

OUCH!

本期話題

- 概述
- 獲取移動應用
- 權限
- 更新應用程序

安全地使用移動應用程序

概述

移動設備如平板電腦, 智能手機和手錶已成為我們在個人和職業生活中使用的主要技術之一。什麼使移動設備如此多才多藝是我們可以選擇的數百萬的應用程序。這些應用程序使我們能夠提高工作效率, 即時溝通和與他人分享, 訓練和教育, 或只是有更多的樂趣。然而, 伴隨著所有這些移動應用程序的力量是風險。以下是一些步驟, 您可以採取安全地使用和充分利用您的移動應用程序。

客座編輯

Joshua Wright是Counter Hack的技術總監和SANS研究所的高級講師。他是[SEC575 : 移動設備安全和道德黑客], [黑客暴露: 無線]的作者。在Twitter [@joswr1ght](#)上可以找到Josh。

獲取移動應用

第一步是確保您始終從安全可靠的來源下載移動應用程式。網絡罪犯已經熟練了他們在創建和分發看似合法的受感染移動應用程序方面的技能。如果您安裝其中一個受感染的應用程序, 罪犯可以完全控制您的移動設備。通過僅從知名的可信來源下載應用, 您可以減少安裝受感染應用的機會。您可能沒有意識到的是, 您使用的移動設備的品牌決定了您下載應用的選項。

對於Apple設備 (如iPad或iPhone), 只能從Apple App Store下載移動應用程序。這樣做的優點是, 蘋果在所有移動應用程序可用之前對其進行安全檢查。雖然蘋果無法捕獲所有受感染的移動應用程序, 但如此受管環境有助於大幅降低安裝受感染應用程序的風險。此外, 如果蘋果在它的商店發現一個認為被感染的應用程序, 它會快速刪除該移動應用程序。Windows Phone使用類似的方法管理應用程序。

安全地使用移動應用程序

Android 移動設備則不同。Android 可以從互聯網上的任何地方下載移動應用程序，從而為您提供更大的靈活性。然而，隨著這種靈活性，帶來更多的責任。您必須更加謹慎地下載和安裝那些移動應用，因為並非所有移動應用都經過審核。Google 會維護一個類似於 Apple 的管理型移動應用商店，名為 Google Play。您從 Google Play 下載的移動應用通過了一些基本的安全檢查。因此，我們建議您只從 Google Play 下載 Android 設備的移動應用。避免從其他網站下載 Android 移動應用，任何人（包括網絡罪犯）都可以輕鬆創建和分發惡意移動應用，並誘騙您感染移動設備。作為額外的保護，可能的話在您的移動設備上安裝防病毒。



安全使用移動應用的關鍵是只安裝來自受信任來源的應用，隨時安裝更新，並僅授所需的應用權限。

無論您使用的是哪個設備，您可以採取的另一個步驟是避免全新，少數人下載或幾乎沒有正面評論的應用程式。應用程式的可用時間越長，使用它的人越多，評論越積極，應用程式的可信度就越高。此外，只安裝您需要和使用的應用程式。問自己，我真的需要這個程序嗎？不僅每個應用程式可能帶來新的漏洞，而且還有新的隱私問題。如果您停止使用某個應用，請從移動設備中移除該應用（如果您後來發現還需要，可以隨時將其添加回來）。最後，永遠不要越獄或root您的移動設備。這是進入設備中並安裝未批准的應用程式或更改現有的內置功能的過程。這不僅繞過或消除了移動設備中內置的許多安全控制，而且通常也會使保修和支持合同失效。

權限

從可信來源安裝移動應用後，請確保已經過安全配置並保護您的隱私。在允許移動應用訪問之前，始終要考慮：您是否要向應用授予其請求的權限，應用真的需要它嗎？例如，某些應用使用地理位置服務。如果您允許

安全地使用移動應用程式

應用始終知道您的位置，則可以允許該應用的創建者跟踪您的移動信息，甚至允許應用作者將該信息出售給他人。如果您不希望授予權限，拒絕權限申請或購買符合您要求的其他應用程式。記住，您有很多選擇。

更新應用程式

移動應用（如電腦和移動設備操作系統）必須更新，以保持最新狀態。犯罪分子正在不斷地搜索並找到應用程式中的弱點。然後他們以利用這些弱點來開發設計攻擊。創建您的應用程式的開發人員還會創建和發布更新以修復這些缺陷並保護您的設備。檢查和安裝更新的頻率越高越好。大多數設備允許您設置系統執行自動更新移動應用。我們建議使用此設置。如果這是不可能的，那麼我們建議您至少每兩週檢查一次移動應用的更新。最後，當您的應用程式更新時，請務必驗證任何新的權限。

進一步了解

歡迎訂閱OUCH!電腦用戶安全意識月刊，以及瀏覽前期OUCH!檔案。想要進一步了解SANS安全意識的方案，請瀏覽我們的網站securingthehuman.sans.org/ouch/archives。

參考資料

社會工程:	https://securingthehuman.sans.org/ouch/2017#january2017
處置您的移動設備:	https://securingthehuman.sans.org/ouch/2016#december2016
保護您的新平板電腦:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH檔案和翻譯:	https://securingthehuman.sans.org/ouch/archives
移動設備安全課程:	https://sans.org/sec575

OUCH! 由SANS Securing The Human發行刊登，遵從[Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/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，你可以自由分享此月刊或使用於你的安全意識計劃。有關翻譯或更多諮詢，請聯絡ouch@securingthehuman.org。

編輯委員會：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
翻譯：巴珊珊



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus