與因應

陳益智

資策會科技法律中心副組長

壹、前言

臺灣相關資通訊網路產業過去十多年來，在電信自由化及網路相關技術的研發日新月異的雙重助力下，價格低廉、幾乎每個家庭都負擔得起的寬頻普及，使網路發展快速，得以造福民眾與企業。根據資策會FIND／經濟部技術處「創新資訊應用研究計畫」統計，臺灣在2006年第一季經常上網人口為963萬人，網際網路連網應用普及率為42%。在2005年全球寬頻網路用戶普及率中，臺灣位居第11名。

隨著網路的發展，線上遊戲也跟著成長，在94年我國線上遊戲產業的產值已經超過新臺幣百億元，而參與線上遊戲的消費者，也已經超過288萬人¹；不過相對的，根據去年（95年）警政統計通報，95年1-7月間發生的電腦網路犯罪發生數也高達12,568件²，主要為妨害電腦使用4,966件（占39.51%）為最多，詐欺案3,885件（占30.91%）次之，違反兒童及少年性交易防制條例1,663件（占13.23%）第3位³。

由於沒有現實世界中那樣有形有體、可觸可感的界限和障礙，很多人也認為網路遊戲世界是虛擬的，在這個網路遊戲中的所作所為並不會有現實的危害性，有些網路使用者容易在好奇心的驅使下，越過

法律的界限。網際網路突破空間限制的特性，確實帶給社會許多便利，也為各種應用帶來無限可能性，但相對的以電腦、網路及周邊設備為工具的電腦網路犯罪，特別是與線上遊戲相關的犯罪與網路詐欺，已然成為人們利用網路時必需小心面對的問題。

貳、詐騙案例與手法

網路詐騙與傳統詐騙相比較，詐騙犯罪主體一般都掌握一定的電腦網路知識和技巧，而純粹網路詐騙的犯罪主體更多為電腦網路方面的高手，有時還要兼備金融、貿易方面的相關知識，而且犯罪平均年齡層多在青少年的年紀。

由於網路犯罪的開展過程、作用對象、犯罪後果等都可以是資訊紀錄，這些資訊容易偽造，也難以據此找到罪嫌；甚至行為人可能只是利用網路程式的漏洞，如果不是對某些資訊密切注意，犯罪結果都是難以覺察的。所以行為人第一次犯罪得逞後，很少會被立即發現，犯罪後所得到的物質利益，會促使其繼續進行犯罪。不僅如此，網路詐騙的成本投入往往僅需要一部電腦終端機和網路連接，而造成的損失則往往數以萬計。所以有人貼切的形容網路詐騙根本就是——「用電子束搬走黃

1 資料來源：http://www.edu.tw/EDU_WEB/EDU_MGT/MOECC/EDU0688001/tanet/tanet-IPR/94plan/06_02_18.htm，最後閱覽日2007年9月10日。

2 惟此數目已較上年同期減少 2,825 件(-18.35%)。

3 95年8月30日警政統計通報第35 號，<http://www.npa.gov.tw/NPAGip/wSite/public/Attachment/f1156734832119.pdf>，最後閱覽日2007年9月10日。

金」、「鍵盤一響，黃金萬兩」⁴。

歸納相關案例與資料⁵，可以整理出網路與線上遊戲詐騙的手法包括：

一、網路詐騙的類型手法

1、透過網路交友找被害標的

歹徒利用網路聊天室與被害人交往一段時間後，即找藉口（例如：有極高的商業投資機會、六合彩內線消息、遭黑道追殺等）騙取被害人金錢，或誘騙被害人向銀行辦理存摺與金融卡提供予歹徒，成為歹徒販賣盜版光碟、網購詐欺等其他犯罪的工具。甚至利用被害人陷入情愛，要求被害人於網路視訊畫面做許多曖昧動作，並予側錄，事後再威脅被害人換回有曖昧動作的DVD。

