2012

行動安全上網學習手冊

教育部全民資安素養推廣計畫

出版日期： 101/6/20

2012.6.20

行動安全上網學習手冊

圖像來源：http://office.microsoft.com/

前言

當無線網路速度越來越快，全球都看到了無線連網時代來臨之趨勢，也有越來越多的行動裝置因應此趨勢而產生，包括早期的小型筆記型電腦 Notebook、智慧型手機、平板電腦等。這些行動裝置越來越人性化的操作介面，以及越來越豐富多元的應用服務，讓許多消費者與商務人士逐漸習慣以手機或平板電腦連上網路，並做為日常搜尋資料的主要裝置。

根據國家通訊傳播委員會的統計，至 2012 年 1 月份為止，臺灣的 3G 門號用戶數已經達到 2,102 萬戶，隨著此波智慧型手機與 3G 門號的日益普及，臺灣民眾利用手機上網的人數持續大幅成長。

根據 Google 與 Ipsos Research 調查機構在 2011 年 8 月所公布的全球智慧型手機使用調查報告，臺灣地區智慧型手機的涵蓋率已經達到 26%；這些智慧型手機的使用者，約有 20% 每天透過手機觀看影片，約 38% 每天都會透過智慧型手機到訪社交網站。

Contents

圖像來源：
http://office.microsoft.com/

臺灣的智慧型手機使用者中，平均每位用戶使用 25 個應用程式，約有 22% 使用者曾經使用智慧型手機進行網購。

國外的分析公司 BI Intelligence 曾經提出，智慧型手機之所以能夠大放異彩得歸功於 2007 年 Apple 推出的 iPhone 手機，iPhone 讓市場看到了智慧型手機可以不只是一個單純具備通訊功能、或可以收發電子郵件的商務功能手機；其在 2008 年陸續推出 App Store，給予消費者對於智慧型手機不同於以往的使用體驗，例如即時 GPS 定位與導航、拍照後立即透過上傳相片與朋友分享、玩憤怒鳥遊戲、閱讀即時更新的線上版報紙、用手機當指南針、學習其他國家的語言、甚至是教你跳韻律舞和做瑜珈！這些改變，已經讓手機、電腦與消費性電子產品間的界線越來越模糊。

數字會說話

根據調查，消費者每天花在各種媒體約 7.2 小時，其中花在手機的時間數為 117 分鐘，佔 27%。

資料來源：InMobi, Decision Fuel & On Device Research, Mobile Media Consumption Research, Feb. 2012

這些越來越聰明且功能越來越強大的手機或平板電腦裝置，其實就像是一個迷你型的電腦，所以平常我們所認識的電腦安全相關注意事項，或是日常使用電腦上網可能會碰到的電腦病毒、駭客等安全威脅，也同樣適用在手機與平板電腦等行動裝置上；更重要的是，使用無線上網或手機上網時，還有可能藏有其他額外的危險。

本學習手冊將介紹行動上網的可能危險以及因應做法，內容將涵蓋民眾無線上網最常利用的 Wi-Fi 上網的安全注意事項，包括如何安全地在公共場所使用公共無線上網服務，以及如何設定安全的家庭無線上網環境。

本學習手冊的另一個重點主題則是使用手機（特別是智慧型手機）或平板電腦可能涉及的資訊安全課題，包括實體安全的防範、個人隱私的保護，並特別針對新興的手機 APP 下載問題，提供大家判斷惡意 APP 程式的小撇步。另外，本學習手冊也將描述時下人們手機使用時間過長，甚至沉迷的現象，說明可能引發心理與身體層面的傷害，並彙整專家對於健康使用手機的建議事項。

圖像來源：http://office.microsoft.com/

主題 1. Wi-Fi 上網安全

許多民眾會在家中、咖啡店、機場、圖書館等公共場所使用 Wi-Fi 無線網路上網，但卻忽略了使用公共 Wi-Fi 無線網路若沒有注意到安全設定，可能會讓自己置身危險。

Wi-Fi 上網是一種短程的通訊方式，在一個建築空間中架設俗稱的無線基地台，而基地台的背後仍然是 ADSL 之類的有線網路，然後行動裝置即可以在一定的距離範圍內與無線基地台通訊及連網。許多民眾使用智慧型手機連網時，為了節省相對價格較高的 3G 上網通信費，也都會選擇使用 Wi-Fi 來上網。

其實無線基地台本身是可以加密通訊，也可以鎖上密碼的，不過目前臺灣許多公共場所提供的免費無線 Wi-Fi 上網服務並沒有加密或設定密碼保護，甚至許多家庭自行設定的 Wi-Fi 無線上網環境中，也沒有注意到加密的設定，讓駭客可以輕易透過未受保護的無線網路，掌握使用者在瀏覽哪些網站、收發電子郵件的內容等；技術更高明的駭客甚至可以查到使用者登錄網路服務的帳號與密碼呢！

本章將從無線上網的風險說明開始，並就設定安全的家庭無線上網環境、以及在公共場所安全使用 Wi-Fi 無線連網等兩方面，提供可操作的實作建議。

資安素養 A to Z

無線基地台

無線基地台，或稱之為無線 AP (Access Point)，主要提供無線網路登入和存取服務，也有人將無線基地台比喻為有線和無線資料的轉運站。

傳統的有線上網是透過網路線來將網路與電腦串接，若不希望被網路線所拘束，那麼在電腦端（或者智慧型手機）就必須要使用無線網卡來收發無線訊號，而網路端用來收發無線訊號的，就是無線基地台了。

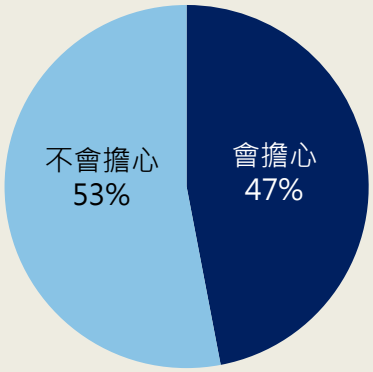
透過無線基地台，只要在其訊號涵蓋範圍內，使用者可以任意移動，以任何自己覺得舒服的姿勢與位子使用筆記型電腦、手機或平板電腦裝置，不必受網路線所拘束，隨心享受連網的樂趣。

圖像來源：http://office.microsoft.com/

數字會說話

- 是否擔心無線上網安全

無線網民擔心網路安全問題與否之比例，47% 表示「會」擔心，53% 表示「不會」擔心。



- 無線上網之網路安全擔心程度

會擔心無線網路安全的無線網民中，有超過 51%「完全不會」因擔心無線網路安全問題而影響無線上網。

完全不會	51.25%
會因擔心而部分影響無線上網	18.99%
會因擔心而儘可能少無線上網	25.95%
因為此原因，所以不無線上網	1.85%
其他	1.93%

資料來源：
臺灣網路資訊中心，『100 年度臺灣無線網路使用狀況調查報告』，2011 年 10 月 13 日

❶ 無線上網的風險

本節將說明在公共場所使用 Wi-Fi 無線上網服務的風險為何，特別因為無線網路利用空氣中的電波傳輸，對於駭客來說，要監聽或竊取此種開放式傳輸的資料更為容易，因此帶來了許多安全威脅與風險。以下歸納與說明 4 種常見無線網路犯罪及攻擊方法。

1. 使用者未經授權管控

駭客最喜歡利用不需通過密碼認證的無線網路，或是完全沒有更改出廠設定之無線 AP，並利用無線網路的資源從事包括濫發廣告信或垃圾郵件、侵犯智慧財產權（例如違法下載、拷貝或散播受著作權法保護之作品）、散布電腦病毒等違法行為，一旦違法事件被追查，背黑鍋的通常都是提供不安全的無線網路服務的無辜使用者。

2. 竊聽與資訊洩露

竊聽是指駭客針對無線網路通訊內容進行監控或監聽的行為，竊聽也可能是最簡單且最有效的攻擊方式，因為它不會留下任何線索，也不需要與 AP 有任何關聯，即使是不太懂電腦或網路技術的人，都可以從網路上輕易搜尋與下載到免費的竊聽軟體，開始針對無線通訊內容、流量或行為進行監控或分析，輕易地獲得他人的伺服器位址、通訊模式、HTTP 訪問紀錄和內容、email 帳戶資訊、無線上網的用戶名和密碼，以及在電腦中所輸入的個人資料等資訊。

圖像來源：
http://office.microsoft.com/

by devdsp (CC BY 2.0) http://www.flickr.com/photos/devdsp/

3. 偽裝與訊息竄改

偽裝是指透過欺騙認證系統，進而非法取用系統資源的行為，駭客會利用社交工程手法或網路竊聽方式騙取被害人的資訊。例如架設假的無線網路認證系統，設定偽裝的無線網路識別碼(SSID, Service Set Identifier)，騙取被害人的登入帳號密碼後，再利用所騙取的帳號、密碼登入系統。或是從網路上擷取某些通訊內容（例如使用者的帳號與密碼等資訊），重新發送認證資訊以假冒合法的使用者， 欺騙無線網路認證系統。

訊息竄改(Message Modification)則是指駭客針對監控的無線網路通訊內容進行增刪或更動，嚴重地危及資料的正確與完整性；更甚者，駭客將扮演中間人的角色，讓兩端的通訊皆通過他傳遞，並在通訊兩端毫不知情的情況下閱讀、增刪、更改傳遞的訊息。

