桃園縣政府警察局分析「LINE」詐騙方式及防制作為

一、LINE 詐騙方式：

(一)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。

(二)詐騙集團取得受害者姓名、身分證字號、手機門號等個資，傳送標題聳動的簡訊，如「這是上次聚餐照片，你不在好可惜！」、「被偷拍的是你嗎？」、「這是那晚你沒來的照片，我被整慘了！」、「我在墾丁拍的照片，你覺得哪張最好看？」、「朋友家的狗狗參加人氣比拼，幫忙讚一下！」、「老同學來看我現在的照片，能想起來我是誰嗎？」、「ＸＸＸ(你的全名)，這是我哥的新女友，是你同學嗎？」、「陳ＯＯ這是上次聚會照片，你好好笑喔！」、「李ＯＯ還記得我嗎？」等並附上偽裝成分享照片連結的釣魚網址，誘使人點擊，藉此舉安裝惡意程式至受害者手機。

(三)惡意程式會自動上傳門號系統商資訊、自動申請電信業者小額付款服務。因惡意程式擁有手機作業系統最高權限，受害者無法親見電信業者傳送之小額付款認證碼簡訊，簡訊僅會傳送至詐騙集團設定之遠端伺服器。

二、LINE 詐騙案例：

(一)突然收到一封簡訊，內容是 Yahoo 奇摩的認證碼，之

後立刻接到陌生電話(或隱藏號碼)，非常急促且有禮貌地說:「不好意思，我在用 Yahoo 奇摩認證的時候，手機號碼輸入錯誤，不小心輸入了您的號碼，能不能請你把剛剛送進您手機簡訊上的驗證碼跟我講？真的很不好意思，拜託拜託！」

(二)「你正在申請網站上網支付 103 年 3 月電費共計 4800 元，若非本人操作請察看電子憑證進行取消」，然後就會出現一串網址，一點進去就會中毒(惡意程式)，然後不只會被自動以手機進行小額扣款還會將該訊息分別傳送到你手機或 LINE 的好友名單中，繼續散播病毒，使多人受害。

※以上是目前小額付款的漏洞，在線上購買遊戲點數卡或是通話卡，在做購買動作時，廠商系統會要求輸入手機號碼，然後再發一組認證碼到手機上，而後把收到簡訊上的認證碼輸入系統後，就完成小額付款的動作了！

三、LINE 帳密被盜高危險群：

(一)設定「公開 ID」。

(二)在公用電腦登入 LINE。

(三)允許手機通訊錄自動加入好友。

(四)授權 LINE 遊戲讀取你和好友的個人資料。

(五)同一組帳號密碼通用，導致 Facebook、信箱等帳密遭破解，LINE 也隨之被盜用。

(六)沒有使用電腦版 LINE，卻沒關閉「允許自其他裝置登入」。

(七)沒有定期更改密碼 。

四、LINE 詐騙防制作為：

(一)LINE 屬於通訊軟體、又是外國廠商，現行資訊管理相關法律都管不到，且 LINE 詐騙以小額遊戲點數為大宗，多被詐騙集團洗到國外去，讓警方無從追查。但 LINE 臺灣分公司也表示，若發生帳號被盜用的情形，用戶可在第一時間上網填寫問題反映表，同時通知親友不要理會冒用帳號的訊息;客服人員會盡可能在 24 小時內，透過使用者指定的郵件信箱與使用者聯繫，也可應使用者的要求，立即鎖住帳號。

(二)避免收到陌生人傳來的詐騙網址，直接擋掉不認識的帳號傳來的訊息作法：LINE→其他→設定→隱私設定→勾選「阻擋訊息」→就不會收到非好友的訊息！另外取消「我的帳號」中「允許自其他裝置登入」，能有效避免駭客取得帳號密碼後從電腦登入。

(三)建議民眾，如無使用小額付費功能需求，可向電信公司要求關閉，且勿代收簡訊，若收到可疑訊息，應以電話向友人聯繫確認，也可打 165 反詐騙諮詢專線查證。

(四)傳送來的訊息裡面帶有連結。無論對方傳什麼訊息過來，裡面若帶有連結，尤其是短網址連結(goo.gl、bit.ly)等等，絕對不要去點它！如果是好友送來的訊息，建議改用另外的方式(打電話、email)與對方聯絡，確定這個連結是安全、沒有問題的之後再開。

(五)LINE 用戶密碼遭竊的情形，多因使用電腦版 LINE 時電腦中毒，因此，如用戶從隱私設定→關閉公開 ID、開啟阻擋非好友訊息等功能，並每 3 個月到半年換一次密碼，皆可降低遭詐騙的機率。

(六)以上 LINE 防制詐騙方式將透過各種管道加強宣導，

以防止民眾遭詐騙，如有疑問將請民眾撥打 165 或 110 查證。