2、個人資料被截取冒名利用

此類型的主要詐騙方式在於取得被害人的個人資料，至於取得資料的方法則五花八門：

- (1) 如利用被害人在ebay拍賣網站下標購買商品，因下標前與賣方在網路上討論細節時公開e-mail帳號，被歹徒利用假借賣方名義發出假的e-mail信件，騙取買家至ATM轉帳匯款。
- (2) 利用被害人在電腦網路上購物消費，致信用卡卡號遭到網路駭客入侵攔截，繼而被冒用盜刷。
- (3) 以「網路釣魚」方式，例如拷貝網路銀行網站的網頁，假冒該銀行之名提供「活期儲蓄存款」、「定存本利和」、「定期儲蓄存

款利率」、「零存整付本利和」等多功能，讓使用者誤上冒牌的網路銀行。

- (4) 誘騙被害人下載安裝藏有木馬程式的軟體，使被害人在利用網路銀行或網路ATM時，在不知不覺中洩漏個人身分證件或銀行帳號及密碼等重要資料，以致信用卡被盜刷或存款被盜領。

3、網路購物詐欺

網路購物詐欺的情況很多，曾出現的案例有：

- (1) 被害人在奇摩拍賣網站上瀏覽商品資訊後，花費2千元向人購買線上遊戲所使用之「天幣」，賣方以簡訊告知先至ATM轉帳匯款，嗣後賣方不知去向。
- (2) 在網路上虛設高科技公司，以低價販賣高科技新產品，並在網站上展示MP3隨身聽等產品，該公司及網站俟收到網友所寄購買產品之款項後，公司便人去樓空，網站亦隨之關閉。
- (3) 在網站、跳蚤市場上張貼販賣非常低廉的商品，或以貨到付款方式取信於買方，結果被害人付款後，沒收到貨，或者拆封才發現收到的是瑕疵、不堪使用、或根本是有包裝而沒東西的貨品⁶。

4、其他利用網路做為詐欺工具的案例

- (1) 信用卡詐騙：歹徒利用信用卡公司在網路上登載檢測偽卡程式，輸入一組正確信用卡卡號，程式產生數千至數萬個信用卡卡號，

4 資料來源參見：http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/theory/2005-12/16/content_5491513.htm，最後閱覽日2007年9月11日。

5 資料來源：法務部全球資訊網，常見詐騙案例犯罪手法及預防方式一覽表，<http://www.moj.gov.tw/ct.asp?xItem=27846&ctNode=11600&mp=001>；<http://www.sinica.edu.tw/as/law/anti-corru/fraud-9604.doc>，最後閱覽日2007年9月11日。

6 刑事警察局曾偵破此類案例，可參見http://www.cib.gov.tw/news/news01_2.aspx?no=42，最後閱覽日2007年9月11日。

再利用所產生之卡號非法上網購物消費。

- (2) 網路金光黨：在網路上以「大家來賺錢，這是真的，不是騙人的」標題，在新聞討論群組張貼郵遞名單事業信件，信中列有5人姓名及地址，指示網友寄給名單上5人各100元，再將列於第1位者之姓名自名單除去，將第2名以下者皆往前遞補1順位，最後將自己姓名置於第5位，以此類推，信中並告訴網友當自己的姓名遞補至第1位時將可獲得約數千萬元。

- (3) 假錄取真詐財：詐騙集團在網路以政府200億元公共服務擴大就業方案為誘餌，要民眾繳交2,000元加入會員，保證得到就業錄取機會。電子廣告信內容指稱職訓局釋出11.5萬個工作機會，並臚列全省各級縣市政府、北高市議員、全省各公立學校、績優國營事業、各縣市銀行及農漁會等名額數十至數百名約聘雇人員職缺，誣稱只要繳交2,000元加入會員，保證可獲錄用等。

二、線上遊戲詐騙的類型

線上遊戲由於虛擬寶物（遊戲中使用的貨幣、遊戲角色所使用的道具與裝備等）的需求，產生了以實際金錢交易買賣虛擬寶物的情況，也使線上遊戲詐騙的案例層出不窮，詐騙手法亦推陳出新，甚至由騙變搶。由遊戲玩家在網路上的遊戲討論區中所提到的案例⁷，可整理歸納其類型如下：

