

OUCH!

全民資訊安全意識月刊

汰除您的行動裝置

概述

行動裝置，如智慧手機、智慧手錶和平板電腦，以驚人的速度不斷進步和創新；結果是，有些人每年更換行動裝置。不幸的是，人們往往沒有意識到有多少個人資料還留存在這些設備上。下面我們將介紹您的行動裝置上可能存在的資訊，以及您在淘汰裝置之前應如何安全地將其清除。如果您的行動裝置是由您的雇主派發的，或儲存了任何與工作相關的資料，請務必先與您的主管確認正確的備份和淘汰流程。

您的資訊

許多人不知道行動裝置儲存的敏感資料往往比電腦還多：



- 您的居住地、工作地點和造訪過的地方。
- 每筆在通訊錄中的連絡資料，包括了家人、朋友和同事
- 手機通話記錄，包括來電、撥出、語音信箱和未接來電
- 即時通訊軟體、遊戲和社交媒體等應用程式中的打字或對話紀錄
- 網頁瀏覽記錄、搜尋歷史記錄、cookie 和暫存頁面
- 個人照片，影片和錄音記錄
- 您的銀行帳號、社交媒體或電子郵件儲存的密碼和存取的權限
- 與健康相關的資訊，包含您的年齡、心跳率、運動史或血壓

清除您的裝置

無論您打算如何處置您的行動裝置，捐贈、換新機、送給家人、轉賣甚至扔掉它，首先您必須要確認是否已抹除所有敏感資訊。僅僅刪除檔案是不夠的，您應該安全地移除裝置上的所有資料，最簡單的方法就是還原您的裝置。不同類型的裝置有不同的還原設定；以下列出的是兩種最常見裝置的還原步驟。更安全的一步是確保您的

設備已啟用加密，然後再將其重新還原。對近期的大多數行動裝置而言，最簡單的方法就是啟用螢幕鎖(希望您已經啟用它)。最後，我們強烈建議您在還原裝置之前先備份資料。



- 蘋果iOS裝置：設定／一般／重置／清除所有內容和設定
- 安卓裝置：設定／隱私／恢復原廠資料

SIM卡或擴充卡

除了您的裝置，您也需要考量如何清除您的SIM卡(用戶識別模組)。行動裝置使用SIM卡進行蜂巢或資料連線。當您清除您的裝置，SIM卡仍會保留與您綁定的帳號資訊。如果您打算保留電話號碼並轉移到新的裝置，請與您的電信業者聯繫，瞭解如何轉移您的SIM卡。如果無法轉移，留下您的舊SIM卡並將其實體破壞以防止有心人士使用它冒充您的身分並獲取您的帳號與資訊。最後，有些安卓系統的行動裝置可插拔SD記憶卡(數位加密卡)來增加儲存容量。在汰除行動裝置前，請取出這些外部儲存卡。這些卡通常可以在新的行動裝置中重複使用，或者透過USB轉接在電腦上當隨身碟。如果SD卡不能重複使用，我們建議您和處置舊SIM卡一樣，將其實體破壞。

如果您對上面介紹的任何步驟有疑問，或者您的裝置有不同的還原選項，請將您的行動裝置帶到購買店家，並尋求專業的技術人員協助。最後，如果您想要扔掉一個裝置，請考慮以捐贈代替丟棄。有許多合適的慈善組織接受二手行動裝置，許多供應商也都提供回收服務。

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站 <http://www.tsc-tech.com/>或臉書@tsctech了解更多訊息。

客座編輯

Christopher Crowley (@CCrowMontance) 是一位專注於安全行動的華盛頓特區獨立顧問。他偶爾會在推特和部落格上發文。請留意他即將發表的一本關於安全行動中心新書。他是SANS研究所的資深講師。



參考資源

SANS課程：行動裝置滲透測試: <https://sans.org/sec575>
SANS課程：進階智慧型手機鑑識課程: <https://sans.org/for585>
聯邦貿易委員會的淘汰行動裝置建議: <https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device>
行政院行動裝置資通安全注意事項: <https://nicst.ey.gov.tw/Page/16FFA138E66A0905/a91dad4c-11e6-43e7-a4bb-23af28029988>

OUCHE!由SANS Security Awareness發行刊登，遵從Creative Commons BY-NC-ND 4.0(創意公用授權條款4.0版)。在不更改本刊物內容的前提下，您能夠自由分享此月刊或使用於您的安全認知計劃。有關翻譯或其他資訊，請聯絡 www.sans.org/security-awareness/ouch-newsletter。
編輯委員會：Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | 翻譯群：黃意雯、宋亞倫、顧君毅、孫權劭、葉力維、莊銘輝