行動裝置資通安全注意事項（簡要版）

一、行動裝置資安防護建議：

(一)軟體下載與使用

- 僅安裝來自可信任來源之軟體
- 注意軟體安裝時所要求之權限是否合理
- 定期進行軟體更新或修補作業
- 安裝資安防護軟體

(二)資料保護

- 注意資料備份與加密防護
- 安裝具「可遠端定位並進行資料清除」功能的資安軟體
- 注意廢棄行動裝置之資料處理

(三)連線功能設定

- 小心使用公開的無線 Wi-Fi 網路
- 小心使用藍芽(Bluetooth)功能
- 小心使用全球定位(Global Positioning System ,GPS)功能
- 小心使用近場通訊(Near Field Communication,NFC)功能

(四)設定行動裝置密碼自動鎖定功能

(五)其他

- 請勿修改或破解行動裝置之安全措施
- 請勿利用行動裝置進行重要交易行為

二、行動裝置存在資安威脅徵兆：

(一)電池壽命變短

(二)通話經常不尋常中斷

(三)電信費用異常

(四)自動下載軟體

(五)手機效能變差

行動裝置資通安全注意事項

行政院國家安通安全會報技術服務中心

一、前言

智慧型手機與平板電腦等行動裝置由於攜帶方便、輕巧靈活，並可提供如：收發電子郵件、儲存文件、瀏覽簡報、遠端存取資料，甚至遠端存取其他網路設備等功能特性，有助提高行動辦公環境的生產力與效率，但同時也帶來新的資安威脅。

為加強行動裝置的資安防護，避免可能的風險與危害，謹提供下列行動裝置防護建議供參。

二、防護建議

行動裝置的資安要求與電腦的資安要求並無二致，即為保護行動裝置的機密性、完整性及可用性：

➢機密性意指確保傳輸與儲存之資料無法被未授權人士存取。

➢完整性意指偵測傳輸與儲存之資料是否被有意或無意的變更。

➢可用性意指確保使用者可透過行動裝置存取所需的資源。

為滿足以上的資安要求，行動裝置需要多項資安保護措施，以下將依軟體下載與使用、資料保護、連線功能設定及密碼設定等類別，分別提出防護建議。**其中連線功能設定與密碼設定係透過行動裝置內建功能即可達成**。

(一)軟體下載與使用

➢僅安裝來自可信任來源之軟體

在行動裝置下載軟體前，除先行針對欲安裝之軟體進行安全性之基本評估（如：檢視要求權限、使用者評論等）外，請儘可能確保軟體來自於合法的官方軟體商店(如 App Store、Google Play)，切勿從無法驗證其可靠性之

來源下載安裝軟體，以避免安裝已遭植入非正當意圖之軟體，導致行動裝置資料遭竊、或被安裝後門程式及對行動裝置產生損害之風險。

➢注意軟體權限

行動裝置上的軟體於安裝或在第一次使用時，大都會詢問使用者其可讀取的軟體權限，惟部分軟體會要求讀取行動裝置的地理位置 (GPS)、通訊錄、通話次數及系統工具等敏感資料。因此，使用者於安裝軟體時，請注意該軟體是否要求不必要的權限。此外，軟體於更新時，大都也會重新詢問其可讀取的軟體權限，請再確認該軟體所要求的權限是否合理，再評估是否進行安裝。

➢軟體定期更新修補程式

行動裝置上的軟體(如瀏覽器)或作業系統，可能因漏洞而遭受駭客攻擊，如，瀏覽網頁時被轉址到惡意網站或釣魚網站，造成敏感資料外洩或被植入惡意程式等資安問題。因此，行動裝置上的軟體或作業系統應定期自動或手動安裝更新修補程式。

➢安裝資安防護軟體

為避免下載已知的惡意程式與瀏覽惡意網站，可透過安裝資安防護軟體（如防毒軟體），以偵測已知的惡意程式與惡意網站。

機關可以利用行動裝置管理系統(Mobile Device Management, MDM)管理機關內的行動裝置。MDM 主要目的在於限制行動裝置上，可以從事的行為，甚至可遠端變更與清除行動裝置的內容，如，機關可透過 MDM 發送簡訊，亦可進行要求行動裝置設置密碼、限制密碼長度、加密行動裝置內的檔案、使用軟體權限等各類政策。