1、社交詐騙型

此類型又可分為：

- (1) 偽裝遊戲角色模式：此模式主要是利用他人的誤認來進行詐騙，方式上必須創造另一類似人物再加上非常相像的帳號來行騙；另一種則是，犯嫌通常會開設一個女生人物的帳號，然後努力裝可憐、無辜、裝新手剛玩，要玩家帶他，等取得玩家信任後，即提出想要或借用虛擬寶物的要求；亦有宣稱是「天堂特派記者」，請求遊戲玩家提供寶物、做採訪，因而詐騙成功；或徵求練功夥伴騙取帳號寶物使用後消失的情況。
- (2) 密技教導：這種方式類如金光黨模式，是利用被害人的貪念，通常在遊戲中他會謊稱發現一個密技，叫玩家跟他到遊戲中沒有人的角落或是偏僻地方，然後謊稱只要把你身上某個裝備，丟在地上滿幾次，在第某次等幾秒後於快消失時撿起來，就會複製該裝備，不過，在丟出裝備時就會被對方或突然出現的第三人取得，然後對方馬上下線離開。
- (3) 社群集體詐騙模式：以遊戲中某社群名義，線上招募玩家加入，騙取虛擬裝備後，即將玩家踢出團體，此等的詐騙手法宛如現實社會不肖人士虛設行號違法吸金的模式。
- (4) 反控盜寶模式：利用社會經驗薄弱的被害人，於交易中設計詐稱提供帳號寶物練功，再反控被害

7 資料來源參見：<http://twbbs.idv.tw/archiver/tid-13616.html>；<http://www.twbbs.net.tw/index.php?forumid=365>；<http://www.gamez.com.tw/archive/tid-74336.html>，最後閱覽日2007年9月12日。

人盜竊，家長因怕子女留下前科，不得不付款和解。

2、交易詐騙型

- (1) 點數或月卡兌換模式：由於線上遊戲通常是以儲值的方式取得使用的權利，因此出現幫對方儲值的方式來取得虛擬寶物的交易模式，詐騙的一方通常會出高價或以正常價引誘玩家上勾，然後一樣會給玩家電話或即時通，等完成儲值手續後就關手機或把玩家列進黑名單拒看訊息。
- (2) 付款惡意不足模式：在交易視窗中，以原定價虛擬貨幣作為條件，但在實際交易中，故意少打一個零，待交易成立後，被害人發現後已無法還原，並造成價差的損失。
- (3) 利用網路資料傳遞時差模式：佯稱要與人交易虛擬裝備，以外掛程式每五秒發送交易訊息，靜待玩家上當，待玩家與其聯絡，先要求買主先行匯款，但往往匯款後，賣主已無法聯絡，並隨即更換角色名稱繼續行騙。

3、帳號密碼騙取型

- (1) 工具利用模式：藉由網咖、病毒、遊戲漏洞，以特洛伊木馬、鍵盤記憶（KeyLog）或外掛程式入侵玩家電腦、或利用監視器、與他人共用之角色帳號、假網站等方法，獲取其他玩家的帳號及密碼，進而竊取該帳號內所有之虛擬寶物，或利用雙方交易時，

強制將對方寶物取走，再趁機以低價線上交易換取現金謀取利潤⁸。

- (2) 帳號密碼變更模式：詐騙一方於賣出帳號後，於對方練到一定程度頗有程度後，再利用遊戲公司為防止帳號濫用，將原始登錄資料某部分設定為無法更改的機制，回頭向遊戲公司提出帳號遭盜取，要求更改密碼，取得帳號的控制權。由於登記資料仍屬第一次登錄者，造成許多人在買到帳號後被騙，無法證明這個帳號為自己所有，不僅無法向遊戲公司申請，更無法報案。

4、內神通外鬼型

就公司而言，玩家所擁有的虛擬裝備、貨幣，只是電腦程式的參數設定，但線上遊戲寶物具有可交易的價值，也曾出現遊戲公司職員利用職務之便，修改系統及角色人物參數值，再進行私下交易買賣行為，以獲取不法高額利潤之案例⁹。

