你使用的 APP 安全嗎？

◎陳婠綺

隨著智慧型手機的普及與其功能越來越強大，如同一台隨身電腦，加上使用者將許多檔案、照片也存放於手機內，因此智慧型手機延伸出的資安問題已成為國人的重要議題。

現在隨處可見的「低頭族」，人手一支智慧型手機，想要下載各種 APP 軟體只要手指輕輕一按就能搞定。APP 市場競爭激烈，不少業者紛紛祭出「免費」軟體吸引消費者，但看似免費的背後，付出的可能是親朋好友的隱私。目前免費的 APP 資安軟體與付費版本最大的差異主要是功能上的不同，免費版本主要是提供基礎的偵測與防護，進階功能則必須購買付費版本。甚至有些 APP 本來是付費軟體，卻在重新上傳後，成為免費軟體，許多人不疑有他，還以為撿到便宜，就在不知不覺中掉入陷阱。Google 雖然在 Android Police 回報後，５分鐘內就將這些軟體下架，但下載數可能已經超過五萬次。更可怕的是，Google 本來還特別提供了名為 Android Market Security Tool 的工具，用以清除那些惡意軟體對手機所做的修改，從而防止手機在感染惡意軟體後，將手機中的重要資訊上傳給不法分子；結果這些歹徒居然也將 Google 開發的反木馬工具，改變成木馬化應用程式。這個軟

體不但會蒐集手機中的相關資訊，傳送到遠端的網站，還會不經使用者允許就執行某些功能和動作，包括修改通話紀錄、攔截或監控訊息，以及下載影片等，可見手機惡意軟體的可怕程度，絕對不輸給個人電腦的惡意軟體。

事實上，相較於個人電腦用戶對下載軟體已有基本戒心，而智慧型手機用戶尚未建立起相同習慣，讓中毒的可能性大增。手機資安的問題，因為越來越多的社交網站都已推出多平台移動設備用戶端，而變得更加嚴重。這些行動裝置端的安全防禦，也比個人電腦端要差很多，加上咖啡廳、機場、旅館等公共場所提供的無線網路安全問題，讓網路犯罪分子可以利用的攻擊管道，變得越來越多。

現今網路正熱門的社群網站 Facebook，也可能成為駭客釣魚的釣餌；駭客假冒 Facebook 名義，發送假警告信件給使用者，但使用者卻不知道其內含釣魚網頁連結，讓使用者誤信帳號已遭檢舉為垃圾帳號，需於 24 小時內立即點選 email 內的連結進行帳號安全性確認，否則帳號將可能遭永久停用。使用者一旦點選該網址後，使用者將被導向特定網頁，該網頁貌似 Facebook 的安全檢測系統，要求使用者輸入註冊 Facebook 的 email 帳號、密碼及生日等個人資料；輸入該網

頁所要求的訊息後，使用者將再被導向另一個網頁，並被要求提供信用卡等相關資訊，最後導致個資外洩。

近來人手一支智慧型手機，使用者個人的隱私風險，也經常暴露在各種惡意程式攻擊的威脅中，智慧型手機的資安問題逐漸浮現。由於現代人將許多重要的資料、照片、訊息都存放在智慧型手機中，手機一旦遺失就可能造成重大的個資外洩問題。現今的手機未必只是一支電話，它還可能成為個人的錢包、身分證、電話簿及家庭相薄，當我們的行動裝置具有以上用途，若遭遺失或被盜，便會造成敏感資料外洩風險。再加上使用者十分依賴各項 APP 程式的功能，根據國外媒體報導顯示，許多手機應用程式的使用條款中，允許手機程式開發商可以查閱手機用戶的個人資料，甚至查看照片、通話對象等，個人資料就在不知不覺中外洩。許多手機用戶在下載付費或是免費的 APP 程式時，未詳閱程式使用條款即按下同意，此舉可能讓手機應用程式開發商有權搜尋手機內的相片，或是手機用戶的所在位置。社群網站 Facebook、Badoo、雅虎公司和照片分享網站 Flickr，皆坦承透過搭載 Android 系統的智慧型手機應用程式，可讀取手機用戶的簡訊。其餘不知名、免費下載的應用程式，大多在使用條款及條件中，也明確寫到有權取得用戶的個人資料。

程式開發商看準個人資訊能讓社群網站的定位更明確，若能提供更貼近使用者的服務則能增添網站的魅力，因此「個資」儼然成了所有業者最垂涎的商品。一項由臉書技術支援的雅虎公司服務，要求使用者提供宗教信仰、政治傾向才能進入；網路電話 Skype 也透過使用者拿到他們朋友的臉書照片和個資。雖然臉書要求 APP 在取得使用者的個資前，必須徵求使用者的許可，但若是朋友資料遭外流，當事人也不會收到任何通知。不少人開始擔心，這些看似免費的服務，實則賠上隱私代價，反倒是握有這些籌碼的業者，能吸引廣告主、APP 開發商或是更大的商機。

隨著手持行動網路的普及，資訊安全已從傳統電腦作業系統，擴展到手持裝置系統，部分消費者也開始建立智慧手機和平板電腦的防毒功能。但資安業者還是提醒民眾，除了安裝適當的防毒軟體之外，更應養成良好的手機使用習慣，以保護自身的資料安全。

面對日益氾濫的手機病毒，手機用戶也不是沒有預防之道，只要遵守下列防毒程序，還是可以將手機病毒有效隔離：

一、慎用藍芽裝置。就像流行性感冒一樣，病毒肆虐期間，如果到公眾場合，最好暫時關閉手機上的藍芽接收功能。如果有陌生的手機，或任何擁有藍芽裝置的機器請求連接，最好不要接受；就算是收

到朋友傳送的多媒體簡訊，對於來路不明的手機程式，還是不要任意安裝。

二、接收到亂碼顯示的文字簡訊和多媒體簡訊時，最好立即刪除，因為這些亂碼簡訊，很有可能暗藏惡意的程式碼。

三、確認手機下載網站的安全性。許多智慧型手機的用戶喜歡到網路上找尋免費的軟體下載，不過這些網站卻可能是暗藏手機病毒的大毒窟。為了要遠離手機病毒，最好不要到來路不明的網站下載軟體程式。

四、如同電腦一樣，安裝防毒軟體，定期掃毒，能夠減少手機遭到數位病毒感染的機率。

由於智慧型手機的普及，導致手機資訊外洩的案例屢見不鮮，加上雲端運算和虛擬化，外洩的個資無論是關於個人品德缺陷或遭敵威脅利誘，都已對國家安全造成嚴重的影響；身為基層的我們雖沒有接觸國家安全的重大機密，也不具有決定國家指導方針的權力，但我們每一個人都是組成捍衛國土的堅實分子，所以我們必須從自身做起，並應該戒慎恐懼，攜手共同面對這項威脅，體認國家安全、匹夫有責的觀念。唯有每個人都自我要求，恪遵規定，才能建構一個堅若磐石的安全網。