(二)資料保護

➢資料備份與加密防護

將行動裝置內的資料進行備份將有利於行動裝置毀損或遺失時，進行資料回復。而使用行動裝置原廠提供之雲端備份服務時，需謹慎檢視與選擇欲備份之資料項目。無論使用官方廠商或第三方提供之行動裝置雲端服務（如 iCloud、Dropbox、Google Drive、Microsoft SkyDrive 等），仍應謹慎選擇使用之資料項目與應用範圍，以避免將機敏資料誤送到雲端。而對於儲存於行動裝置內的敏感資料，可透過安裝加密軟體予以防護。

➢遠端定位與資料刪除

行動裝置遭竊或遺失時有所聞，除建議不要在行動裝置中留存重要資料外，另建議安裝具有「可遠端定位並進行資料清除」功能的資安軟體（iOS 用戶在註冊登錄 Apple ID 帳號後，均可綁定屬於自己的 Apple 行動裝置，可使用 Find My iPhone 軟體進行行動裝置追蹤與遠端資料刪除，但行動裝置須與網際網路連線的情況下；Android 則無預設的官方行動裝置追蹤保護功能，須透過安裝額外軟體達成）。

➢廢棄行動裝置之資料處理

行動裝置於報廢、販賣、捐贈或回收等行為時，應完整清除其上所有資料，並回復為行動裝置之出廠設定。

(三)連線功能設定

➢小心使用公開的無線 Wi-Fi 網路

行動裝置可透過無線 Wi-Fi 與行動上網等方式連線使用的網際網路，由於這些通訊系統可能遭到竊聽，或遭遇「中間人攻擊(Man-in-the-middle」，MITM)，因此建議應避免使用公開無線 Wi-Fi 網路傳輸隱私性高或機敏資料，並確保所使用的網路系統為可信任的網路（如 iTaiwan），而不使用未知的無線 Wi-Fi 網路。此外，行動裝置在未使用 Wi-Fi 功能進行無線上網時，應將其關閉，以避免有心人士利用 Wi-Fi 訊號或 Wi-Fi 介面進行竊

聽、干擾或藉由漏洞破壞 Wi-Fi 服務，進而竊取個人連線資料或入侵行動裝置。

➢小心使用藍芽(Bluetooth)功能

行動裝置上的藍芽功能也可能受到「中間人攻擊」的影響，因此，不使用藍芽功能以進行無線耳機、無線鍵盤或檔案傳輸連結時，應將其關閉，以避免有心人士利用藍芽介面進行干擾或藉由漏洞破壞藍芽服務，進而入侵行動裝置。

➢小心使用全球定位(Global Positioning System ,GPS)功能

行動裝置多具備 GPS 功能，許多軟體如導航、社群及廣告等均依賴此功能的定位能力，以更正確地提供個人化、在地化及客製化的服務。然而這些定位資訊涉及用戶的個人行蹤，可能被有心人士用於目標式攻擊，攻擊對象的實體位置與裝置資訊可被更容易掌握。因此，於使用軟體時，若須將定位功能開啟，請確認其必要性，並於未使用定位功能時，將其關閉。

➢小心使用近場通訊(Near Field Communication,NFC)功能

行動裝置若內建 NFC 功能，則可與其他 NFC 標籤互動，將其內容讀取至行動裝置內解譯，並進行資料處理。這些資料可能是一個網址、一段訊息或一段程式碼。因此，惡意的 NFC 標籤可能將行動裝置導至惡意網站，建議使用者在不需要使用 NFC 時，應將其關閉。

(四)設定行動裝置密碼自動鎖定功能

為使用方便起見，我們通常並未將行動裝置設置密碼。為避免未經授權的第三人藉機存取行動裝置內各項資料，行動裝置應設定為當行動裝置重新啟動、閒置或按下待機鈕後一段時間內未使用時，自動進入畫面上鎖模式。此模式之解除，應以密碼為之，而此密碼則應注意長度、複雜度及避免多個帳戶使用相同密碼等。