4. 服務阻斷

阻斷服務是網路上常見的攻擊手段之一，是指利用網路系統軟體或通訊協定的漏洞，透過大量且密集的封包傳送，壓榨有限的網路系統資源，使被攻擊的網路系統無法提供服務或降低服務品質。常見的攻擊方式有 ICMP Flooding、SYN Flooding 及 Mail Bomb 等。

資安素養 A to Z

Mail Bomb（電子郵件炸彈）

一種程式碼，在執行時會向同一位址傳送大量郵件，目的是耗盡磁碟空間或使電子郵件或 Web 伺服器過載。

ICMP Flood

ICMP 是「網路控制訊息通訊協定」(Internet Control Message Protocol)的縮寫，主要用於報告 TCP/IP 訊息中的錯誤及交換受限狀態和控制資訊。而 ICMP floods 是透過向未良好設定的路由器發送廣播資訊佔用系統資源的做法。

SYN flood（洪水攻擊）

洪水攻擊是一種駭客透過向伺服端發送虛假的包以欺騙伺服器的做法，也是分散式阻斷服務攻擊 DDoS 的方式之一。具體說，就是將封包中的原 IP 位址設定為不存在或不合法的值。伺服器一旦接受到該封包便會返回接受請求包，但實際上這個封包永遠返回不到來源處的電腦。這種做法使伺服器必需開啟自己的監聽埠不斷等待，也浪費了系統資源。

資料來源：

賽門鐵克安全應變中心網站(辭彙)、i-Security 網站

圖像來源：http://office.microsoft.com/

❷ 設定安全的家庭無線上網環境

越來越多的家庭擁有多台電腦，例如爸爸和媽媽各自有自己的筆記型電腦，小孩也擁有自己的桌上型電腦，每個家庭在安裝寬頻上網後也要能夠讓多台電腦同時上網；為了方便移動、或為了不要讓線路爬滿家裡地板或牆壁的美觀考量，加上無線網路環境的設定方式越來越簡單，因此有越來越多的人在家中架設無線基地台，以建立一個可提供全家人同時共用的上網環境。

許多人為了要趕快享受在客廳沙發上悠閒地悠遊網路，或者在睡前放鬆地在床上和朋友 MSN 聊天，總是急著完成家庭無線網路架設工作。這其實是很危險的，因為無線上網環境架設雖然容易，但其安全的設定可能會稍微費時或者需要一點外力的協助，只要稍有疏忽，可能導致眾多的安全問題。以下是改善家庭無線上網安全環境的 10 個注意事項與應採取的步驟！

1. 變更預設的管理帳號與密碼

整個家庭 Wi-Fi 無線網路的核心就是無線基地台（或稱之為無線 AP），大部分的製造商都會提供一個 Web 介面讓使用者管理無線基地台，並且設有預設的管理帳號與密碼，以方便使用者進行第一次操作，然而在同型式的無線基地台上，預設的管理帳號與密碼都是一樣，若開始使用無線基地台後，沒有將這些預設的管理帳號與密碼進行變更，駭客或攻擊者很容易就可以在你不知情的情況下，利用預設管理帳號與密碼來存取你的無線基地台。

為避免這種危險，請變更無線基地台的預設使用者名稱和密碼，詳細的變更指示或步驟，可參考你所採購的無線基地台裝置所隨附的使用者手冊或操作指南。

為加強家庭 Wi-Fi 無線網路的安全，建議你不要開啟可透過無線或寬頻網路管理無線寬頻分享器的功能，僅透過用有線區域網路來進行設備的設定，比較安全。另外，也建議你設定一個不容易讓他人猜測到無線基地台的管理者密碼，覺得網路安全有疑慮時，更換該管理者密碼。

小專題：
優質密碼設定小撇步

1. 密碼長度建議 8 碼以上，且最好混合大小寫英文字母、數字及特殊符號。
2. 應儘量避免使用易猜測或公開資訊為設定，例如直接使用和帳號一模一樣的密碼、或留空白不設定密碼、或字典裡頭查得到的英文單字等。
3. 不使用過度複雜而不易記憶的密碼，以免為擔心遺忘，而必須將密碼記錄在某處（或直接存放在你的電腦中），反而提高了密碼外洩的風險。

2. 開啟無線基地台的 WEP/ WPA 加密功能

幾乎所有的 Wi-Fi 設備都支援加密的功能，透過 WEP 或 WPA 加密技術，可在無線基地台與 Wi-Fi 設備之間建立安全的訊息傳輸通道，所有傳遞的資料都會受到加密保護，以避免遭到竊聽而洩漏，為無線網路傳輸提供基本安全之防護，詳細的設定方式可參考您所採購的無線基地台裝置所隨附之使用者手冊或操作指南。

以 WEP(Wired Equivalent Privacy)加密技術為例，設定尚須由使用者設定無線網路的名稱(SSID)，然後在 WEP Key 的設定方塊中自行輸入金鑰（亦即密碼）。要特別注意的是，若你已啟用無線網路安全功能設定，卻未設定金鑰或者金鑰長度太短，無線網路安全性功能仍然不會有作用；在 WEP 設妥後，你必須在你的電腦端也設定相同的金鑰（密碼）才連線到該無線基地台，以順利地連上網路。雖然 WEP 加密存在演算法及金鑰管理的弱點，但還是能提供第一線保護機制。

WPA(Wi-Fi Protected Access)則是改變了 WEP 金鑰的生成方式，以頻繁變換金鑰來獲得安全，亦增加了訊息完整性檢查功能，防止封包偽造，安全性較 WEP 來得高；目前幾乎所有 AP 都已提供 WPA 功能，建議使用者在能使用 WPA 的情形下，應捨 WEP 改用 WPA。

3. 更改預設的 SSID 識別碼

每個無線網路都有一個「服務設定識別碼」(SSID)，任何一台電腦想要加入該無線網路時便需要使用相同的 SSID，否則將被拒之門外。

通常無線基地台的製造商都在同型式產品中設定相同的 SSID，若只使用預設的 SSID，或未設定 SSID 識別碼，任何電腦都可以使用你家中的無線網路；更改 SSID 識別碼除了可以避免附近使用同型號之無線網路基地台的鄰居意外地進入您家中的無線網路，也不會為駭客開啟一道方便之門。

資安素養 A to Z

防火牆 (Firewall)

防火牆會控制和監控所有外部和內部網路通訊，包括讓內部使用者對外取得整體的服務，而對於外來使用者則以選擇性的條件加以檢驗，只允許經授權的使用者連線使用，阻擋可能進入企業內部網路的駭客、病毒和蠕蟲。

Wi-Fi 保護存取(WPA)

WPA 是 Wi-Fi Protected Access 的縮寫，有 WPA 和 WPA2 兩個標準，是一種保護無線電腦網路安全的系統，它是因應研究者在前一代的 WEP 中找到的幾個嚴重的弱點而產生的安全機制。

服務設定識別碼(SSID)

SSID 中文為「服務設定識別碼」，是指無線網路的名稱或識別碼，它可以是任何字母（可包含大小寫字母）和數字所構成的字串，最長可輸入 32 個字元。任何連接到無線網路的裝置都要知道該網路的 SSID 為何。

資料來源：
维基百科 Wikipedia 網站、
i-Security 網站

4. 啟動網路卡實體位址(MAC address)篩選功能

每個能存取網路的設備都有個獨一無二的識別碼，稱之為 MAC 位址（Media Access Control Address, 媒體存取控制位址），例如筆記型電腦、平版電腦、手機等都有其 MAC 位址，你可以觀察你的筆記型電腦底部，有的廠商會將 MAC 位址直接貼在電腦的底端，MAC 位址大概是 6 組 2 碼的英文與數字以破折號或冒號連結的組合，像是「01-23-45-67-89-ab」等。

無線基地台會記錄所有連線的無線裝置 MAC 位址，大多數也有限制 MAC 位址存取的功能，使用者可把家中網路設備的 MAC 位址輸入允許使用清單中，設定完成後，無線基地台就僅允許使用清單內的設備連線，如此一來即可防止未知的無線設備連入家中的無線網路。

5. 取消無線基地台 SSID 廣播服務

無線基地台通常會固定一段時間對外廣播其 SSID，我們稱之為 SSID 廣播，目的是方便無線網路設備利用其 SSID 來建立連線，此功能雖然方便使用者快速找到無線基地台，但只要在無線基地台服務範圍內，所有無線網路設備都會收到 SSID。一般家庭用無線網路使用成員相對固定，建議將 SSID 廣播服務關閉，家庭成員只要在第一次連線時，以手動設定 SSID 即可。

6. 電腦不連線到未加密的 Wi-Fi 網路

你可能曾經遇到不知原因地在家就是無法無線上網，可能是 ISP 業者的線路問題，也可能是自己的電腦或數據機或無線基地台的問題，在搞不清楚如何是好時，發現自己的電腦偵測到可能是鄰居家的無線網路，因為急著想要上網，就直接連接到了這個來路不名的無線網路了。其實，連接到開放的 Wi-Fi 網路，例如免費的無線熱點或鄰居家的無線網路，會讓你的電腦安全產生風險。建議只連線到你所信任、並且已啟用加密機制的無線網路，如無可靠的無線網路服務來源，請先暫時中斷無線網路連線。