參、因應與預防之道

探究所有詐欺案中，以被害人「貪小失大」的原因居多，是以防詐第一要務為：「勿存貪念」。在拍賣網站與遊戲討論網站也都有網路購物與相關法令或詐騙處理的說明，在其互動討論區中也有許多網友的經驗分享，可藉由他人經驗獲得網路詐騙自保之道的常識及方法，以下歸納其重點供讀者參考：

8 案例參見刑事警察局偵破「天堂」線上網路遊戲詐騙新臺幣並盜用帳號密碼後竊取寶物、道具的新型態犯罪案件，http://www.cib.gov.tw/news/news01_2.aspx?no=14，最後閱覽日2007年9月12日。

9 刑事局偵九隊一組曾偵破一起「天堂」線上遊戲管理員（GM）盜用客戶帳號密碼後再竊取虛擬道具的監守自盜案件，所竊得的夢幻道具每項市價皆值新臺幣數萬元。刑事局偵九隊是在去年三月初接獲遠從雲林北上的民眾報案指稱，他在家上網玩「天堂」網路遊戲時連續二度遭人以不明方式踢下線並竊走價值昂貴的虛擬道具，警方對該玩家都在自己家中上網玩遊戲卻仍會發生帳號被盜用及道具遭竊的情形感到非常詫異，經九個多月來積極偵辦，終獲線查出該遊戲公司一離職楊姓員工及王姓男子涉有重嫌，二嫌到案後皆供稱因好奇及貪玩而利用工作之便犯案，警方將繼續追查有無其他共犯後將全案以違反刑法詐欺及竊盜罪移送臺北地檢署偵辦，詳見http://www.cib.gov.tw/news/news01_2.aspx?no=40。

一、網路詐騙的因應¹⁰

1、謹守「人身安全優先」原則

網路聊天室為「虛擬空間」，網友身分及相關資料是否正確均難查證，切勿輕易匯款或答應對方留下「視訊畫面」，以免後患。若因網友不斷糾纏，千萬不可答應對方任何要求（留下視訊畫面、借帳號），應立即切斷往來，以爭取理智與冷靜判斷空間，若因而遭到恐嚇、騷擾，可撥打「165」向警方請求諮詢或協助。

2、避免個人資料外漏或被冒用

詐騙歹徒擅長掌握人性弱點，以套交情、裝可憐來博取信任。因此，網路交友要格外小心，本身應避免存有不當動機而遭人設計，也切忌留下個人資料，以免成為歹徒恐嚇詐財對象。另最好紀錄網友的IP位址、交談紀錄，以利事後提供警方追查。若遺失身分證，應立即向警方報案，再到戶政單位申請掛失，最後要記得將經戶政機關簽章，確認無誤的「身分證補換申請書」影本，函送「金融聯合徵信中心」建檔。

3、維護個人帳號密碼的安全

在電腦的使用上不要與他人共用同一帳號，如果一定要與朋友共用帳號，要有受到各種損害狀況的心理準備。在密碼的使用上要避免使用與帳號同樣數字或英文當密碼，也不要使用身分證字號、個人生日、電話當密碼。其他有助於維護安全的方法，包括鍵入帳號密碼時盡量不要讓他人看到；在使用帳號密碼時可利用鍵盤

輸入與滑鼠點選，使盜用者取得的是錯誤的資料；不貪圖他人誇張不實之引誘，因而洩漏帳號密碼；不隨意下載安裝不明之程式軟體，避免木馬入侵；盡量不在開放式環境中的電腦鍵入帳號與密碼；電腦不隨意外借，避免被不肖人士竊取資料或植入密碼；也不要隨意開啟不明郵件，避免中毒。

4、確認信用記錄且盡量面交

網路購物應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，且應選擇有信譽之拍賣網站或購物網站，並瞭解欲交易之貨主之信用、風評等，而交易方式最好能以當面交易並銀貨兩訖的方式，絕對不要在未確認物品的情形之前就將款項匯出。

二、線上遊戲詐騙的因應

1、遊戲帳號被盜的處理¹¹

當發生遊戲帳號被盜的情況時，應立即查詢遊戲歷程。每家廠商申請手續以及完成時間不一，部分需要收費或是扣除遊戲點數。此動作也可查明是否為廠商疏失造成。接下來即前往警局報案，建議前往縣市警察局，因為大多數的分局裡沒有電腦犯罪偵查組，在接受玩家報案後，還是會轉至縣市警局的電腦犯罪偵察組。若抓到該犯罪者時，可以「無故入侵電腦罪」或依刑法第359條「保護電磁紀錄」處罰¹²。

2、了解常見的虛擬貨幣與寶物詐騙手法

¹⁰ 資料來源：http://tpa.judicial.gov.tw/politics/politics_show.php?id=27，最後閱覽日2007年9月12日。

¹¹ 資料來源參見<http://law.gamebase.com.tw/index.jsp>；<http://www.gamebase.com.tw/forum/content.html?tno=&n=0&sno=71544376>，最後閱覽日2007年9月13日。

¹² 刑法第359條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」。

線上買賣虛擬貨幣與寶物的詐騙通常會在標的上以相近物交易、故意在交易金額數字上減少；而且以多數玩家經驗，詐騙者多以新手角色交易或者將帳號名字取得跟受害者的朋友相似，有些詐騙者會將帳號取一些奇怪的符號呈現，甚至連系統都不能顯示出來，以延誤被害玩家向遊戲管理者（GM）檢舉的時間；至於以遺棄道具至地上，再給對方撿起的交易方式，因為丟在地上的行為在遊戲裡會被判定為遺棄刪除指令，並無法向遊戲管理者（GM）請求回復。而且，若遊戲公司禁止虛擬寶物交易，縱使交易成功，事後還是可能被遊戲公司刪除。

3、避免遊戲帳號的買賣

遊戲帳號是以原始玩家的身分證字號去申請，就算對方將帳號賣出，只要原始玩家傳真身分證等證明，一樣可以跟遊戲廠商調出新輸入的帳號密碼，於登入後再將密碼變更，被騙的玩家仍然無法取得帳號的使用權利。如果買來帳號的原玩家涉嫌不法，該帳號會被廠商刪除，徒增自己的困擾，而且如果無法舉證，還可能會受到牽累。同樣的，新玩家利用買來帳號涉嫌不法，原玩家也會被牽累。

4、於網咖玩線上遊戲要注意資料安全

由於網咖是不特定人共同的電腦，因此資料易被有心人竊取，在使用時最好讓電腦重新開機，讓裝有系統還原卡的電腦啟動還原；開機後，即關閉自動完成輸入的功能，並取消系統紀錄帳號密碼的功能。下線後則將電腦關閉或至少重新開機，以免有心人取得帳號密碼資料，家中有電腦

者盡量再上線更改遊戲密碼，以求安全。

肆、結語

由於網路的便利性，吸引許多人透過此虛擬世界進行資訊交流、意見表達，而且亦有許多網路交易、網路購物等行為，在虛擬網路世界中不須暴露真實身分與面貌，使網路詐欺這類網路犯罪亦隨之而生。其中網路遊戲便是網路詐欺最常發生的來源之一。遊戲原本應該只是單純的娛樂，但虛擬人物間的互動卻是由真實世界的人來操控，網路與現實或許有虛擬與真實之別，但人性卻永遠不會改變，一旦涉入了金錢的交易，就是一個容易顯露人性黑暗面的真實世界。無論如何，法律並不會因為網路的虛擬性而失其效力，即使是網路或線上遊戲中的詐欺行為亦須負民事侵權責任與刑事詐欺、妨害電腦使用之罪責。因此，即使在虛擬的網路世界，仍須抱持防人之心不可無，害人之心不可有的謹慎態度，更重要的是多充實網路犯罪手法的資訊，才能增強自己的警覺性與因應能力。