

駭客盯上 LINE-山寨簡訊別開

全球用戶達 2.5 億的 LIEN，近來成為不肖業者鎖定的目標，透過傳送山寨版的更新連結訊息給使用者，用戶一不小心連結到偽裝的釣魚網站後，不但手機裡的個資外洩，還會自動散發垃圾訊息或病毒給朋友。

駭客跟著潮流走是訊息萬變的科技世界裡不變的趨勢，從過去使用的 MSN、現在的臉書或 LIEN，都是鎖定使用者高度依賴的社交程式或網站，因為使用頻率高，越會失去警覺心。

以 APP 來說，使用者依賴度越高，越會鎖定更新訊息，LIEN 每次更新都會新增使用功能或可愛圖貼，讓民衆對相關訊息習以為常，收到更新要求便迫不及待點開連結，忘記注意連結是否為官方下載平台，而成為受駭戶。例如:有不少 LIEN 用戶曾收到一則附有連結網址的購物訊息:「多種品牌的衣服、鞋子、包包、手錶飾品，感到興趣的水水們請進相簿查看看

喔:<http://photoxxxxxxx/k1252480xxxxx> 有喜歡的商品可以直接加客服的 LIEN 詢問訂購喔!Lien ID:www.19869x」上述連結卻是釣魚網站。想避開老手法的受駭招數，除了不要亂點連結，安裝防毒軟體也是方法之一，不要以為使用智慧型手機就沒有中毒的顧慮。

城鄉發展分署政風室關心您

(資料來源：臺中市政府社會局政風室)