7. 為你的連網電腦設定固定 IP 位址

大多數的無線基地台都擁有 DHCP 的服務功能，可以自動分配動態 IP 位址給連線的網路設備，透過 DHCP 服務可以讓網路設備輕鬆的連線使用。然而此便利性也帶來了安全的隱憂，駭客或攻擊者很容易透過 DHCP 服務取得合法的 IP 位址。因此在家庭成員固定的家庭網路中，我們建議關閉無線基地台的 DHCP 服務，然後針對家庭中每一個連網的電腦設備分配固定的 IP 位址，並在您的無線基地台上設定允許連線的 IP 位址列表，以防止其他使用者非法入侵家庭無線網路的情形。

1. 啟動防火牆功能

目前市面上的無線基地台產品多內建有防火牆功能，防火牆能阻擋來源不明的網路連線行為，我們建議你開啟無線基地台的防火牆功能。為了提供更大的保護，也建議你考慮在每一台連網電腦設備上安裝個人防火牆軟體。

2. 將無線基地台放在適當的位置

無線基地台是靠無線電波形式進行數據的傳播，而此數據傳播都有一個有效範圍，通常家庭無線基地台信號的範圍會包含家裡的範圍，根據你自己的家庭，選擇最佳的位置，一般而言，放置在家庭最中央是最合適的。

將無線基地台擺放在家庭最中央位置或許不容易達成，但也不必過於擔心，因為小部分的信號超出家庭範圍不會造成大礙，但是當信號的範圍越強時，就要特別考量網路安全，倘若家庭無線網路設定為完全開放的情況下，駭客越容易偵測到你的無線網路訊號，那麼並且在你家附近就可以登入你的家庭無線網路。

3. 長時間不使用無線網路時，關閉整個網路服務

最佳的無線網路安全措施就是關閉你的網路，此做法可以完全阻撓駭客的入侵！雖然頻繁地關閉或開啟無線網路的做法並不實際，建議你至少考慮在旅遊或長時間不使用家庭無線網路的情況下，關閉你的無線基地台。

若你家裡的無線基地台只有用來連接有線的電腦設備，你也可以只關閉其 Wi-Fi 功能，而不必擔心整個網路會因此無法使用。

小專題：
Wi-Fi 上網的流言與真相

【流言】

有駭客爆料，在像是星巴克或麥當勞等地方所提供的免費 Wi-Fi 公共場所，只要一台 Windows7 的筆記型電腦，加上一個網路封包分析軟體，在 15 分鐘內就可以竊取利用手機上網的使用者的個人資訊、密碼，包括網路銀行的帳號與密碼、信用卡號碼等。

【真相】

無論使用筆記型電腦、平版電腦或是智慧型手機，只要透過 Wi-Fi 上網，所傳輸的資料都有可能被控制住提供 Wi-Fi 服務基地台的駭客所攔截，駭客手上的電腦也不一定是要 Windows 7 作業系統。

任何種類的資訊或資料都有可能被駭客所竊取，尤其是未經加密處理的用戶 ID 與密碼資訊。使用具加密機制的協定，駭客則無法獲取使用者的網路銀行密碼或信用卡號碼。

參考來源：

北京新浪網，用公共 Wi-Fi 上網會被盜取銀行密碼？2012/03/03

by Yutaka Tsutano (CC BY 2.0)
http://www.flickr.com/photos/ivyfield/

主題 2. 手機上網安全

根據 2012 年 2 月份由行政院研考會所公布的 2011 年「數位機會調查報告」指出，臺灣的網路人口已接近 1,500 萬人。在國內各家電信業者積極推出智慧型手機與平板電腦的優惠專案情況下，我國 12 歲以上的網路族群中，有三分之二至少擁有一種的行動上網設備；而曾經使用過筆記型電腦、手機或平板電腦行動上網的比例也從 2009 年的 4 成 2 成長至 2011 年的 7 成，其中又以 20 歲至 30 歲的年輕族群最熱中行動上網，使用率超過 8 成。不僅臺灣如此，世界各國也普遍有類似的趨勢。例如，根據 InMobi 與 comScore 兩家調查機構進行的研究，手機是許多非洲家庭唯一的螢幕裝置。

參考 InMobi 調查機構發布的 2011 年第 4 季全球行動媒體內容觀賞調查報告，「便於使用」、「易於使用」以及「具隱密性」是行動裝置使用率提高的三大因素。消費者有 27%的媒體內容收看時間是在行動裝置上進行，比例已經高於電視機(22%)，換言之，消費者利用行動裝置收看媒體內容所花的時間已經超過電視機，而超過半數的行動用戶也有透過行動裝置購物的經驗，亦有 66% 的受訪者表示其對於行動廣告、電視廣告的信任感均為相同。

案例：手機網路用量大增，原來被植入木馬

某位在公關公司工作的李小姐，因在外跑業務因此經常需要利用手機上網，李小姐所使用的是電信公司所推出每月 500M 的上網方案，幾個月使用下來發現，500M 的流量通常都用不完。

就在今年過完年後，李小姐發現，不到一個星期的時間，500M 的上網流量已全部耗盡，將手機送至維修中心檢查後才發現，自己的手機中竟然被安裝了不少的惡意程式，而自己卻渾然不知。

維修人員告知，許多木馬程式是利用手機的作業系統漏洞進行攻擊，不僅可以強制開機啟動，還會自行將手機連上網際網路，甚至竊取並對外傳送用戶手機中的各種資訊。

在本案例中，李小姐的手機流量因惡意程式而被大量消耗的同時，也已經破壞了手機系統的完整性，影響手機的正常使用。

參考資料：
新華網，黑客病毒產業鏈盯上移動終端 隱私資金受威脅，2012 年 3 月 14 日

毫無疑問地，手機已經成為許多人日常生活中不可或缺的通訊工具，加上越來越多智慧型手機與平版電腦的上市，像是 iPhone, HTC 的 Android 手機等，價格也越來越平易近人，這些行動裝置逐漸成為我們與朋友互動、聊天、傳電子郵件、使用 facebook、寫部落格、傳訊息、玩 APP 遊戲的娛樂工具。

行動裝置，特別是智慧型手機的風行，也造就了許多可能在 2~3 年前都還不曾出現過的新街頭景象，例如在公車站、捷運車廂、餐廳、咖啡店、甚至是人行道上，我們常常可以看到所謂的「低頭族」或「打卡族」，不是低頭在打電動玩具，就是利用 APP 在和朋友聊天，或者在餐廳服務生將餐點送上桌時，立刻用手機拍照再上傳到臉書上打卡或與朋友分享。

有關手機安全上網的章節中，將分為 5 個主題來提醒民眾使用手機以及透過手機上網的安全注意事項，內容包括：

❶ 手機實體安全防範
❷ APP 使用風險與安全建議
❸ 享受社群網路服務同時保護個人資料
❹ 預防手機使用過度（沉迷）
❺ 給家中有青少年低頭族父母的建議

❶ 手機實體安全防範

過去，我們的手機裡儲存的個人資料可能只有通訊錄內親朋好友的手機號碼，隨著手機的照相功能越來愈強大，手機內開始出現大家隨手拍的照片或影片等比較屬於個人私密的內容。近期因為智慧型手機的推出與風行，加上 3G、Wi-Fi 行動上網的普及，也讓越來越多的消費者開始利用手機登入自己或公司的電子郵件、在 Facebook 上與朋友互動、上傳 YouTube 影片，或直接在手機上進行線上購物、買票、銀行轉帳交易，甚至現在手機還可以當作是進出高鐵閘門的票券！

正因為現今智慧型手機中所包含的資料已經與過去大不相同，除了基本的通訊錄與照片外，上述各種網路服務的帳號與密碼，也都會儲存在手機中，一旦手機遺失，也代表這些個人帳號、密碼、交易資料，都有洩漏的可能。

手機遺失可以再買，但若是其中的私人照片、簡訊、各式帳號與密碼遭有心人士盜用，可能造成比手機本身更大的損失！本節將說明如何運用手機所提供的保全功能，透過保護手機的實體安全來降低他人未經同意而使用你的手機撥打電話或上網之風險。

最基本應該注意的手機實體安全事項為，避免將您的手機留在車上或沒有人看管的地方，例如在餐廳用餐時直接放在桌上而前往洗手間等。另一個基本注意事項，同時也是大家都容易忽略的為，在購買新手機時，要仔細閱讀手機的使用者手冊，特別是瞭解該手機所提供的安全功能有哪些，並瞭解如何啟動這些安全功能。以下提供 3 個基本的手機實體安全小撇步。

小撇步 1. 設定手機密碼保護手機

手機密碼是指當開機時須輸入的密碼，此密碼是對手機本身的鎖定，輸入後手機才能夠使用，一般手機的預設密碼值是 1234 或 0000，建議使用者必須更改為自己的密碼。

小撇步 2. 使用 PIN 碼保護手機 SIM 卡

PIN 碼可保護你的手機 SIM 卡，避免他人未經同意使用你的手機撥打電話。當你第一次將 SIM 卡插入手機並開機時，系統會要求你輸入 PIN 碼。 PIN 碼的長度為 4 到 8 位數字，此 PIN 碼也通常會隨著你手機業者所提供給你的 SIM 卡一起提供， 建議你將電信公司提供預設 PIN 碼變更為自己的密碼。設定後，你每次打開手機電源時，系統便會提示你輸入 SIM 卡的 PIN 碼。

