

。 手機點選惡意連結中毒實測報告

詐騙集團利用簡訊濫發惡意連結，進行小額付費詐騙時有所聞。刑事警察局反詐騙中心(165專線)進行實測，發現惡意程式除了會代收發簡訊外，還會用中毒手機繼續發送惡意簡訊，甚至阻斷撥打電話，請民眾務必提高警覺。165專線以易付卡門號進行實測，發現手機點選惡意連結，依照指示下載程式中毒後，經過1個禮拜就開始有民眾回撥，詢問該門號是否為黑貓宅急便公司，因為有收到此門號所傳送的快遞簽收通知單。經調閱通聯紀錄，發現此門號被惡意程式綁架後，會出現以下情形：

- 一、代收發簡訊：歹徒利用中毒手機門號進行小額付費，收發認證簡訊，並且將收件夾簡訊刪除，令手機持有人無法察覺異狀。
- 二、濫發簡訊：發送含有惡意連結的簡訊給其他門號，短短5分鐘即發送了120封訊息，將300元的預付額度使用完畢才停止寄送。並且將寄出的簡訊自動刪除，因此寄件備份裡沒有相關資料。

目前惡意連結的簡訊內容，已經從裝好友察看照片、宅急便快遞簽收、電費網上支付，再演變成假冒公務機關的罰單或訴訟通知。警方呼籲，收到附有連結的簡訊時，不要直接點選，務必先向相關單位查證，以免誤載惡意程式。另外在手機的設定裡，務必到安全性-允許未知來源程式的項目，確定是不允許的狀態，避免下載到非google play市集的應用程式。

手機的小額付費，其費用會出現在下一期的帳單，不少被害人是在收到帳單後才發現慘遭詐騙，建議不需要使用這項功能的民眾，可以打電話向電信公司要求關閉。除此之外，也向電信公司呼籲，對於短時間內發送大量訊息的異常使用狀況，應主動告知民眾，提醒渠察看是否中毒，保障用戶財產安全，共同為治安盡一份心力。