

OUCH!

本期話題

- 主要概況
- 獲取應用程序
- 權限
- 應用程序更新

安全使用移動應用程序

主要概況

移動設備如平板電腦和智能手機已成為我們在個人和職業生活中使用的主要技術之一。是什麼讓移動設備如此多才多藝，是因為有數以百萬計我們可以選擇的應用程序。這些應用程序使我們的工作效率提高，即時溝通，並與他人分享培訓和教育，或者只是有更多的樂趣。然而，所有這些移動應用程序的好處也帶來風險。這裡有一些步驟，您可以採取安全地使用和維護您的移動應用程序。

編輯嘉賓

是獨立的顧問，和認證SANS講師以及課程作者。他以@CCrowMontance活躍在Twitter上，以+ChrisCrowley活躍在 Google plus上。

獲取移動應用

第一步是確保您總是從一個安全，可信的來源下載。請記住，幾乎任何人都可以創建一個移動應用程序，所以您要小心從哪裡得到它們。網絡犯罪分子已經在創造和分配，似乎是合法的感染病毒的移動應用程序來磨練他們的技能。如果您安裝了一個感染的應用程序，這些罪犯可以控制您的移動設備，包括讀取電子郵件，聽您的談話，並獲取您的聯繫人。從只有知名，可信來源下載的應用程序可以減少安裝受感染的應用程序的機會。您可能不知道的是，您移動設備的品牌決定了您的選擇。

對於蘋果設備如iPad或iPhone，您只能從，蘋果App Store的託管環境裡下載移動應用程序。這樣做的好處是蘋果做即時移動應用程序和其作者的安全檢查。雖然蘋果不能捕獲所有的壞人或所有受感染的移動應用程序，這種管理的環境，有助於減少您安裝受感染的應用程序的風險。此外，如果蘋果發現被感染的應用程序，他們會迅速取消此移動應用程序。Windows手機採用了類似的方法來管理應用程序。

安全使用移動應用程序

Android的移動設備是不同的。 Android給您更多的靈活性，能夠從互聯網上的任何地方下載移動應用程序。然而，隨著這種靈活性是更多的責任。您必須要小心下載什麼手機應用程序，因為不是所有的都經審查安裝的。Google保持了類似蘋果店的移動應用程序管理，被稱為Google Play。您從Google Play下載的移動應用程序有一些基本的檢查。因此，我們建議您下載到Android設備的移動應用程序只能從Google Play下載。避免下載來自其他網站的Android移動應用程序，因為任何人，包括網絡犯罪分子可以很容易地創建和分發惡意移動應用程序，並誘騙您感染您的移動設備。作為一個額外的保護，考慮在您的移動設備上安裝防病毒軟件。



安全地使用移動應用程序的關鍵是只從信任的來源安裝的應用程序，以及確保您的應用程序更新，並驗證您的權限。

為了更加降低風險，避免全新的，只有幾個人下載，或者很少有正面評價的應用程序。時間越長的應用程序越有更積極的評價，越可以被信任。另外，只安裝您需要的應用程序和使用。問問自己，我真的需要這個程序？不僅每個應用程序可能會帶來新的安全漏洞，而且也有新的隱私問題。您停止使用的應用程序，應從您的移動設備中刪除它（如果您發現您需要它，您以後可以隨時添加回來）。

最後，您可能想越獄或root您的移動設備。這是侵入並安裝未經批准的應用程序或改變現有的內置功能的過程。我們強烈建議不要越獄或者root，因為它不僅會繞過或消除了許多內置到您的移動設備的安全控制，而且往往也違反了保證和支持合同。

權限

一旦您從一個可信賴的來源安裝一個移動應用程序，下一步就是確保其安全配置，並保護您的隱私。安裝和/或配置的移動應用程序經常需要授予特定的權限。總是在授權任何訪問之前想想，您的應用程序是否確實需要這些權限來完成其既定的工作？例如，一些應用程序使用地理位置服務。如果允許一個應用程序總是知道您的位置，您可能

安全使用移動應用程式

會允許該應用程式的創建者追蹤您的動作，也許他們甚至可以出售這些信息給他人。如果您不希望給予一個應用程式請求的權限，貨比三家找另一個應用程式，直到滿足您的要求。請記住，您有很多選擇。蘋果設備允許一些權限的設置，或在運行時改變，如獲得地理位置信息。Windows和Android的移動設備不同，它們是一個全有或全無的方式。如果不授予所有指定的權限，則無法安裝應用程式。

更新應用程式

移動應用程式，就像您的電腦和移動設備的操作系統，必須保持當前更新。犯罪分子正在不斷尋找和發現應用程式的弱點。然後，他們利用這些弱點制定攻擊。創建您的應用程式的開發人員還可以創建和發布更新修復這些弱點，並保護您的設備。您越經常檢查並安裝更新越好。大多數平台可以設置您的系統自動更新移動應用程式。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個星期檢查更新您的移動應用程式。然而，當您的應用程式總是被更新，確保您驗證任何它們可能需要的新的權限。

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<http://www.securingthehuman.org>。

參考資料

社會工程:	http://www.securingthehuman.org/ouch/2014#november2014
處理您的移動設備:	http://www.securingthehuman.org/ouch/2014#june2014
保護您的新平板電腦:	http://www.securingthehuman.org/ouch/2013#december2013
常見的安全條款:	http://www.securingthehuman.org/resources/security-terms
SEC575：移動設備安全課程:	http://www.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
翻譯：巴珊珊



securingthehuman.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



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



[securingthehuman.org/gplus](https://plus.google.com/securingthehuman.org)