當不正確的 PIN 碼輸入太多次（通常為 3 次），為防止他人未經同意利用你的 SIM 卡撥打電話，你的電信服務業者會封鎖 SIM 卡，讓 SIM 卡無法繼續正常使用。若只是不小心忘記 PIN 碼而造成 SIM 卡被封鎖時，必須連絡電信業者以取得 PIN 解鎖碼 (PUK)。如果輸入不正確的 PUK 碼太多次，則 SIM 卡將會永久封鎖，而你便需要向電信服務業者取得新的 SIM 卡。

by renaissancechambara (CC BY 2.0)
http://www.flickr.com/photos/renaissancechambara/

小撇步 3. 記下你的手機唯一識別碼 (IMEI)

每一個手機都有一個獨立的手機序號列，稱之為 IMEI 碼，相當於行動電話的身分證號碼。IMEI 碼是一組 15 位數字，這組數字會標示在包裝硬盒外側，或貼在機身背面(通常在電池下方)，同時也存在於手機記憶體中，通常可以在手機上輸入 *#06# 後即可以查詢自己手機的 IMEI 碼。

請記下你的手機 IMEI 碼，當你的手機被偷或遺失時，這組號碼是電信公司向警察單位查詢尋獲手機或贓機的辨識號碼，通常在失竊手機報案時，警察也會詢問你的 IMEI 碼。

小撇步 3. 保護手機內儲存資訊的安全

功能強大的智慧型手機，儼然就是一部迷你電腦，以往只被拿來作為撥打電話的行動電話，如今已衍生出上網、拍照、聽音樂、查地圖、定位資訊服務等多重功能，而使用者儲存在手機中的資料與資訊，已經遠超過以往的通訊錄、簡單行事曆、或隨手拍的低解析度照片而已，因此保護手機內儲存資訊的安全也顯得越來越重要。

以下歸納 4 個保護手機內儲存資訊的安全實行重點。

- 將手機內的資訊進行加密

  某些手機會提供將資訊加密並且儲存在手機記憶卡內的功能，若手機沒有提供，也有一些安全軟體開發商提供加密工具或加密 APP 的服務。將手機內的資訊加密可確保當你的手機遺失或遭竊時，拾獲者無法輕易地從手機中取得你的隱私資訊。

  不過，非常隱私的照片、影片或機密文件，也建議不要存放在手機裡頭!!

- 絕對不把密碼儲存在手機中

  許多人為了方便或擔心忘記，會把密碼（尤其是不常使用的密碼）儲存在手機中，也有許多人喜歡利用手機的電話簿功能，直接將密碼或 PIN 碼儲存成為一組電話號碼（當然這組電話號碼是撥不通的）。在你的電話遭竊或遺失時，這樣的做法是很危險的！

  因為惡意人士多瞭解這樣的技巧，會嘗試著從中猜測出你的重要服務的密碼。

圖像來源：http://office.microsoft.com/

- 定期備份手機內的重要資訊

  大部分的智慧型手機會支援手機與你的電腦同步資訊的功能，你可以設定好每一次手機與電腦進行同步的同時，也將你的手機資訊備份至電腦中。或者，你可以直接用手機的備份服務或工具，將資訊定期備份到記憶卡中，並將該備份記憶卡放置在安全的地方。

- 避免在擁擠公共場合以手機進行與財務有關的線上服務

  大家可能都有這樣的經驗，在擁擠的公車或捷運車廂裡，甚至是電梯內，可以清楚地看到左右或前方位置的人正在輸入的手機簡訊內容，或看得到對方正在瀏覽哪些網站。

  建議你避免在擁擠的公共場所以手機進行線上交易，例如輸入信用卡號結帳，或者輸入自己的網路銀行帳號與密碼，智慧型手機的螢幕普遍都比較大，視角也較廣，且密碼輸入在手機畫面時，明碼也會先顯示出來後才會轉變成我們平日在電腦中所熟悉的「*」符號。這些重要的財務資訊，很容易被身邊路過者所窺視，若對方心懷不軌，你的重要資訊也可能因此被竊取與盜用。

by Cristiano Betta (CC BY 2.0)
http://www.flickr.com/photos/cristiano_betta/

❷ APP 使用風險與安全建議

智慧型手機、平板電腦等行動設備其實也是一種電腦，有處理器、記憶體與儲存空間，可以安裝各種軟體，能夠上網、玩遊戲和瀏覽影音等，因此也像一般電腦一樣可能存在惡意程式竊取你的資料，或偷偷執行其他動作。

今(2012)年的 4 月 16 日，網路資訊安全公司 Sophos 揭露了一則有關智慧型手機界最流行的 APP 遊戲 – 「憤怒鳥太空版」可能藏有電腦病毒的消息，根據 Sophos 的說明，該款最新遊戲 APP 被發現內藏木馬程式，若 Android 手機使用者曾經從中國的網站下載安裝這款遊戲 APP，遊戲雖可正常運作，但手機會完全被駭客操縱，使用者在手機中所輸入的各項帳號或隱私資訊，駭客皆可一覽無遺。

過去也曾發現一款偽裝成遊戲的 APP，使用者安裝後每隔 15 分鐘，該 APP 會自動向 APP 開發者的伺服器回報該用戶的位置資訊，即使結束遊戲畫面，也會在背景下動作，持續傳輸。還有一種惡意軟體一旦安裝並啟動後，會在使用者不知不覺中向付費的內容服務商傳送簡訊，而使用者也因此必須負擔昂貴的簡訊傳輸費用。

手機 APP

常常聽到的 APP 其實是英文應用程式 application 的縮寫。

APP 是由軟體開發者針對智慧型手機及平板電腦所開發與設計，它會透過專屬的應用程式平台讓使用者進行下載，這些專屬的應用程式平台通常是由手機的作業系統廠商所提供，例如蘋果的 Apple APP Store、谷歌的 Google Play、黑莓機的 BlackBerry App World、及微軟 Windows Phone Marketplace 等。

這些免費或收費的 APP 會下載至特定的行動裝置上使用，最常見的有 iPhone, iPad, Android 手機、黑莓機等。而 APP 的類型也越來越多樣化，從早期的電子郵件、行事曆，演變到現在以遊戲類型的 APP 最受到歡迎。

資料來源： Wikipedia

使用智慧型手機下載 APP 時，APP 的交易平台會明確地告知使用者有關即將下載的 APP 會使用到的手機系統各項權限（不適用 iPhone），例如授權該 APP 可以取得你的手機號碼、可以幫你發簡訊、可以讀取甚至編輯你手機中所有聯絡人的資訊等。若使用者不同意授予 APP 所要求的權限，就不能夠安裝該 APP，這也是最基本的手機程式下載防護措施。

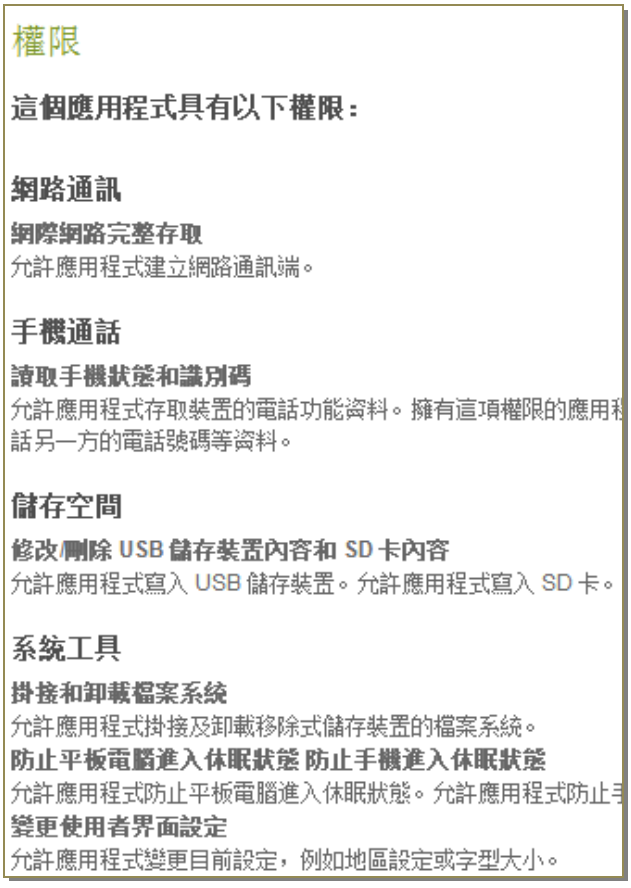
不過，不同的手機作業系統針對系統授權的說明有異，例如在 Google Play 平台下載 APP 之前會提醒使用者該 APP 會取得的各項系統權限，並取得使用者的同意；但是在 Apple 的 APP Store 下載程式時，便少了使用者同意的步驟，亦沒有授權條款的說明。

這是因為 Google 對 Android 市集是採取開放態度，不需要經過審核，程式開發者便可以將應用軟體放上 Android 市集上提供使用者下載，據 Android 程式開發者表示，Android 是採使用者審核，品質不良的程式，自然被評分機制所淘汰；也因此 Android 的 APP 市集中存有較多的惡意軟體。

雖然 Android 的 APP 市集提供使用者授權與否之權利，但問題是，許多的惡意 APP 會想盡辦法引誘使用者按下同意按鈕，最常見的惡意引誘方式，就是盜用知名動漫圖片、遊戲或色情圖片來引誘下載，例如，在 Android 的 APP 市集上就有多款山寨版憤怒鳥 (Angry Birds)。

相對於 Google 的 APP 開發管理方式，Apple 則是採用封閉的管理，所有軟體都必須透過審核才能上架。儘管 Apple 具有審核流程，在去(2011)年底，英國 BBC 報導仍指出，資安專家 Charlie Miller 為 iPhone 及 iPad 設計了一個藏有惡意程式的軟體，企圖測試 Apple 的 APP store 的安全程度。

