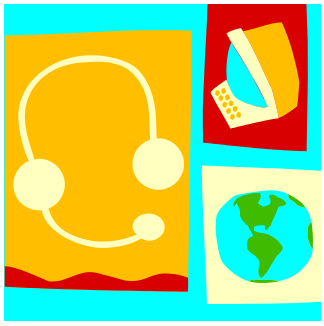
網路詐騙手法與防範



手冊內容

§ 前言

越來越多歹徒把線上遊戲玩家當作詐騙對象

新的線上遊戲推出速度越來越快，也越來越多樣化，包括像是角色扮演、戰略、養成、冒險、動作、競速、益智等多種類型。

在不影響正常作息，並且能夠兼顧工作、家庭與休閒活動，玩玩線上遊戲也是一種不錯且可以放鬆心情的休閒娛樂。也是因為線上遊戲越來越受歡迎，也就有越來越多的歹徒與詐騙人士，把遊戲玩家當作是詐騙的對象。

若你有玩線上遊戲的經驗，或許你曾經碰過在玩遊戲時，遇到陌生人主動提議要賣你稀有寶物，或告知有可以在短時間內累積經驗值的外掛程式，這些都有可能是網路詐騙喔！

日前有報導指出，有歹徒鎖定青少年喜愛的舞蹈網路遊戲，以「免費洗點數」、「免費外掛程式」為由，與小玩家在聊天室中搭上線，要求玩家提供電話及身分證字號，再以這些騙到手的個人資料去盜買遊戲點數，一個月左右就有將近 20 名的受騙者，其中，有一半的受騙者都是 15 歲以下的青少年，最小的也只有 13 歲而已。

若用專業術語來描述詐騙，就是所謂的「社交工程」，或者用通俗的話，就是金光黨。社交工程是利用溝通技巧誘騙取得信任，以獲得資訊或利益。

本手冊將介紹網路上常見的社交工程手法，還有這些社交工程所可能造成的影響；最末則提供防範網路詐騙的小撇步，提醒大家在使用網路時的注意事項，不要讓自己因為一時疏忽成了無辜的受害者。

歹徒利用社交工程技巧所進行的網路詐騙活動，若成功，不只是會對你自己、你的電腦、甚至是你的家人、無辜的其他人造成傷害，以下說明這些可能造成的傷害類型。

惡意程式一旦安裝到你的電腦後，這個惡意程式可能會偷取你在電腦中儲存的個人資料或私密的檔案！

1. 對電腦安全之危害

對電腦安全造成傷害最常見的例子是，歹徒寄給你外表看起來很正常又很專業的電子郵件，信中會騙你必須點選某個超連結或下載附加檔案，一旦你點選了超連結或下載檔案，惡意程式便會在你不自覺的情況下下載並安裝在你的電腦中。一旦惡意程式安裝到你的電腦中，該惡意程式可能會偷取你在電腦中所儲存的個人資料，或是側錄你在上網時所輸入的帳號與密碼，並透過網路把這些資訊傳送出去，歹徒即可利用這些個人資料來假冒你的身分，從事不法行為，例如假借你的名義濫發垃圾郵件。

2. 上網買到冒牌貨

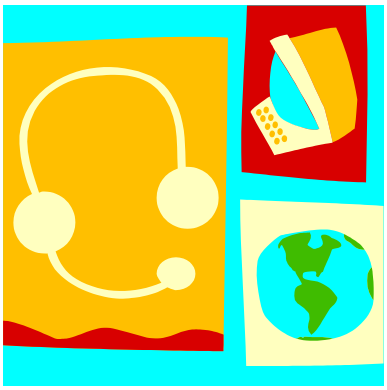
另外一種常見的狀況是，在拍賣網站上，不法人士以比市價還要低很多的價格販售線上遊戲所使用的「天幣」、最新款智慧型手機、平板電腦，或是最新上市且很難買得到的限量款球鞋等，結果網友以為撿到便宜很開心的下標購買並完成轉帳匯款後，不但沒有收到商品而且賣方就不知去向；或是收到的商品，根本就是個山寨版的冒牌貨。

3. 取得信任並要求你去匯款

歹徒也可能會假冒是你的朋友，或者先充當你的網友一段時間取得你的信任後，利用很多不同的理由與藉口，像是幫忙在線上遊戲中練功累積經驗值、自己或家人臨時發生重大變故...等，向你提出借錢、請你去轉帳、或是請你幫忙買遊戲點數卡的要求。一旦錢騙到手後，歹徒就消失得無影無蹤，你不但甚麼都沒拿到，還損失了一大筆金錢。

瞭解網路詐騙常見手法，提高警覺可以避免受騙！

歹徒可能會假冒說他是正派經營公司、或者學校、甚至是政府機關等，讓你覺得可以信任的對方，然後騙你告訴他有關你在網路上常用的帳號與密碼資訊，例如用來收發email、玩臉書、撰寫部落格、使用網路相簿，還是登入線上遊戲或聊天室時會使用的帳號與密碼。



歹徒會假冒是你在MSN 或即時通上的好友傳訊息給你，請求你的幫忙，像是向你借錢或請你去買遊戲點數...

