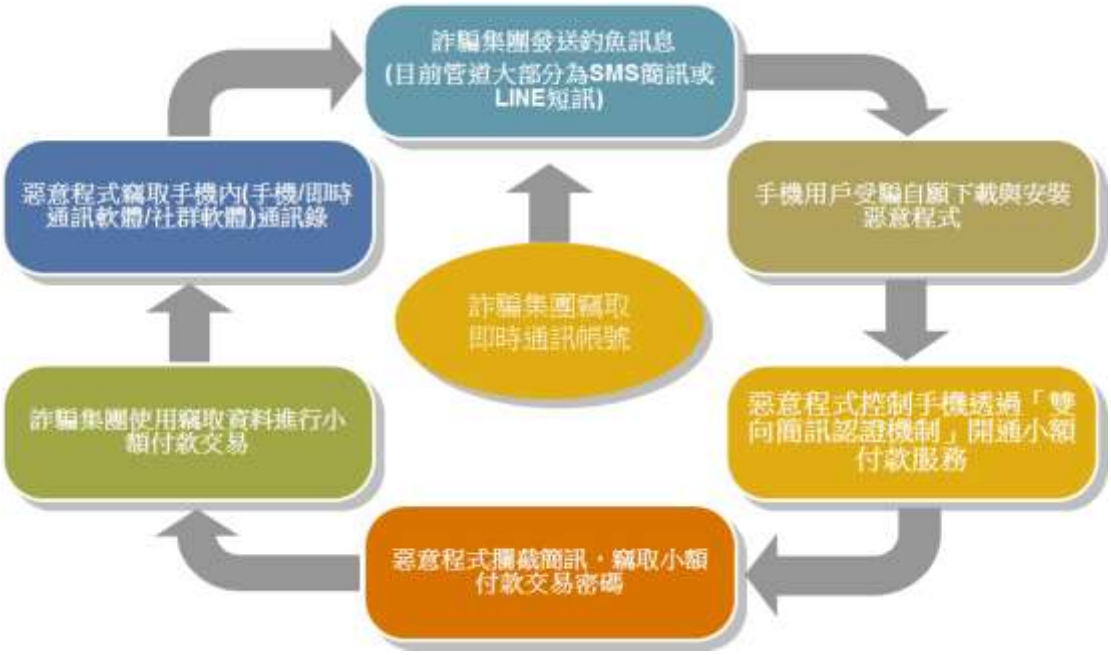
預防智慧型手機詐騙宣導手冊

一、手法說明

智慧型手機惡意程式連結詐騙，是以不同內容與理由透過不同傳輸管道傳送含有惡意程式網址連結的訊息。收訊人一旦點選連結或配合操作，當受訊人手動完成安裝惡意應用程式，手機即遭到詐騙集團控制，盜用電信帳單小額付費服務進行小額付費扣款。常見的詐騙理由是看相簿、支持按讚、假冒好友要求代收驗證碼或是假冒商家要求下載安裝程式，最近歹徒的訊息內容是取消網上電費支付與快遞簽收單。目前常見的訊息傳輸媒介為：手機簡訊與 LINE。

手機傳訊詐騙流程如下圖所示：



手機傳訊詐騙流程圖

手機傳訊詐騙的過程中，有越來越多的案例，詐騙集團

是透過即時通訊軟體LINE來傳送詐騙短訊。盜取帳號來進行詐騙，也被詐騙集團納入工作流程中。目前LINE與臉書帳號可進行整合，提供臉書單一簽入驗證服務，使用同一組帳號密碼即可同時登入臉書與LINE。因此，詐騙集團會透過針對臉書與LINE的釣魚攻擊，收集帳號密碼，再針對通訊錄內的名單進行社交工程詐騙。

二、防護建議

1. 限制惡意程式的安裝

設定手機不允許安裝非市集中的應用程式。設定手機，取消勾選「設定」內的「安全性」/「應用程式設定」中「未知的來源」。

2. 加強LINE的安全性

(1) 開啟「阻擋訊息」功能，設定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，降低收到釣魚訊息的機率。

(2) 不公開個人ID，取消勾選LINE→其他→設定→個人資料→公開ID，避免被陌生人與詐騙集團加為好友

(3) 沒有使用電腦版 LINE的用戶，取消勾選LINE→其他→設定→「我的帳號」中「允許自其他裝置登入」，避免駭客取得的帳密後從電腦登入。

3. 取消電信小額付款機制

請透過手機撥打電信業者客服，告知客服人員取消服務。相關客服電話：中華電信：800; 台灣大哥大：188; 遠傳電信：888; 亞太電信: 999, 威寶: 123。

4. 養成良好使用習慣

(1) 使用任何通訊軟體與社群軟體，切勿使用懶人密碼。

(2) 絕對不要點選傳送來的訊息裡面的連結。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。

(3) 不隨意提供個人資訊，也不轉知簡訊收到的密碼。

(4) 需要使用小額付款的使用者，應啟用「即時消費通知」，若發現詐騙發生，請務必報警，才可當作是被詐騙證明，要求電信業者不能列入帳單或是可到臨櫃辦簽結退款。

(5) 安裝手機防毒軟體。