結果證明，該偽裝成追蹤股價程式的惡意程式，成功地通過了審查並在 App Store 上架；一旦使用者安裝該程式後會開啟遠端遙控介面，可以在受害者不知情狀況下讀取聯絡人資料與執行其他操作。因此，Apple 的使用者仍必須有所警覺，不能完全信任 App Store 所下載的任何軟體都是安全的。



圖像來源：Google Play

電腦病毒與手機病毒的五個共通點

根據防毒軟體公司 Trend Labs 趨勢科技全球技術支援與研發中心的歸納，電腦病毒與手機病毒的五個共通點簡述如下：

1) 都可能讓受害者收到意外的帳單

例如，惡意程式會讓你的手機撥打昂貴的付費服務或長途電話、未經你的同意下幫你訂閱高價的服務等。

2) 都可能以木馬程式出現

在行動裝置上已發現越來越多偽裝成各種實用手機應用程式的木馬程式，這些木馬程式會暗中側錄並傳輸你的資料至外部。

3) 電腦與手機交互感染

跨不同裝置的病毒威脅已經出現，病毒可能會從個人電腦擴散到行動裝置，再回到個人電腦。

4) 都可能會使用網路釣魚伎倆

許多智慧型手機使用者會透過手機收發電子郵件，也因此，透過電子郵件型式的網路釣魚（Phishing）以及詐騙問題，同時會發生在個人電腦與手機上。

5) 都會鑽漏洞

鑽漏洞式的病毒攻擊，都是傳統個人電腦上曾出現的威脅，加上手機的螢幕尺寸限制，無法透過功能完善的工具來查看裝置背後執行的應用程式，使得手機或平板電腦使用者更難察覺自己可能遭到攻擊。

手機病毒的危害

1) 導致使用者資訊遭竊。

越來越多的手機使用者將個人資訊儲存在手機上，這些資料也引起駭客透過編寫各種病毒入侵手機的方式來進行竊取，再使用於詐騙或冒用身分等不法行為。

2) 傳播非法訊息

就如同一般個人電腦中毒可能造成的危害，一旦你的手機中毒或被植入惡意程式，駭客會以你的名義，透過你的手機簡訊或電子郵件等管道，大量對外散布色情、非法圖片、電影等資訊或垃圾郵件。

有名的案例是 2010 年 12 月中時報導有關在中國出現的一個稱為「惡靈古堡」的簡訊病毒，一旦手機感染該病毒，駭客便可以透過該手機大量發送廣告或垃圾簡訊給其他人，導致受害者的手機帳單在不知不覺中出現大量簡訊費用。現在已有好幾百種手機病毒出現了。

3) 使手機無法運作

這是最常見的手機病毒危害，病毒或惡意程式會破壞手機的軟、硬體或系統，導致手機無法正常運作。

手機 APP 下載使用安全建議

根據防毒軟體業者 McAfee 的 2012 威脅預測報告指出，過去兩年來已經發現越來越多的智慧型手機或其它行動裝置的攻擊事件，攻擊手法已從相對簡單的破壞性惡意程式，演進到騙取錢財的惡意程式或間諜軟體。這些惡意程式會利用系統漏洞進行攻擊，也因此取得對智慧型手機更大的操作力量。McAfee 也預測到了 2012 年，這些攻擊者不會停手而且會持續加強其攻擊，而手機使用網路銀行的攻擊事件可能會越來越多。

透過以上的章節我們瞭解到手機 APP 的使用可能風險有哪些，本手冊接下來將提供手機 APP 下載使用安全建議或注意事項，以提醒民眾，在享受著有趣的手機遊戲或使用各種實用的 APP 程式時，應隨時提高警覺，不要因為一時的疏忽，造成難以彌補的傷害。

手機 APP 下載須瞭解事項

1) **手機個人資訊範圍不只是你的資料而已**

   若下載安裝了不安全的手機應用程式，你必須瞭解你可能會面對到個人資訊揭露的風險，而這些屬於你的個人資訊會包括你的所在地理位置、聯絡人資訊、行事曆資料、儲存在手機中的簡訊等。

2) **你是擁有授權與否的決定者**

   使用 Android 作業平台的智慧型手機時，在你安裝 APP 的當下，會詢問你是否允許該 APP 存取哪些手機中的個人資訊（例如聯絡人、行事曆等），或允許使用哪些手機系統功能（例如允許使用照相設備、允許更改 Wi-Fi 連線狀態等），因此你是擁有授權與否的決定者。

   英國 Sunday Times 曾報導，包括臉書、雅虎、Flickr、Badoo 等業者均承認，其 Android APP 會讀取使用者的簡訊內容。而部分 iPhone APP 開發業者也會在未告知使用者前提下，直接從手機通訊錄取得你的聯絡名單。

3) **再三考量哪些資料適合放在手機中**

   你的智慧型手機中可能存放著大量的個人資訊，這也會讓取得你的手機或有機會監控你的手機活動的惡意人士更容易進行詐騙。你必須再三考量哪些資料適合出現在手機中，這些資訊若落入他人手中時，是否有可能對你或你週遭的人產生影響？

   例如你曾透過手機進行網路銀行業務或下載一份銀行的對帳單，相關的金融資料可能會留存在手機中；或者你的聯絡簿中可能會記載了所有親朋好友的真實姓名、所屬單位、辦公室或家庭聯絡電話與地址、個人或公用電子郵件等詳細聯絡資訊等。

手機 APP 安全使用注意事項

1) **注意警告標語**

需特別注意會詢問你是否允許某個軟體安裝到你手機的警告標語，如果你不清楚該軟體是什麼內容，就不要安裝，因為犯罪者會試圖欺騙用戶下載惡意程式。

2) **只在信譽良好的網站中下載 APP**

只在信譽良好的網站中下載 APP，或儘量避免透過手機的瀏覽器下載 APP 程式，因為從未知或不可靠的來源下載的程式有可能就是惡意程式。建議只在像是 Apple APP Store 或 Google Play Store 等作業系統業者所提供的 APP 交易平台下載。

3) **關閉手機的 GPS 功能**

不使用定位服務(GPS)時，請關閉手機的 GPS 功能。雖然 GPS 提供了尋找地點的便利功能，但它也可以被他人利用來監控你或者是你的手機的確切位置，這可能有個人隱私曝光的疑慮。

4) **關閉藍芽(Bluetooth)功能**

當你不使用手機藍芽服務時，請關閉該功能，以確保你的手機不會被其他的行動裝置透過藍芽進行連線，換言之，駭客也無法透過藍芽連接你的手機。當使用藍芽連線功能時，應儘量避免在人潮多的地點使用。

5) **使用完服務後登出會員**

利用手機瀏覽某個網站服務結束後，記得進行會員登出(Log out)。許多人為了方便或節省時間，會勾選允許手機瀏覽器記住你在某個網站的帳號與密碼，建議你最好能夠避免勾選此功能，因為一旦你的手機遺失或遭竊時，他人也能輕易地以你的身分登入你的網路服務。

6) **點選超連結之前請三思**

透過手機收到含有超連結的訊息，可能是來自於他人傳來的簡訊、多媒體訊息，或者是現在很流行的手機傳訊息或聊天 APP，例如 Line、WhatsApp 或 skype 等。點選超連結之前請三思，特別是當這些訊息來自於你完全不認識的電話號碼或傳訊來源時，一定不要點選訊息中所包含的超連結，因為這些超連結可能會暗藏間諜軟體或病毒，或引導你前往惡意網站。

7) **安裝手機防毒軟體**

手機也可以像電腦一樣安裝防毒軟體，當你透過安裝 APP 時，它會自動掃描檔案的安全性，避免惡意軟體竄入手機。

小專題：手機受病毒感染的癥狀

當你發現以下癥狀時，你的手機可能已經遭到惡意程式或病毒的感染了！

- 電話帳單金額沒有任何理由地暴增。
- 手機簡訊與電子郵件信箱的寄件備份中，出現你不曾寄出過的訊息或電子郵件。
- 手機使用介面（如桌布、主題、手機桌面的擺設方式）突然自行改變。

8) **每次少量的 APP 下載**

許多剛使用智慧型手機的使用者，會因為一切都很新奇，而一次下載大量的 APP。但在手機相關使用及性能尚未熟悉的狀況下，容易造成使用上的不穩定，萬一下載到惡意軟體也較難發覺，故建議下載 APP 時，宜少量下載並先使用過後，保留適當的觀察時間來確認 APP 的執行狀態、手機連網的速度變化、電池是否突然大量消耗等現象。若不小心下載到惡意程式時，也可以較快的速度找出問題點在哪裡，並加以處理與解決。

9) **留意孩童玩手機 APP 遊戲**

據 TVBS 報導，2010 年 8 月曾發生節目主持人下載 iPhone 遊戲軟體給他 7 歲的小孩玩，結果小孩玩了十多分鐘後，家長便接到信用卡公司簡訊，通知她已經刷了數百歐元，後來才知道小朋友玩遊戲時用 iPhone 買了 6,000 多元的虛擬珍珠！

若你將自己的手機或平板電腦交給孩子玩遊戲時，請瞭解孩子在玩的遊戲內容是否涉及進一步需要付費的服務，也要儘量避免把 APP 下載的密碼提供給孩童自行使用，因為有些免費遊戲有付費升級或購買遊戲金幣等額外付費的設計，即使有相關的訊息提醒消費者，也可能因為小孩不懂英文，或是一不注意就輸入密碼，使得家長因此收到奇怪的簡訊或大筆金額的電話或信用卡帳單。

小專題：
給孩童的手機安全使用建議

手機可以用來打電話、傳簡訊、傳照片，是和同學及朋友連繫與互動很棒的工具，不過就像是上網要注意安全一樣，手機使用上也有一些注意事項喔！

- 隨時把手機帶在身邊，因為手機體積很小，很容易遺失或被偷；
- 只能夠把自己的手機號碼告訴你的朋友還有你信任的人；
- 不要把手機借給你不認識或不信任的人，或者把手機留在其他人很容易拿走的地方。
- 設定你的手機密碼，大部分的手機都可以設定開機密碼，只要是不知道密碼的人拿到你的手機，他們是沒有辦法開鎖和使用你的電話號碼的；
- 要是有人一直逼你要告訴他你的手機號碼，一定要把這件事情告訴你的爸爸媽媽或老師，請求他們的協助；
- 如果你的手機有藍芽功能，沒有在使用的時候，請一定要關閉藍芽。

小專題：如何判別手機惡意程式?

以下提供 3 個可做為判別是否應該要下載某個 APP 程式的簡單小撇步，不過這些都只是初步過濾可能藏有惡意程式的參考建議而已，平日多注意相關的病毒新聞或訊息，也一樣重要喔！

- 注意該 APP 的星級評價

在 APP 交易平台中，每一個 APP 都有自己的星級（如下圖）。

圖像來源：Apple APP Store
製圖： NII 產業發展協進會

星級可以讓我們了解其他的下載使用者對於該 APP 好壞的評價，若大家給的評等都很低（例如 1-2 顆星），可能代表這個 APP 不好用，但是 4 或 5 顆星的 APP 也不一定都是沒問題的，應該要注意給評價的人數，若只有 10 個人說這個 APP 有 5 顆星，參考價值可能就不高，若上千個人都給予高評價，那麼就可以考慮下載。

- 觀察使用者對該 APP 之評論

除了星級之外，還可以透過觀察其他使用者對該 APP 的評論內容來查探一下有沒有其他人被該 APP 欺騙過。在 APP 交易平台的下載頁面中就能找到其他已經下載過該 APP 的使用者評論，如果你看到評論中已有受害者的控訴言論，那麼就不要冒險下載這個 APP 囉！

圖像來源：Apple APP Store
製圖： NII 產業發展協進會

- 查看該 APP 的存取權限設定

作業平台為 Android 的手機使用者在下載 APP 前，手機的頁面上都會告訴你這個 APP 會存取手機的哪些權限，請仔細閱讀，不要為了趕快玩 APP 遊戲而一直按下一步。如果你只是要下載一個手電筒照明功能的 APP，但這個 APP 卻要求要有 GPS 定位的權限，這時候你就要注意這個 APP 是否有其他的意圖，而不要輕易下載喔！

by Jorge Quinteros (CC BY-NC-ND 2.0)
http://www.flickr.com/photos/jorgeq82/

❸ 享受社群網路服務同時保護個人資料

根據尼爾森在 2011 年第三季針對美國手機 APP 下載的調查中發現，手機使用者對於社群網路類別的 APP 下載率高達 54%，而無論是何種手機作業系統平台（如黑莓機、iPhone 或 Android），手機版的 Facebook APP 下載皆排名第一。再檢視國內的智慧型手機使用者的習慣，依經濟部工業局的「2011 臺灣智慧型裝置持有與服務使用行為」調查報告，臺灣消費者使用智慧型手機行為以社群、拍照及定位為三大關鍵應用。

隨著社群網路滲透率提高，智慧型手機夾帶的 3G 行動上網優勢，降低了使用者對於社群網路服務的使用時間及地點上的限制，使得利用智慧型手機或平板電腦使用社群網路成為趨勢。利用行動裝置玩社群網路固然有趣，但在這背後也藏有許多經常被忽略的風險，本節主要將提醒使用者，在缺乏充分的資安認知情況下用手機玩社群網路服務，很容易讓自己或親朋好友的重要資訊及隱私被竊取或曝光喔！

小專題：利用手機與朋友互動

Twittter、噗浪、臉書、無名小站等社群網路服務在國內外已經流行了一陣子，這些社群網路服務提供我們與朋友更多的連結與互動機會，當智慧型手機開始流行後，這些社群網路服務也開始移轉到手機平台，讓我們與朋友們可以隨時隨地，甚至 24 小時地串連在一起，分享生活中的大小事。

我們通常可透過以下三種方式，來利用智慧型手機玩社群網路服務：

- 下載手機版本的 APP，再透過 APP 來使用服務
- 透過手機瀏覽器直接連線到社群網路的網站
- 將你的照片或是你欲上傳的文字、資訊寄送到特定的電子郵件（通常會由社群網路服務業者指定）

資料來源： LG Electronics

手機社群網路服務應用的特性

歐洲資安推廣組織 ENISA (European Network Information Security Agency) 曾評論，使用者在行動或移動過程中也要能夠使用到社群網路服務的需求增加，是社群網路應用很自然的發展；這是因為消費者本來就習慣透過打手機或傳簡訊等方式與親朋好友溝通及互動。對廣大的消費者而言，利用手機使用社群網路服務不但不會改變其原有的習慣，反而還會讓消費者體驗到更豐富和有趣的溝通經驗。

不像個人電腦，我們得固定在特定的地方才能使用，幾乎每個人都將手機隨時帶在身邊，也因此，消費者更可即時地、經常地與朋友、同儕或親人傳達最新的現況資訊，包括自己身在何處、正在做些什麼事情、有哪些新鮮事、正讀到哪一則有趣的新聞等，透過手機上傳資料或照片到自己的社群網路頁面上，也只需要幾個簡單步驟，這也是讓手機社群網路應用普遍受到歡迎的原因之一。

下列圖片歸納了五個主要的手機社群網路服務特性。

參考資料：ENISA

手機社群網路服務應用的風險

每一位社群網路使用者都應該瞭解相對應的使用風險有哪些，常見的風險包括了隱私權、身分遭竊取、惡意程式、使用者的地理位置追蹤等四種類型。

風險 1. 隱私權課題

無論你使用的是手機或一般個人電腦，只要是使用社群網路服務，都可能涉及隱私權遭到侵害的風險，而這些隱私權侵害的問題可能來自三種來源，其一是來自於第三方、其二為其他社群網路使用者、其三為社群服務網站本身。

第三方可以透過你填寫在社群服務網站上的個人資料頁面，或者單純地撿到你的手機就可以取得你的相關個人資訊。第三方取得隱私資料的原因不一定是與技術入侵或駭客有關連，大多數的情況是使用者自己本身在這些社群網站上的隱私權設定不夠周延的結果。正派經營或具規模的社群網站都會提供使用者自行設定哪些個人資料可以公開、公開給誰等功能。

其他社群網路使用者不小心洩漏你的個人隱私的情況也不少，例如，朋友在自己的社群網站頁面上寫下與你有關的事項，或者在未經你的同意之下在上傳的照片中 tag 你的名字。也因此，慎選你在社群網站上的朋友是很重要的，許多人對於社群網站中的朋友邀請，無論和對方熟不熟悉，甚至對於陌生人，都來者不拒。此做法存在的最大的風險即是，你在社群網站上與至親好友所分享的生活點滴、照片或影片，都有可能被陌生人看到，或甚至轉寄出去，造成不必要的隱私揭露。

雖然使用者可以透過隱私權設定方式來決定哪些人可以看到自己的資訊，然而對於**社群服務網站業者**而言，他們可以取得所有的個人資訊，甚至是網站使用所衍生的其他軌跡資料，例如你連網的 IP 位址等。有些你放在自己的社群網站頁面上的資訊，還會被搜尋引擎給搜尋出來呢！

圖像來源：http://office.microsoft.com/

風險 2. 身分遭竊取

身分遭竊取是手機社群網路服務應用的風險之一，有心人士可能透過惡意攻擊程式或以偷取手機等方式，或者只是拾獲你遺失的手機，便可輕易地取得並取代你在手機中的身分。當有心人士取得你的手機或你的帳號的掌控權，其可能會更改你的社群網站密碼與註冊的電子郵件，並以你的名義在你的社群網站頁面上散播惡意程式連結，或以你的名字刊出不當言論，你的朋友可能因為對於你所刊登的超連結不疑有他，點選後手機即會自動下載惡意程式。

據 ETtoday 報導，今年 4 月國內也發生一名年輕女子將自己的手機送至手機業者門市店包膜，沒想到手機裡穿著薄紗的清涼照片，竟被包膜師以該名女子的帳號上傳到臉書。該名女子的友人看到照片後，不是驚訝就是留言消遣，造成女子莫大困擾。

風險 3. 惡意程式

因為社群網路服務允許各個使用者相關串連與交換訊息，因此也建構了理想的惡意程式散布的平台，特別是針對手機所設計的惡意程式可能會竊取儲存在手機中的各種資訊，而不只是與社群網路服務有關的資訊而已；此外此類惡意程式還會透過你的手機上的連絡人清單，以你的名義利用簡訊或電子郵件等方式大量傳播惡意程式。

