資安宣導：
使用智慧型手機小心勿點選不明簡訊上的連結

國內惡意簡訊詐騙盛行，刑事局以預付卡門號手機安裝惡意程式進行實測，發現手機遭入侵後在 5 分鐘內就發送 120 則訊息給其他人，直到易付卡儲值的 300 元耗盡才停止。而收訊者還可能遭感染，成為歹徒下一波攻擊的跳板。

刑事局 165 專線以使用易付卡門號的手機，點選惡意簡訊上的連結，依指示下載惡意程式。該手機 1 週後陸續接到民眾回撥，詢問是否為某家快遞物流公司，因為這些民眾收到了以宅急便公司為名義送出的快遞簽收單。

刑事局特別調出該手機的通聯紀錄，發現安裝惡意程式後，在使用者未察覺的情況下手機會代收發簡訊偷偷使用電信業者的小額付費服務，消費者往往到下一期帳單才會發現。

一般而言，小額付費服務多會以簡訊通知交易行為，但手機植入惡意程式後，收到小額付費認證簡訊時也會自動將其刪除，因此使用者也無法在寄件匣中看到發送紀錄，完全無法察覺。另外，收到惡意簡訊的手機也會成為被利用的工具，再將含有惡意程式連結的詐騙簡訊發送給其他人。

通聯紀錄顯示被植入惡意程式的手機，該門號在短時間內發送大量惡意訊息給更多人，試圖使更多人也受害。該手機在安裝惡意程式後一週陸續收到民眾回撥確認發話方是否為快遞公司。

由於手機在短時間內大量發送簡訊，易付卡內的金額很快被用光，電信業者以簡訊通知易付卡用戶餘額已用盡。

刑事局表示，惡意簡訊內容，已從假冒使用者的好友、宅急便快遞簽收、電費網路支付，演變為最近假冒公務機關罰單或法院訴訟通知，民眾若收到這類陌生的簡訊最好不要隨意點選，應先向相關單位查證，以免手機被載入惡意程式。另外，基於安全考量，Android 手機應避免安裝 Google Play 以外的 App，最好進入手機的「設定」-「安全性」，關閉「允許未知來源程式」的功能。

由於小額付費服務通常出現在下一期帳單，被害人都是在收到帳單後才驚覺，刑事局也建議手機用戶向業者主動關閉小額付費服務。同時也希望電信公司從系統端偵測到用戶短時間內大量簡訊異常行為，能夠主動提醒用戶，讓用戶可以檢查手機是否中毒。