桃園縣立同德國民中學　　101 年 11 月 04 日出刊

科學新知週報

第 173 期

發行人：曾素鳳 校長　　本期主編：顏瑞俐老師　　自然與生活科技領域編製

資安。知安

<資安危機~裝熟簡訊又來詐騙>

■以為老朋友...怎麼都不認識

自由時報報導南投草屯警方指出，近來接獲 6、7 名中華電信用戶民眾報案，指在智慧型手機的 Line 或臉書接獲訊息，傳訊者會標註被害人姓名，訊息顯示「看著這些照片，好懷念以前的日子！」、「被偷拍的是你嗎？」等字眼，下方則有連結網址，不疑有「詐」的人，直覺以為是老同學或老朋友傳來，或擔心照片遭移花接木，就直接點選該網址。

■木馬程式來襲 啟動小額付款

有 4 名被害人一點選附加網址後，即出現不熟識者照片，心裡正納悶：「照片上的人怎麼都不認識？」1 小時後即收到電信公司小額付款通知簡訊，有人因而損失 5000 元。

另有 3 名被害人收到「被偷拍的是你嗎？」訊息，一點選連結網址後出現色情照片，有 2 人莫名其妙地被扣小額付款 1000 元，另一人嚇得趕緊將手機關機，讓植入木馬程式的應用程式無法繼續執行，因此沒有被扣款。

警方說，這類新型詐騙手法，歹徒利用流行的 Line 或臉書軟體，以傳訊息「裝熟」或「恫嚇」方式，讓被害人點選其附上的連結網址，一連結就被植入並啟動木馬程式，並利用被害人名義以小額付款功能購買遊戲點數，當電信公司發簡訊通知被害人認證碼時，木馬程式即自動攔截簡訊，藉以取得認證碼完成購買點數，帳就記在被害人頭上。

■小額付款預設開啟 最好取消

警方指出，經由 IP 追查，這類詐騙集團的主機都設在中國，讓警方難以直搗其總部，提醒民眾，要避免被騙，就是不要點選來歷不明的訊息連結網址，也不要下載可疑的 APP 軟體，最好打電話要求電信公司取消小額付款功能

**什麼是小額付款?

- 以中華電信來說：HiNet 小額付款系統是整合認證、授權和計費三種技術成為一個標準平台，提供給消費者和內容廠商安全、便利、通用的小額付款收費系統。
- 中華電信客戶依不同身份，以帳號和密碼做身份驗證，費用隨網路及電話費用帳單收取。

<資安危機—會造成簡訊費暴增的 Android 木馬病毒>

這個 Android 木馬是由知名的防毒大廠卡巴斯基的實驗室所發現，並且認定為目前最難搞的一支木馬程式，中了之後可能會自動幫你傳送簡訊到「收費較高的號碼」、下載更多惡 意程式，且取得相當多的有關手機資訊回傳至遠端的伺服器，簡單的說，中了這支病毒，可能會導致手機費用爆增，除此之外，最恐怖的應該就是有機率透過藍牙或 是 Wifi 傳播出去，相當的驚人。

這個病毒的名稱目前被命名為「AndroidOS.Obad.a」，透過這個病毒再去下載回來的惡意程式同時擁有管理員權限，且不會出現執行清單 中，所以會持續默默的在背景運作，也刪不掉，而會回傳到遠端伺服器的內容包括 MAC 位址、電信營運商、電話號碼、IMEI、裝置帳號的可用金額、當地時間，以及有否取得裝置管理權限等。

■如何避免安裝到惡意 APP？

❖觀念一：盡量在 Play 商店中安裝

Play Store 是 Google 官方本身的 APP 下載平台，當然最基本的就有審核機制，雖然他們的審核相較 APPLE 較沒那麼嚴謹，不過總比沒有好，至少已經可以避掉一些惡意程式，所以千萬不要為了一點小錢去安裝來路不明的破解檔案。

❖觀念二：常下載破解檔案，就要懂的保護自己

如果你真的就是不想花錢購買任何付費的 APP，一天到晚也都在各論壇裡下載盜版破解的 APP，那麼建議你至少要安裝手機的防毒軟體，可以幫你擋下大部份的惡意程式，至於應該安裝哪一套，我想只要到 Play Store 裡搜尋「防毒」，然後挑比較知名的安裝一款即可，至於知名的定義，可以到 Google 搜尋就會有相關資訊囉。

❖觀念三：安裝 APP 之前查看要求授權內容

不論你是透過 Play 商店或是其它管道取得的 APK 檔案，在安裝的過程中，至少都一定會跳出這樣的畫面，告訴你會需要哪些權限，取得你的個人資訊或是相關控制等等，這時可能要多注意是否有被額外要求其它權 限，特別是需要「裝置管理員」權限的 APP，可能大有問題，但大部份人在安裝時並不會去注意這件事情，所以通常都是這麼中毒的。

只要做到以上三點，基本上就已經大幅降低中毒的機率，其它像是掃描 QR Code 可能也要多注意，養成更多良好習慣，才不會讓自己中毒也禍害朋友。

【參考資料來源】

- 趨勢科技雲端運算與網路安全趨勢部落格 http://blog.trendmicro.com.tw/4
- 部落格：就是教不落 http://steachs.com/archives/3224