風險 4. 使用者的位置追蹤

許多智慧型手機內建了手機裝置位置的追蹤功能，這代表手機的持有者本身也會一起被追蹤，有些業者會將此地理位置追蹤的功能運用在其手機社群網路服務中，提供用戶更有趣好玩的互動服務，例如即時公開自己的所在位置、知道朋友目前所在位置等。若使用者在社群網站上的隱私設定不當，等同是向全世界宣告你當下在何處，但是對有心人士而言，卻可能是綁架、跟蹤、攻擊或闖空門的機會。

據 TVBS 報導，去年底已破案在台中發生的大學生遭綁架勒贖事件，歹徒就是利用被害者在臉書上所公開與打卡的資訊，確定被害者為工廠小開以及每日上班時間，因此鎖定目標與下手時間進行綁架勒贖。

案例：臉書帳號被盜用，信用卡遭盜刷

臺東一名男子玩臉書開心農場遊戲曾經利用信用卡購買農民幣數次，今年 2 月份在瀏覽臉書朋友的塗鴉牆時，不小心點選了一則不明的超連結，隔日就遭駭客入侵竊取臉書帳號，冒名盜刷信用卡購買兩筆農民幣計 1 萬 5 千餘元。

提醒臉書使用者，若發現自己的塗鴉牆或朋友的塗鴉牆與留言中，有不明的網址超連結，千萬不要點選觀看，以免誤觸惡意程式造成帳號被盜用的後果。另外也建議可向發卡銀行申請簡訊通知刷卡服務，一旦收到異常通知，才能夠立即辦理止付停卡，確保自身權益。

參考資料：
自由時報，
臉書帳號遇「駭」遭盜刷，
2012/04/16

手機的社群網路應用個資保護小撇步

小撇步 1. 只接受你認識的朋友邀請

盲目接受來自任何人的朋友邀請是非常危險的，接受邀請之前應確認對方為自己所認識且可信任的朋友，若發現已經加入成為朋友者有問題，也可以透過從朋友清單移除方式，與對方切斷關係。

小撇步 2. 謹慎思考要張貼哪些資訊

在社群網站中張貼越多有關自己的資訊，包括文字、照片、影片、對他人留言的意見等，你公開在網路上的資訊就會多，尤其是手機提供了更為即時的狀態更新管道，許多使用者都會忍不住多分享了一些。

許多人也會將自己的全名、email、電話、手機、生日、寵物名字、爸媽或伴侶的名字、婚姻狀況等私密資料全部公開，請務必謹慎思考要張貼哪些資訊在你的社群網站中，儘量避免提供過多的個人資料細節，以免遭到詐騙集團或有心人士的利用。

小撇步 3. 幫朋友打卡與 Tag 前，先取得同意

用手機上網「打卡」可以即時秀出自己的所在位置，並能夠看到附近的親朋好友，馬上相約碰面。不過有些人在打卡或上傳照片的時候，喜歡將身旁朋友也一起標示在訊息中，特別是 facebook 的 tag 功能，可以讓使用者將發布的訊息、相片、影片、網誌同步在朋友的塗鴉牆上，達到擴散的效果。

若未取得身旁朋友的同意就標示上的話，很可能會讓朋友的隱私也受到侵害，例如朋友不願意讓其他人知道他的行蹤等，從尊重他人隱私的角度，建議幫朋友打卡與 Tag 之前，應該先取得對方同意後再進行。

若很難掌握朋友幫你進行 Tag 的標示行為，也建議你在自己的隱私設定中，「勾選」標籤審查，可先行查看朋友在你發布的內容所貼上的標籤，再決定是否可以出現在 Facebook 上。

畫面來源：Facebook

小撇步 4. 定期檢視你的隱私權設定

部分社群網站預設的使用者隱私權設定為公開讓所有人看得到你的個人資料，但是大多數的網站都允許使用者可以進一步做調整與客制化其隱私權設定，建議使用者一定要調整自己的隱私權設定值，最小化可以取得你個人資料的人數。

此外，一些社群網站也會不定期地修正其隱私權聲明或隱私權設定方法，例如為了讓網站的某個新功能得以運作，必須降低使用者的安全設定，本手冊也建議你定期檢視自己的隱私權設定是否仍符合自己的安全需求。

按下臉書頁面右上角「首頁」右方的向下箭頭標誌，可開啟有關隱私設定之畫面，如下圖，使用者可依需求，進行貼文、應用程式更新、個人檔案等內容可與哪些人分享之隱私設定。

Facebook 隱私權設定畫面，畫面來源：Facebook.com

按下噗浪個人頁面右上方「我的帳號」按鈕，即可於「我的帳號」視窗中的「隱私權政策」功能下設定您的時間軸公開對象，以及哪些人可在噗浪上搜尋到您。

噗浪隱私權政策設定畫面，畫面來源：plurk.com (製圖：NII 產業發展協進會)

按下 Google+右上角自己的大頭照右方向下箭頭標誌(如下圖)，可開啟隱私設定之畫面，使用者可依需求，進行自己社交圈的管理與訊息與哪些人分享之隱私設定。

Google+ 隱私權設定之畫面，畫面來源：google.com（製圖：NII 產業發展協進會）

By brunotto (CC BY-NC-ND 2.0)
http://www.flickr.com/photos/brunauto/

❹ 預防手機使用過度

赫爾辛基資訊科技研究院（Helsinki Institute for Information Technology）和英特爾實驗室的研究發現，重度使用智慧型手機的人，可能每 10 分鐘就要確認一次手機，一天確認次數高達 34 次。也有醫師擔心，過度使用智慧型手機不只讓人容易脫離現實，當遠離智慧型手機，甚至可能引起焦慮、失眠、憂鬱等症狀；本段落將說明過度使用手機上網可能引發心理與身體層面的傷害，並彙整專家在健康使用手機方面的建議事項。

低頭族崛起

最近出現一個新名詞「低頭族」，指的是到處可見「低頭」使用智慧型手機或平板電腦的族群。最常看到低頭族的地方有公車站、火車站、捷運車廂、餐廳、咖啡店、電梯裡、甚至是名勝古蹟的重要地標前，或許是通勤時間無聊打發時間，就低頭看著智慧型手機玩遊戲、傳簡訊、用 APP 聊天等；或許是要與朋友分享自己的最新狀態，例如在臉書上打卡；又或者是要為朋友按個讚或是回應朋友的近況消息等。

不只是臺灣有低頭族，國外也是，前陣子 YouTube 上流行一段影片，一位加拿大的妙齡女子從辦公大樓走出來，一邊走路一邊低頭傳簡訊，一不留神竟踩空從階梯上摔下來，當眾「仆街」，女子的窘態不但被全程直播，還被許多網友不停地轉載分享，才幾天的時間就已經累積超過 75 萬人次點閱。邊玩手機邊走路看似容易，但其實很危險，行人除了會因為使用手機造成走路速度變慢之外，人的大腦也會因為無法接收足夠的訊息，即使頻頻抬頭看路，也無法精準判斷路上的階梯和斜坡，導致行走錯誤。

情況嚴重的低頭族也可能是過度使用手機或網路、甚至屬於成癮的行為，專家發現，現代人出現這類「手機網路症候群」的比例越來越高。精神醫學會前任理事長、凱旋醫院院長陳正宗曾在中國時報的報導中指出，「網路成癮」雖然目前仍沒有共同的定義準則，如果一天連續上網七個小時，連續三個月都出現同樣行為模式，離開電腦網路就坐立不安、焦慮易怒，就屬於成癮現象。

智慧型手機的過度使用不只造成精神與心理層面的問題，也會對身體造成影響，例如視力受損和手腕發炎的案例。2011 年 11 月中國時報也有報導，出現民眾因為躺在床上連續使用觸控式手機 2 小時，結果竟造成手腕嚴重發炎，差點導致脫臼。壢新醫院復健科主治醫師許嘉麟就本案例提到，因不正確使用觸控手機最容易引發的就是關節炎及拇指肌腱炎，這是因為拇指、食指過度運動，導致外擴肌腱受傷，症狀頗類似臨床常見的「媽媽手」，而新聞也戲稱因為玩智慧型手機造成受傷的手為「愛瘋手」。

小專欄：你有手機使用過度或成癮的症狀嗎?

