全民資訊安全意識月刊

OUCH!

本期話題

- **概述**
- **取得行動裝置應用程式**
- **權限**
- **更新應用程式**

安全地使用行動裝置應用程式

概述

客座編輯
Joshua Wright是Counter Hack的技術總監和SANS協會資深講師。他也是SEC575：行動裝置安全和道德駭客（SEC575:Mobile Device Security and Ethical Hacking），以及駭客現形：無線網路篇（Hacking Exposed: Wireless）兩書的作者。可以搜尋Josh的Twitter帳號**@joswr1ght**與他聯繫。

行動裝置如平板電腦、智慧型手機和智慧型手錶已成為我們在個人日常生活和職場工作中不可或缺的科技產品。數百萬個可供選用的Apps，使得行動裝置有了許多不同的功能。這些Apps不僅使我們能夠提高工作效率，可以與他人即時溝通和分享，進行教育訓練，甚至能夠滿足娛樂需求。然而，使用這些厲害的Apps同時也帶來了風險。遵循以下的步驟能夠使您安全地充分使用Apps。

取得行動裝置應用程式

第一步是確保始終從安全可靠的來源下載Apps。網路罪犯已經擁有高超的技術，能夠開發和散佈看起來合法的惡意Apps。如果您安裝了其中一個受到感染的App，犯罪份子就可以完全控制您的行動裝置。因此，只從知名且可信任的來源下載Apps，能夠減少安裝到受感染Apps的機率。另外，您可能沒有意識到的是，行動裝置的品牌決定了您下載Apps時的選項。

對於蘋果（Apple）設備來說（如iPad或iPhone），只能從Apple App Store下載Apps。這樣做的優點是，這些 Apps在上架前都會經過蘋果公司的安全檢查。雖然蘋果公司不見得能找出全部有問題的Apps，但透過這個管控平台有助於大幅降低安裝到受感染App的風險。此外，如果蘋果公司在Apple App Store中發現任何確信受到感染的Apps，也會立即刪除。Windows Phone也使用類似的方法管理Apps。

而安卓（Android）行動裝置則是採取不同的做法。安卓可以從網路上的任何地方下載Apps，這使您能更有

安全地使用行動裝置應用程式

彈性的使用, 但也帶來更多的自我管控責任。您必須在下載和安裝Apps時更加謹慎, 因為並非所有行動Apps都有經過審核。谷歌 (Google) 會維護一個類似於Apple App Store的App商店, 名為Google Play。從Google Play下載的Apps通過了一些基本的安全檢查。因此, 建議您只從Google Play下載安卓裝置的Apps, 避免從其他網站下載Apps, 因為任何人 (包括網路罪犯) 都可以輕鬆開發和散佈惡意Apps, 並誘騙您下載安裝進而感染行動裝置。另外, 盡可能在您的行動裝置上安裝防毒軟體作為額外的保護。

安全地使用行動應用程式的關鍵在於只從受信任的來源安裝Apps, 安裝可用的更新, 以及僅同意必要的Apps權限。

無論是使用哪種裝置, 另一個您可以採取的防範措施是避免安裝全新的、下載人數極少或幾乎沒有正面評論的Apps。只要是被使用的時間越長、使用的人越多、正面評論越多, App的可信度就越高。此外, 只安裝必要的Apps。試著問自己, 我真的需要這個App嗎? 每個App不但都有可能造成新的資安漏洞, 還會帶來新的隱私問題。如果您不再使用某個App, 請從行動裝置中將其移除 (如果日後需要使用, 可以再次安裝) 。最後, 永遠不要刷機 (root) 或越獄 (jailbreak) 您的行動裝置, 因為這會造成裝置被入侵並安裝未經授權的Apps, 或是改寫現存的內建功能。這不僅跳過或取消了許多行動裝置內建的安全性設定, 而且通常也會使得原廠保固及維修服務合約失效。

權限

一旦從可信任的來源安裝App後, 下個步驟是確保其符合安全設定及隱私保護規範。在允許App存取功能之前, 請務必考慮: 您是否要同意App請求的權限? 這個權限真的是必要的嗎? 例如, 某些Apps會使用地理定位服務; 如果開啟持續定位功能, 您可能視同允許開發者追蹤您的行蹤, 甚至同意開發者將該資訊出售給他人。如果不願意授予權限, 就拒絕權限請求或購買其它符合您需求的App。請記得, 您還有許多的Apps可供選擇。

安全地使用行動裝置應用程式

更新應用程式

Apps就如同電腦和行動裝置的作業系統，必須透過更新以保持最新狀態。犯罪份子不斷地搜尋Apps中的弱點，然後利用這些弱點開發攻擊的方法和工具。開發人員會建立和發佈更新以修復這些弱點並保護您的裝置；檢查和安裝更新的頻率越高越好。大多數裝置允許您的系統設定自動更新Apps，我們建議使用此設定。如果沒辦法做到，我們建議您至少每兩週檢查一次更新。最後，當Apps更新完成，請務必確認任何新提出的權限請求。

進一步了解

歡迎訂閱OUCH!　全民資訊安全意識月刊，以及瀏覽前期OUCH!檔案。想要進一步了解SANS資訊安全意識方案，請瀏覽我們的網站 securingthehuman.sans.org/ouch/archives.

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。

參考資料

社交工程:	https://securingthehuman.sans.org/ouch/2017#january2017
安全地處理掉行動裝置:	https://securingthehuman.sans.org/ouch/2016#december2016
保護您的新平板電腦:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH檔案及翻譯:	https://securingthehuman.sans.org/ouch/archives
行動裝置安全課程:	https://sans.org/sec575

編輯委員會：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley
翻譯群：邱俊傑、黃意雯、宋亞倫、孫權劭、王澤薇