(五)其他

➢避免修改或破解行動裝置之安全措施

行動裝置會內建一些保護措施以加強其安全性（例如不能安裝非官方 App 等），惟使用者可透過破解方式，取得行動裝置上的最高權限，以完全掌控行動裝置功能。但此行為將因內建保護措施被規避，而造成行動裝置面臨資安上的威脅。因此，建議不要破解行動裝置之安全措施。

➢網路使用行為

行動裝置逐漸成為駭客攻擊的主要目標之一，建議不要利用行動裝置進行重要交易，倘若無法避免，則應透過平時收藏的書籤或知名搜尋引擎，直接點擊進入官網。並且不要相信不明網站、不明簡訊及社群網站所分享的連結，甚至廣告連結都不應過度相信，以確實降低誤觸零時差攻擊與惡意 JavaScript 攻擊的風險。此外，應儘量避免透過行動裝置上的通訊軟體（如 Line、WhatsApp、WeChat 等）討論重要資訊或交換檔案，並且避免加入來歷不明的聯絡人，以免遭受社交工程詐騙上當之風險。

三、洞燭機先

以下 5 個徵兆，可能是在提醒您該檢視行動裝置（一般為手機）的資安情形：

(一)電池壽命變短

資安威脅會讓行動裝置電池比平常更加耗電，通常的原因是來自惡意廣告和垃圾軟體，不斷顯現的廣告會讓電池過度耗電。不管是隱藏在執行程式中或是偽裝成普通 App 的惡意軟體，異常的電池表現通常就是告訴您，行動裝置可能存在有資安威脅了。

(二)通話經常不尋常中斷

資安威脅有可能影響行動裝置的通話功能，會造成不尋常的通話中斷；您可以先打電話給電信商，確定是否為線路問題，如果不是的話，可能某人正在竊聽您的通話，或進行其它可疑活動。

(三)電信費用異常

資安威脅可能讓受感染行動裝置自動發送簡訊，不過並非所有的資安威脅皆會發送大量的簡訊，可能會發送小量簡訊，以免讓用戶起疑，如果覺得帳單異常，宜確認行動裝置是否已存在資安威脅。

(四)自動下載軟體

資安威脅會在您不知情的狀況下，偷偷下載軟體，檢查上網費用帳單就可知道是否有異常；如果想確認是否有這樣的情況，可以設定下載限額，如此也可以避免因為資安威脅過度下載軟體而導致高額的通訊連網費用。

(五)行動裝置效能變差

資安威脅會企圖透過行動裝置讀、寫或散播資訊，因此極可能導致嚴重的效能問題；試圖想像，每天數次重新啟動資安威脅，當然會占去過多的效能，因此發現行動裝置效能變差，也可能是資安威脅已經存在的線索之一。您可藉由檢查 RAM 使用量或 CPU 負載量，得知資安威脅是否存在。

就如同電腦系統，任何有效的技術防禦措施仍須搭配可行的管理規定並落實執行，才能減少資安威脅的持續存在，甚或對外散佈與啟動。當然，任何的管理，都會帶來不便，但在資安威脅的打擾及清靜的行動裝置使用環境兩者中，相信您將選擇後者。

參考文獻

[1]Top 10 Smartphone Security Tips,
http://www.smallbusinesscomputing.com/webmaster/article.php/3931201/Top-10-Smartphone-Security-Tips.htm。

[2]FCC Smartphone Security Checker, http://www.fcc.gov/smartphone-security。

[3]智能手機資訊保安實用電子指南,
http://www.smartguard.hk/pdf/smartguardebook.pdf。

[4]NIST SP800-124 Revision-1(Draft),
http://csrc.nist.gov/publications/PubsSPs.html#800-124。

[5]Ten Steps to Smartphone Security,
http://www.fcc.gov/sites/default/files/smartphone_master_document.pdf。

[6]Smartphone Survival Guide -10 Critical Security Tips in 10 Minutes,
http://www.sileo.com/store/product/smartphone-survival-guide/。

[7]行動裝置資安防護參考指引,
技服中心網站-http://www.icst.org.tw 的共通規範項下。

[8]國安會國家安通安全辦公室，資安月會提報資料。