美國探討數位生活的有趣網站 Digital Trends 曾經發表過一篇有趣的文章，該文章以幽默文字歸納出 10 個手機使用成癮的症狀，雖然不是很正式的參考指標，但也有網友表示讀完文章後覺得心有戚戚焉。請你也不妨以輕鬆的心情來試著讀以下的 10 種症狀，看看自己是否也有手機成癮或過度使用的跡象？

10) 你花在手機的週邊設備費用比手機本身還要多。例如備用電池、螢幕保護貼、保護殼（套）、汽車充電器、藍芽無線耳機與收話器、專屬喇叭或擴音機等。

9) 你的智慧型手機中安裝了超過 30 個 APP，且每一個 APP 都在使用。

8) 你的手機已設定鈴聲提醒你生活中的每一件大小事，從重要公司會議到醫生看診預約時間等，若你的手機設定提醒你本週三傍晚要倒垃圾的話，你過度仰賴手機的程度算是很嚴重喔！

7) 一有機會就使用手機。

6) 省下所有的生活必需開支以負擔手機通話與上網費用，例如用走的省下公車錢、吃泡麵省下餐費。

5) 一顆充滿電力的電池無法支撐你手機一日的使用，每天上班第一件事情就是幫手機充電，下班一回家的第一件事情也是。

4) 手機故障時，就好像失去了一個好朋友般。

3) 當遇到一位和你使用相同款式手機的朋友，你只想和對方討論有關手機的主題。

2) 將手伸到口袋或手提包底部卻沒摸著手機的瞬間，會感到驚慌，你不一定是遺失了手機，而只是忘記把手機帶在身上而已。

1) 你會帶著手機一起如廁。

by manwithface (CC BYD 2.0)
http://www.flickr.com/photos/poopface/

❺ 給家中有青少年低頭族父母的建議

兒童福利聯盟在今年初所公布的「臺灣學童手機使用狀況調查」結果發現，近 4 成兒童有手機成癮症狀，國內也有半數以上的國小 5~6 年級學童有手機，國中學生更高達 7 成使用手機，遠高於中國、日本和美國學童使用手機的比率。

此近 4 成的小朋友們出現的症狀包括：睡前躲在被窩裡玩手機佔 40%，邊用手機邊吃飯佔 43%，學童自認手機上花太多時間佔 45%，因沒帶手機而感到緊張佔 48%。

沉迷於智慧型手機或平板電腦與網路成癮是密不可分的，馬偕紀念醫院協談中心呂奕熹諮商心理師在中時媒體所刊出的報導中，提供了 5 個給家中有青少年低頭族父母的建議，以改善青少年過度使用手機或平板電腦的行為。本手冊將該報導所提供的 5 項建議摘要重點如後。

建議 1. 確認孩子需要的手機功能，夠用就好

若孩子希望有一支智慧型手機是為了炫耀、或者為了跟同學一樣，或是為了可以玩臉書、打電動等，那麼擁有一支高階手機是不必要的。當家長給予孩子手機之目的是為了瞭解孩子的去向，那麼一台普通的能撥打電話的手機就已經足夠，只給孩子適當的需求，不要超過。

建議 2. 不要試著介入孩子的社群

孩子需要網路社群，是因為虛擬世界中有更廣大的人際關係互動，而父母的介入，或是不時去回應監督，往往讓孩子很快就放棄這個社群，另外申請新的帳號重新開始；甚至連原有的朋友也不敢加入，害怕讓父母知道自己的最新動態。父母越想去親近孩子，孩子就會逃得更遠，或許保有一定的距離，才不會逼得孩子離自己更遠。

建議 3. 建立「奢侈品要成年工作賺錢後自己買」的概念

父母有時會把智慧型手機等高單價的 3C 產品，當成孩子成績進步的獎勵。但每個月手機通話與網路費，卻是父母要負擔；若使用上網吃到飽方案，也容易讓孩子更沉迷於網路世界。部分父母雖然會要求從零用錢中扣除相關費用，但無法解決沉迷問題，家長應幫助孩子建立奢侈品要成年後自己賺錢自己買的概念，教導孩子為自己行為負責。

建議 4. 以身作則，放下自己的手機

許多孩子的行為是模仿父母，若只要求孩子不沉迷於臉書、網路，但家長卻忙著用網路與手機，孩子絕對不會服氣。不管是網路成癮或是手機成癮，如果不能夠全家一起改變，每個人都遵守相同的原則，成癮者的症狀絕對很難被改變，由父母放下手機做起是與孩子溝通的基本誠意。

家長可適當提醒孩子在網路上要保護自己，並告訴孩子不管發生什麼事，需要幫忙的時候，父母親一定全力協助，不要害怕告訴父母，然後就是，請信任你的孩子。

建議 5. 不經意的案例提醒，比說教有效

在與孩子溝通臉書或網路成癮時，若能加入一些事實案例，對孩子會更有說服力，例如因為曾經在臉書上使用謾罵的字句，造成後來求職時不被聘任的理由，這樣會讓孩子在網路上的行為言語更為謹慎。

案例：一個寒假玩遊戲視力降到 0.5

一名 4 年級的小朋友貝貝寒假到外婆家過年，因為考試成績不錯，舅舅送了一台平板電腦作為新年禮物，貝貝一玩 APP 遊戲後就停不了手，家長因為覺得過年放鬆一下，便沒有做太多的管束，加上爸爸媽媽返回大陸上班後，貝貝一整個寒假都留在外婆家玩 APP 遊戲。開學後因為貝貝看黑板老是瞇眼睛，在家看電視也是越看越近，家長帶著去眼科醫師檢查後才發現，過去視力都保持在 1.0 的貝貝，視力竟然只剩下 0.4 和 0.5 了。

南方醫院眼科臨床醫生 湯明芳教授建議，孩子玩平板電腦每次不可超過半小時，讓眼睛得到休息，同時要控制螢幕合理的明暗對比度，也要控制使用電子產品的距離。

資料來源：今日新聞網

參考資料

[1] About.com Guide, "10 Tips for Wireless Home Network Security"

[2] BI Intelligence, "10 Ways The iPhone Changed Smartphones Forever", 2009/06

[3] European Network and Information Security Agency, "Online as soon as it happens", 2010/02

[4] McAfee Labs, "2012 Threats Predictions", 2011/12

[5] Nielsen, "Social Media Report - Q3 2011 US", 2011/09/11

[6] Nick Mokey, "Top 10 Signs of Cell Phone Addiction", 2010/01/25 (Digital Trends)

[7] ZDNet, "Facebook, Flickr, others accused of reading text messages", 2012/02/26

[8] 1111 人力派遣中心，『你 App 了沒?-上班族使用 App 習慣調查』，2012/02/13

[9] ETtoday，『性感薄紗內衣照莫名上臉書　妙齡女怒控包膜師』，2012/04/10

[10] TVBS，『何戎子玩 iPhone 10 分鐘花 6 千』，2010/08/11

[11] TVBS，『臉書掌握個資行蹤 3 嫌策劃綁親戚』，2011/12/11

[12] 今日新聞網，『iPad 是孩子的「毒蘋果」！？ 因損視力減睡眠』，2012/03/27

[13] 中時電子報，『注意！你的手機安全嗎？』，2010/12/14

[14] 中國時報，『出遊必打卡 你...網癮上身了嗎』，2012/2/28

[15] 中國時報，『手機玩過頭 當心愛瘋手上身』，2011/12/20

[16] 自由時報，『臉書帳號遇「駭」遭盜刷』，2012/04/16

[17] 行政院研考會，『』2011 年「數位機會調查報告」，2012/02

[18] 呂奕熹，『孩子是「低頭族」 怎麼辦』，2011/11/18 (中時電子報)

[19] 兒童福利聯盟，『2011 年台灣學童手機使用狀況調查』，2011/12/23

[20] 曾保彰，『無線網路安全簡介』，臺灣大學計算機及資訊網路中心資訊網路組

[21] 資安人科技網，『Check 你的無線網路是否安全』，2004/07/05

[22] 資安人科技網 ，『你噗浪了嗎？你臉書了嗎？你... 洩密了嗎?』，2009/11/30

[23] 經濟部技術處，2011 臺灣智慧型裝置持有與服務使用行為調查報告，2011/12

[24] 聯合新聞網，『惡意軟體鑽漏洞 闖進 app store』，2011/11/10

[25] 臺灣大哥大，『惡意 APP 不要來』

[26] 臺灣新生報，『沈迷智慧手機、平板電腦 損眼傷筋打亂身心』，2011/08/29

[27] 臺灣電腦網路危機處理暨協調中心，『802.11 無線網路安全白皮書』，2003/02

[28] 創市際市場研究顧問公司，『網友使用 Facebook 時數佔上網總瀏覽時數 27%；與去年同期相較使用時間佔比持續成長！』，2011/09

[29] 趨勢科技全球技術支援與研發中心，『電腦病毒與手機/平板電腦病毒的五個共通點』，2012/02/13

[30] 趨勢科技全球技術支援與研發中心，『安裝手機應用程式前要注意的三件事』，2012/02/01

[31] 蘋果日報，『瘋啥？下載中國版《憤怒鳥》 恐中毒』，2012/04/06

[32] 新華網，『黑客病毒產業鏈盯上移動終端 隱私資金受威脅』，2012/3/14

[33] Facebook 官方網站，www.facebook.com

[34] Google 官方網站，www.google.com.tw

[35] i-Security 官方網站 www.i-security.tw

[36] Nokia 產品簡易故障排除說明官方網站 www.nokia.com

[37] Plurk 官方網站，www.plurk.com

[38] 维基百科 Wikipedia 官方網站 www.wikipedia.org

[39] 賽門鐵克安全應變中心官方網站 www.symantec.com/zh/tw/security_response/

行動安全上網

出 版 者　教育部

發 行 者　蔣偉寧　教育部部長

召 集 人　吳國維　財團法人中華民國國家資訊基本建設產業發展協進會執行長

　　梁理旋　財團法人中華民國國家資訊基本建設產業發展協進會協理

指導委員　何榮桂　教育部電算中心主任

　　韓善民　教育部電算中心副主任

　　楊文星　教育部電算中心高級管理師

　　苗宗忻　教育部電算中心資訊管理組組長

　　劉玉珍　教育部電算中心資訊管理組程式設計師

審查委員　李宗薇　國立臺北教育大學教育傳播與資訊研究所教授

　　郭秋田　國立空中大學 管理與資訊學系助理教授

　　賴守全　銘傳大學 電腦與通訊工程學系助理教授

撰稿人員　梁理旋　財團法人中華民國國家資訊基本建設產業發展協進會協理

承辦單位　財團法人中華民國國家資訊基本建設產業發展協進會

出版日期　民國 101 年 06 月

此手冊內容係對特定議題所提供之學習教材，僅供各界參考，非本部相關政策。