網路詐騙手法與防範

手冊內容

§ 前言

線上遊戲小玩家請注意！

有越來越多新的線上遊戲，像是找寶物、累積經驗值、打怪物、攻城、跟好友組隊一起練功、跳街舞、養寵物等，在不影響課業及正常作息的情況下，玩玩線上遊戲也是一種不錯的娛樂活動。

不過你知道有越來越多的線上遊戲小玩家被歹徒詐騙嗎？想想看，你有沒有在玩遊戲的時候遇到陌生人主動說要賣你稀有的寶物，或是主動說要教你在很短的時間內累積很高的經驗值呢？請你千萬要小心，這些都有可能是網路詐騙喔！

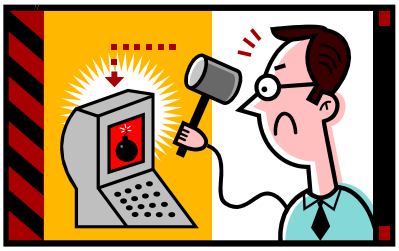
日前新聞有提到，有歹徒鎖定青少年喜愛的舞蹈網路遊戲，以「免費洗點數」、「免費外掛程式」為藉口，與小玩家在聊天室中認識，要求小玩家提供電話及身分證字號，再以這些騙到手的個人資料去盜買遊戲點數，一個月左右就有將近 20 名的受騙者，其中，大多數的受騙者都是 15 歲以下的青少年，最小的也只有 13 歲而已。

我們稱這一種詐騙手法為「社交工程」(Social-Engineering)，簡單來說就是利用騙術達到不法的目的。

在這本手冊中，我們將會介紹網路上歹徒可能會使用的「社交工程」手法(例如：線上遊戲、MSN 傳訊購買點數...等)，並且說明這些「社交工程」可能造成的影響，也提供你一些防範詐騙的小撇步，提醒你在上網時應該注意的事項，不要讓自己在不小心的情況下變成了受害者。

1. 網路詐騙的傷害

歹徒如果利用「社交工程」技巧進行網路詐騙，成功的話，就有可能會傷害到你自己、你的電腦、你的家人、甚至是其他無辜的人，以下是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或者你的家人放在電腦中的所有個人資料或私密的檔案！

危害電腦安全

舉例來說，歹徒會寄給你一封你完全不會懷疑的電子郵件，信中會騙你點選某個超連結或下載附夾檔案，當你點選後，在你不自覺的狀況下，惡意程式就會安裝在你的電腦中。

一旦惡意程式安裝到你的電腦中，這個惡意程式可能會偷取你存放在電腦中的個人資料，或是偷看你或你的父母上網時所輸入的帳號與密碼，惡意程式還會透過網路把這些偷到的資訊傳送出去，而歹徒就可以利用你的個人資料來假冒你或你的家人，從事不法行為。

網路購物時收不到商品或是買到冒牌貨

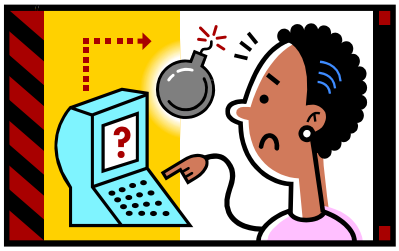
有時候，你可以在知名的拍賣網站上看到有人在販售線上遊戲所使用的「天幣」，或者是比市價還要低很多的最新款智慧型手機、最新上市且很難買得到的限量款球鞋等。結果在你開心地下完標並且轉帳匯款之後，並沒有如預期收到商品而且賣方也消失不見了；或者收到的手機或球鞋，根本就是個山寨版的冒牌貨。

騙你去轉帳或匯款

甚至，歹徒會利用你的個人資料、或向你騙取你爸爸媽媽的信用卡號碼等重要的個人資料，也有可能會利用很多不同的理由與藉口，像是幫你練功累積經驗值、送你手機獎品等，或者先當你的網友一陣子後，再向你提出借錢的要求、騙你拿家長的提款卡到銀行進行轉帳、或是要你用零用錢去買遊戲儲值卡等。一旦錢騙到手之後，歹徒就消失得無影無蹤，而你不但什麼都沒拿到，還損失了一大筆錢。

2. 讓我們一起來瞭解網路詐騙常見手法

歹徒可能會假裝他是正派經營的公司、學校或政府機關等，讓你信任他，然後騙你告訴他你的網路帳號與密碼等資訊。而這些可能是你平常用來收發 email、玩臉書、寫部落格、使用網路相簿、或登入線上遊戲還是聊天室時會使用的帳號與密碼。



手法 1. 假冒是你的 MSN 或即時通上的好友

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。通常因為是朋友傳來的訊息，你很容易就會信任對方所說的話。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，即使是朋友傳來的，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）

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 2. 先和你成為好友，騙到你的個資後再冒名使用

歹徒會和你一起玩線上遊戲一段時間，成為你的好友取得信任，然後再用各種藉口騙取你或家長的手機號碼、身分證字號等個資。騙到這些個資後，他就可以用你的名義以手機小額付費方式去買遊戲點數，再把點數拿去賣錢，可是買點數的錢卻是由你來付。

以下是歹徒可能會用來騙你的個資的藉口，碰到這樣的情況時，一定要拒絕！

- 免費給你虛擬貨幣
- 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. 利用社群網站的惡意連結騙取你的個人資料

因為臉書 (Facebook)與噗浪 (Plurk)等社群網站的流行，這些網站也逐漸成為詐騙集團的目標，歹徒會透過聊天室、傳訊息、在你的塗鴉牆上留言等管道，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，當你按下同意按鈕時，你也同意這個來路不明遊戲的廠商可以正大光明地取得你在臉書中所留下的個人資料、聯絡方式、你的照片、甚至是你的所有好朋友名單。

3. 防範網路詐騙的五個小撇步

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！

(1) **不輕意透露個人資料**：網路遊戲公司大多會和電信業者合作，讓你可以方便地購買遊戲點數，而這些點數的費用會算在你下個月的電話帳單中，這就稱為「小額付款」。不過，提醒遊戲小玩家，不要貪小便宜或輕信網友，而把自己或家長的手機號碼、身分證字號等資訊提供給他人，因為歹徒會利用你的手機號碼小額付款來買點數。

(2) **小心求證**：朋友以即時通方式傳來訊息要向你借錢、或者請你幫忙買東西時，一定要先求證，例如直接打電話詢問朋友，千萬不要輕易就依照對方的要求而提供幫忙喔。

(3) **按下滑鼠之前請再想一想**：臉書或噗浪等社群網站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會藏有木馬程式，下載後就會偷取電腦中的資料。在你決定點選臉書上的超連結或要玩某個小遊戲之前，可以先上網查一查別人是否有類似的受騙經驗，以免你的個人資料遭到不法利用喔。

(4) **不隨意點選網頁連結**：不任意下載讀取來源不明的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被盜取的風險。這些超連結可能出現在別人寄給你的電子郵件中、傳給你的即時通訊息內、臉書的塗鴉牆、聊天室或留言版等，所以點選時一定要小心。

(5) **設定安全的密碼**：設定安全網路服務密碼，不要為了方便，把自己的電子郵件、線上遊戲、聊天室、臉書或噗浪等服務，都使用同一組帳號與密碼，才不會讓歹徒可以方便地盜用你的所有網路身分！

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
潤稿人員　鄭貴內　嘉義市教育網路中心教師
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。