

【板橋榮家消費者保護教育宣導篇】

NCC 公布 110 年手機內建軟體資安抽測結果

強化消費者權益

日期：111/06/08 資料來源：國家通訊傳播委員會

智慧型手機已與民眾日常生活密不可分，手機資安防護如有不足，可能造成民眾個資及隱私遭洩露、冒用，甚至財物損失。為促使智慧型手機製造商重視內建軟體資安，積極送測取得手機資安標章，以保護消費者權益，及提升消費者手機資安意識，國家通訊傳播委員會（下稱 NCC）於 110 年下半年至 111 年第 1 季，針對電信事業 110 年第 1、2 季銷售量較高且未取得資安認證之 10 款不同廠牌智慧型手機，再加上 5 款中國大陸廠牌手機，進行手機系統內建軟體之資安檢測，經完成初測、複測及改善程序後，15 款手機均通過檢測。

NCC 表示，鑑於手機資安威脅日漸升高，本次抽測更著重於應用軟體及通訊協定應有之個資保護及加密機制，從台灣資通產業標準協會(TAICS) 110 年公告之「智慧型手機系統內建軟體資安測試規範」中，挑選「內建軟體應將帳號、通行碼或金鑰儲存於作業系統保護區內或以加密方式儲存」、「內建軟體應避免交談識別碼遭重送攻擊」、「與付費功能伺服器間傳輸，應使用安全之加密演算法」、「不可於執行期間將敏感性資料儲存於系統日誌檔案」、「存取敏感性資料前，應取得使用者同意」等 10 個與資安相對應之項目進行檢測。通過檢測之 15 款手機如下：

一、初測即通過：APPLE iPhone 12。

二、複測後通過：初測未通過，經手機製造商積極配合改善後複測通過，包括 ASUS ZENFONE 7、HTC DESIRE 20+、三星 GALAXY A42、SONY XPERIA 5 II、OPPO A72、OPPO RENO 5、REALME X50、REALME C3、SUGAR T30 64/3G DUAL LTE、VIVO Y20、VIVO Y50、REDMI Note 9T、REDMI NOTE 9 PRO、MI 10 LITE 5G 等 14 款。

NCC 強調，手機內建軟體之資安檢測係依行政院國家資通安全會報 103 年 6 月 24 日第 26 次會議決議辦理，前述通過資安檢測之各款手機，代表其系統內建軟體版本在檢測當下符合測項要求；惟考量目前資安事件層出不窮及駭客攻擊手法日新月異，通過檢測的手機，並不能保證未來手機之安全性，手機內建軟體如有更新版本，手機製造商應就更新部分重新檢測及驗證，始

能維持其通過之資安等級，如事後被發現其系統內建軟體仍有資安漏洞或風險時，手機製造商仍應及時修補。

籲請民眾注意相關修補資訊及更新手機內建軟體同時，NCC 另提醒，民眾於手機「自行安裝」之 APP 及其使用習慣等亦存在資安風險，民眾須提高資安風險意識及警覺性選擇值得信任的手機品牌。NCC 並提供民眾保持使用手機良好習慣的「三不五要」口訣，以加強保護個資與隱私安全：

一、三不：

- (一)不瀏覽：不瀏覽可疑網站，以避免可能在手機使用者未注意情形下，自動下載軟體駭入手機，竊取手機內個資或隱私。
- (二)不連接：不連接可疑之 Wi-Fi，具惡意接取點可能監聽手機使用者通訊內容，提升重要資訊洩露風險。
- (三)不強取：不強行取得管理者權限，如利用可疑 APP 取得手機管理者權限，可能導致手機上所有個資及隱私遭竊。

二、五要：

- (一)要更新：要定期更新密碼，並應避免過於簡單之密碼，易遭駭客破解。
- (二)要備份：要更新軟體程式及備份資料，以避免舊版程式漏洞造成損害及資料遺失。
- (三)要關閉：要關閉未使用的 Wi-Fi/藍牙/NFC 等介面，以減少具惡意設備連接，降低手機被駭風險。
- (四)要加密：連接的 Wi-Fi 要開啟加密防護，可避免有心人監聽手機網路通訊取得重要資訊。
- (五)要刪除：手機不再用時要刪除機敏資料，可避免機敏資料遭他人擷取。

NCC 進一步強調，為強化民眾對智慧型手機資安防護意識及確保消費者權益，NCC 已在官方網站設置宣導專區提供相關資訊供民眾參閱，並適時向民眾揭露手機內建軟體可能存在之資安威脅或風險，亦將持續關注國際間對連網設備之相關資安防護建議及措施，滾動修正手機系統內建軟體相關檢測規定。未來 NCC 仍會在有限的行政資源內，持續推動智慧型手機內建軟體資通安全抽測及公布結果，並加強抽測中國廠牌手機，以促使手機製造商在手機設計製造時更加重視手機內建軟體資安，確保消費者權益。

連絡人：吳副處長銘仁

電話：02-3343-8202

行動電話：0928-601-199