

你的手機安全嗎? - 智慧型手機安全防護宣導

定威科技有限公司經理 林志遠

近年來，行動設備發展快速，早期需行動上網時，最喜歡台北市，城市中有許多無線基地台可直接使用，只需透過搜尋所有地是否有無線基地台且沒有設密碼，即可連線使用，這是早期克難的使用方式。現今科技進步，行動設備的功能與一台電腦已無太大差異，駭客可輕易利用行動設備入侵網站或攻擊伺服器，此類手法阻擋難度高且不易追蹤，目前針對行動式入侵並無一套完整的解決方案。

手機中毒已不是新聞，目前常見的 iPhone、Windows Mobile、Android 作業系統都有安全漏洞，能讓駭客輕易控制手機，偷竊手機內敏感資料。特別是 Android 系統，屬開放平台，駭客可輕易在平台上分享含有惡意程式的軟體，讓一般不知情使用者安裝，即可於遠端操控手機上的任意功能。

您安裝了手機惡意程式嗎?

如果常亂下載 APK (Android 上的安裝檔)來安裝的朋友，可能就要檢查一下自己的手機了。要是不慎安裝了手機惡意程式，簡訊、通話內容、通話紀錄就可能受到監控，若將監控到的訊息上傳至伺服器，即造成隱私洩漏或是私密照片外流。

如何預防？

下載手機軟體前請注意不給多餘的權限，危險不容易上身：您的位置：透過手機 GPS 或是 LBS 基地台的方式來取得你的位置。一般來說，只有與地圖相關的應用程式才會使用到這個權限。

應用程式內購買：可以讓應用程式直接用手機撥打電話、簡訊給特定對象，理論上很少有遊戲會用到這個權限。

身分識別：應用程式會存取這台手機上的 Google 帳戶、密碼。一般來說，除了 Google 本身的 App 之外，其他程式應不會用到。

裝置 ID 和通話資訊：很多應用程式都會要求這個權限，這個權限的要求可大可小，透過這個授權可以讀取手機中的聯絡人資料。

系統工具：這個授權可以讓應用程式設定為在開機的時候，自動將程式載入到背景。如果是應用程式要求這個授權還算合理，如果是遊戲的話則很奇怪。

Android 系統智慧型手機需特別注意：

請檢查手機「下載」功能，是否含有「*.apk 檔案」(下圖舉例)，apk 檔案為 android 系統安裝程式，從《PLAY 商店》下載軟體並不會存任何 apk 檔案於下載目錄中，圖中檔案為今年發現的一種手機簡訊木馬程式，會讓使用者手機自動播打小額付費電話。

建議作法：請拿起手機自行檢查下載目錄中是否含有.apk 檔案，如果沒有使用請直接刪除檔案，避免不小心點到。此外，手機誘人受騙

上當的軟體也相當多，目前智慧型手機功能強大但並非萬能，下圖為例為手機太陽能充電 APP，大家都知道並不會安裝了此類 APP，手機就多了太陽能充電的功能吧!

常見手機漏洞簡介—簡訊快遞簽收 APK 後門程式

行為模式

- 1.若不慎點擊經由簡訊傳送的惡意網站，網站會直接下載並且安裝惡意 apk 程式於手機作業系統，這個程式不會顯示任何 ICON 圖示，使用者不會察覺自己被安裝了什麼東西。
- 2.這個程式會於手機執行小額消費交易行為，大多數手機於申辦時並未停用「小額交易(3000 以下金額) 免通知」服務，該程式會利用此種方式進行小額消費，使手機使用者在無察覺的狀況下損失錢財。
- 3.由於手機小額消費部份電信公司是認手機 SIM 卡，並不會再次確認是否為使用者操作行為。傳染途徑受感染的 Android 設備透過簡訊發送功能，把你的姓名加上一串隨機問候語，以及一個惡意鏈結，包裝後用簡訊方式寄送，收到的人不疑有他（上面有你的名字，看起來就像是當事人傳來的簡訊），點擊簡訊裡的惡意鏈結，會自動下載惡意程式 APK 檔或透過轉址網站(<http://goo.gl/>) 連接第三方網站下載惡意程式，手機就會「中毒」。

檢測與預防

Android 的安全性設定裡，有一個「未知的來源」選項，勾選後會允

28

許安裝非《PLAY 商店》線上應用程式商店的軟體，請記得要把這個

選項「取消勾選」，可以降低不小心安裝 APK 程式的風險。

檢測方式可以透過檢查手機電池消耗工具，檢查是否有程式造成電池

異常耗電，或是透過手機隱私顧問清查工具清查存取連絡人程式中是

否有異常程式。

智慧型手機防護大作戰

第一招：找找看 Android 手機「設定」中的「安全性」是否有勾選

「驗證應用程式」的選項，如果有，表示已經開啟了 Google 為

Android 內建的防毒軟體。

第二招：安裝 Clueful 程式，可掃描手機安裝的應用程式，即可了

解每個應用程式取得的資料，以及可能的用途。

建議作法：使用 Clueful 掃描如出現紅色燈號，代表該手機為高風

險，內有程式可能造成個人隱私外洩。

第三招：中毒請恢復原廠設定，還原最乾淨系統，如果真的不幸點擊

到簡訊、LINE 裡的惡意鏈結，也確定下載、安裝了不乾淨的 APK 檔，

建議把手機「恢復原廠設定」，將所有的資料都刪除，重新開始，以

免夜長夢多。

第四招：關閉小額付費，不怕收到額外帳單，連絡 ISP 業者，例如

中華電信，將「小額付費」功能關閉，如果確定不會用到此功能，開著只是徒增被盜用的風險。

第五招：安裝手機防毒軟體，不安裝來路不明的 APK、不安裝 Google Play 應用程式商店以外的軟體等是最好的自保之道，但如果有防毒軟體可以事先把關，在遇到危害前提出警訊，可將損失降到最低。

摘自法務部調查局 105 年 9 月清流月刊 __