手法 1. 假冒是你的 MSN 或即時通上的好友

歹徒會利用偷取到的 MSN 或即時通帳號與密碼登入，然後利用受害者的好友朋友名單傳出詐騙訊息，像是請求幫忙等。通常大家會因為是朋友傳來的訊息，很容易就信任對方所說的內容。

以下是常見且真實發生的假冒訊息，當你收到類似的訊息時，即使是朋友傳來，也要提高警覺，不要輕易相信：

- 請幫我衝衝部落格的人氣！！（提供網址要你點選）
- 我現在不方便，請你幫我去便利商店買線上遊戲點數卡，我再還你錢囉！！
- 要不要用用看這個新的 MSN 外掛程式？很漂亮喔！（提供網址要你點選）

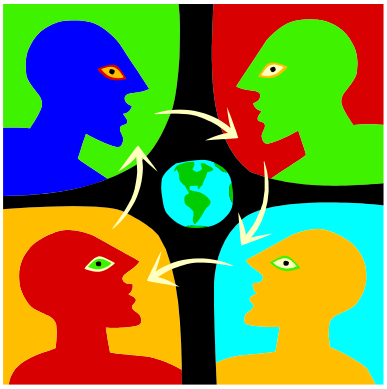
手法 2. 先套交情騙到你的個資，再冒名使用

歹徒也可能會利用線上遊戲或聊天室尋找目標，並花時間經營雙方的關係以取得信任，然後再用藉口騙你告訴他你的手機號碼、身分證字號等個資。這些個資到手後，歹徒便可以利用你的名義以手機小額付費方式去買遊戲點數，再把遊戲點數拿去賣錢，帳單卻是由你來付。

以下是歹徒可能會用來騙你的個資的藉口，一旦遇到這樣的情況，一定要拒絕！

- 免費提供虛擬貨幣
- 外掛升級增加點數
- 不用付月費
- 可以買到比較便宜的遊戲點數

手法 3. 社群網路的惡意連結越來越流行



因為臉書 (Facebook)與噗浪 (Plurk)等社群網路服務越來越流行，社群網路的使用者也成為詐騙集團下手的目標。歹徒會透過先要求加你成為朋友，在你的塗鴉牆上留言，請你點選或下載藏有惡意程式的超連結，或是邀請你一起玩來路不明的臉書遊戲，當你按下同意按鈕玩遊戲時，你也同意該遊戲的開發者可以正大光明地取得你在臉書中所留下的相關個人資料，包括你的照片、你的好朋友名單、你的家庭狀況、你的所在位置，以及你的聯絡方式等資訊。

只要有你的手機號碼加上身分證字號，歹徒就可以假冒你的名義去買遊戲點數囉！

防範網路詐騙的五大注意事項

(1) 網路遊戲公司普遍都有和電信業者合作小額付款機制，讓用戶可以方便地用手機號碼購買遊戲點數，然後點數費用可以連同手機帳單費用一起支付。提醒遊戲玩家，不要貪小便宜或輕信網友，而把自己的手機號碼、身分證字號等資訊提供給他人，以免遭到歹徒利用，使用你的手機號碼小額付款來買點數。

(2) 朋友以即時通方式傳來訊息要向你借錢或請你幫忙買東西時，一定要用即時通以外的其他方式再次求證，例如直接打電話詢問朋友，不要輕易地就答應對方的要求。

(3) 臉書或噗浪等社群網路服務中也可能暗藏有詐騙的陷阱，像是臉書遊戲或應用程式已經發生暗藏木馬程式的案例。在你決定點選臉書上的超連結或要玩某個小遊戲之前，請再想想是否真的很必要，或者上網查一查別人是否有類似的受騙經驗。

(4) 不任意下載讀取來源不明之電腦檔案及開啟不明網頁連結，以減少下載惡意程式與帳號密碼遭盜取之風險。這些惡意超連結可能出現在電子郵件、即時通訊息內、臉書塗鴉牆、聊天室或留言版等處。

(5) 設定安全網路服務密碼，不要為了方便，把自己的所有網路服務都設定同一組帳號與密碼！這樣一來反而給了歹徒一個最方便的方式取得並盜用與假冒你所有的網路身分。

出 版 者　教育部
發 行 者　蔣偉寧　教育部部長
召 集 人　吳國維　財團法人中華民國國家資訊基本建設產業發展協進會執行長
　　梁理旋　財團法人中華民國國家資訊基本建設產業發展協進會協理
指導委員　何榮桂　教育部電算中心主任
　　韓善民　教育部電算中心副主任
　　楊文星　教育部電算中心高級管理師
　　苗宗忻　教育部電算中心資訊管理組組長
　　劉玉珍　教育部電算中心資訊管理組程式設計師
審查委員　林杏子　國立高雄大學資訊管理學系教授
撰稿人員　梁理旋　財團法人中華民國國家資訊基本建設產業發展協進會協理
承辦單位　財團法人中華民國國家資訊基本建設產業發展協進會
出版日期　民國 101 年 02 月

※此手冊內容係對特定議題所提供之學習教材，僅供各界參考，非本部相關政策。