網路詐騙手法及防範之道

一、詐騙案例

1、假冒親友 LINE 訊息詐騙：

(1) 被害人林小姐在手機上接到朋友 LINE 訊息，請她幫忙去便利商店購買 my card(遊戲點數卡)，林小姐不疑有他，購買 5000 元遊戲點數卡後再依照指示告知序號及密碼，被歹徒詐騙得逞。

(2) 被害人張小姐在手機上接到朋友 LINE 訊息，說上網購物,手機故障收不到簡訊,請她代收並提供身分證字號。張小姐信以為真提供身分證字號，手機上接到一封認證碼簡訊，依歹徒指示回傳簡訊後，就被歹徒用張小姐的手機小額付款購買 3000 元遊戲點數，後來向朋友查證才發現上當。

2、LINE 釣魚訊息詐騙：

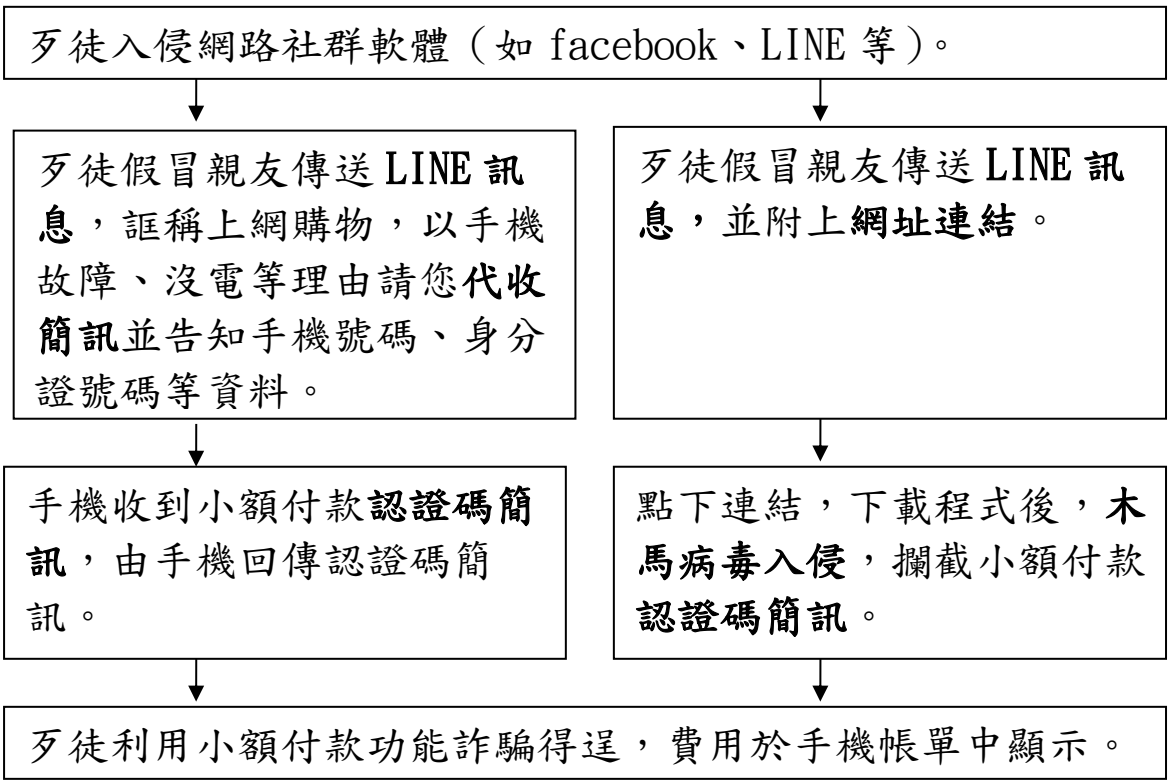
被害人李先生收到 LINE 訊息，內容是「李○○，這是上次聚會的照片，你好好笑喔!」，並附上一串網址。李先生點選網址連結後，歹徒的惡意程式入侵他的手機，惡意程式會攔截認證碼簡訊，歹徒利用李先生的手機小額付款購買遊戲點數，李先生在月底收到電話費帳單才發現自己被騙。

3、手機釣魚簡訊詐騙：

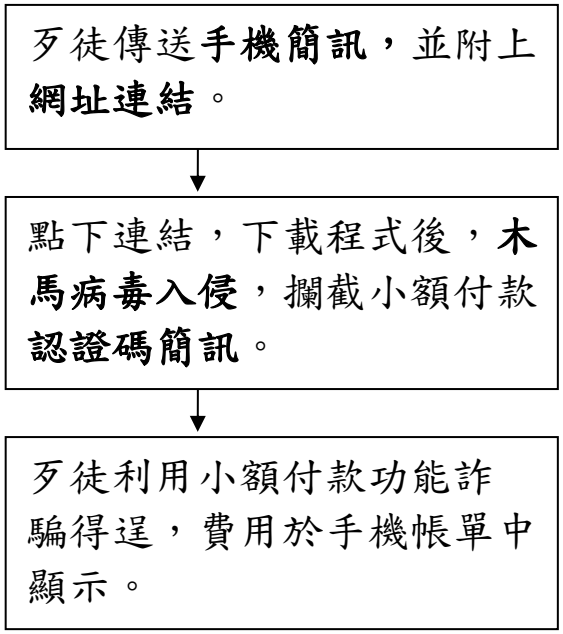
被害人陳先生收到手機簡訊，內容是上網支付電費(或快遞簽收單)，並附上一串網址連結。陳先生點選連結進入網頁,網頁上顯示同意及取消兩種選項,他點選取消交易，歹徒的惡意程式入侵他的手機。惡意程式會攔截認證碼簡訊，1 小時後就收到電信公司傳來的 1000 元小額付費通知。

二、詐騙流程

1、假冒親友 LINE 訊息詐騙及 LINE 釣魚訊息詐騙：



2、手機釣魚簡訊詐騙：



三、防範之道

1、收到有附上**電話或網址連結**的可疑訊息，請勿**回撥或點選**，避免手機被惡意程式入侵。。

2、切勿提供自己的個人資料（如手機號碼及身分證字號）給他人，也不要幫忙**代收簡訊、回傳認證碼簡訊**。

3、若無需要可以致電電信公司客服，**取消小額付款**功能。

4、依照以下步驟更改手機設定：

a. 在手機安全性設定中關閉「允許未知的來源」選項，以免讓不明程式危害手機。

b. 在 LINE 隱私設定中關閉「公開 ID」功能，並開啟「阻擋訊息」功能，讓非好友的用戶無法傳訊給您。

c. 在 LINE 帳號設定中關閉「允許其他裝置登入」功能，讓他人無法以電腦登入您的帳號。

d. 在 LINE 帳號設定中「換機密碼」，降低帳號被盜用的風險。