

OUCH!

全民資訊安全意識月刊

保護您的行動裝置

概述

現今行動裝置使您與朋友聯絡、在網上購物、使用網路銀行、觀賞電影、打電動和進行其他各種活動變得格外有趣以及容易。行動裝置已嚴然成為大家生活中重要的部分，這邊有幾個簡單步驟可以保護您和您的行動裝置安全。

保護您的行動裝置

大家可能會很驚訝，在使用行動裝置時最大的風險是來自於您自己，而不是駭客，因為大家遺失行動裝置或不小心將它遺留在某處的可能性比被人駭入還要來得高。因此，保護您的行動裝置第一要務是啟用自動鎖定螢幕功能，通常稱為螢幕上鎖。這意謂每次要使用行動裝置時，要以高強度的密碼或是您的指紋來解鎖螢幕。這可以確保如果行動裝置遺失或是失竊時，其他人將無法存取裡面資訊。此外，以下幾個小秘訣可以用來保護您的行動裝置：

✔ 軟體更新

請啟用自動更新功能，讓行動裝置作業系統或應用程式可以隨時維持在最新的版本。駭客通常會鎖定軟體弱點進行攻擊，為此廠商會持續地釋出更新版軟體或修補程式來修正這些漏洞。經由維持最新版本的作業系統及應用程式，可以使您的行動裝置較難被人駭入。

📍 追蹤軟體

建議安裝或啟用可以透過網路遠端追蹤您的行動裝置的軟體，如此一來，若行動裝置不小心遺失或失竊，可以透過網路連線至行動裝置，並且找到它的所在位置；甚至在最糟的情況下，您可以遠端清除行動裝置上的所有資料。

✔ 受信任的應用程式

建議只從信任的來源下載您需要的應用程式。如果是Apple iPad或是iPhone系列，請在Apple App Store下載應用程式。對於Android系統來說，可從Google Play商店來下載；另外，Amazon 平板裝置則

應從Amazon App Store下載。雖然大家能夠從其他網站下載應用程式，但這些應用程式並未經過審查，而且很可能已遭到感染；此外，下載任何應用程式之前務必請確認是否有得到正面的評論，並且廠商會積極進行更新。千萬不要使用那些上架沒有多久、幾乎沒有得到正面評論、或很少在更新的應用程式。最後，不論您是從哪裡下載這些應用程式，只要您不再需要使用，或甚至很少使用，我們建議請從您的行動裝置上移除。

隱私選項

當安裝新的應用程式時，請確認已查看過隱私選項。舉例而言，那些要求存取您所有好友資訊及其他聯絡訊息的應用程式，是否有其必要性？同時我們建議請先關閉全部的定位功能，再為有需求的特定應用程式來開啟。如果您不確定應用程式要求的權限是否合理，建議找其他符合您需求的應用程式；另外，請定期確認這些權限要求是否已變動。

備份

請定期備份資料。行動裝置通常會自動備份大量關於您的資料，像是照片或簡訊，甚至包含了您行動裝置的個人設定、應用程式、及其他有關的資訊，這讓裝置在不慎遺失或是更換新裝置時可以快速的進行資料復原。

工作

當在工作的時候要特別小心，絕對不要拍到可能含有敏感資訊的照片或影片，像是白板或是電腦螢幕上的畫面。

現今的行動裝置已嚴然成為功能相當強大的工具，在您盡情使用的同時，只要遵循以上這些簡單步驟就可以對您和您的行動裝置安全大有助益。

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

密碼短語:	https://www.sans.org/u/A3E
密碼管理器:	https://www.sans.org/u/A3z
雙因子驗證:	https://www.sans.org/u/A3u
備份:	https://www.sans.org/u/A3p
SANS每日安全小秘訣:	https://www.sans.org/tip_of_the_day.php

執照

OUCH!由SANS Securing The Human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, Cathy Click, Cheryl Conley | 翻譯群：黃意雯、宋亞倫、顧君毅、孫權劭、葉力維、莊銘輝