**你今天APP了嗎？**

◎魯晏汝

　　在現今幾乎是人手一支智慧型手機的年代，也應運而生出各式各樣的名詞，像是「低頭族」、「APP」等等。什麼是「低頭族」呢？就是指不管在什麼場合，只要有空閒便拿出手機低頭玩遊戲、傳訊息、看影片的人；而這些智慧型手機裡的遊戲或軟體，正是常聽見的「APP」。（「APP」是「Application」的縮寫，此指應用程式或應用軟體。）

　　智慧型手機是一種可以隨意安裝或移除應用軟體（APP）的手機，它擁有開放的系統環境，可讓第三方自行研發的APP，以付費或免費的方式提供給使用者自由運用；而透過這些APP軟體，使用者可以隨時隨地更新資訊，例如新聞媒體的APP點開後即可瀏覽最新的新聞訊息；社交應用類的APP可以發送免費的訊息或是撥打免費的網路電話等，因此，智慧型手機可說已完全融入現代人的生活。然而，對手機的依賴度越高，手機裡存放的私人或機密資料也就越多，而使用者對於手機的安全防護意識並未相對提高，所以對駭客來說，攻擊手機的容易度及成功率遠較電腦為高，智慧型手機自然就成了新一代駭客攻擊的目標。

　　儘管手機和電腦所使用的網路傳輸模式不太相同，但是駭客採取的攻擊模式卻極為類似，目前最主要的攻擊管道不外乎是SMS或MMS簡訊、作業系統或瀏覽器的安全性漏洞，亦或是仿造熱門下載的APP軟體，從中放置惡意程式等。不久前即曾經出現過「假Skype」事件，就是針對這些高人氣軟體，在使用者不知情的情況下安裝APP後，也會自動安裝其他加值服務或是惡意程式，然後透過惡意程式自動發送簡訊給通訊錄裡的名單，造成帳單金額暴增；而這些惡意程式也透過手機裡的通訊錄，不斷地四處發布有毒的手機簡訊或不明連結網址，一旦不小心誤點連結後，不只會讓手機遭受控制無法使用，更可能導致個人資料的外洩，造成難以想像的損失。因此，無論是電腦設備或是手機的使用，都應時時保持高度的警覺心。

　　筆者曾經遇過一位朋友的MSN被駭客盜取後，不斷地發送不明連結給通訊錄上的朋友，這都歸責於對資訊安全的敏感度太低，不僅有個人資料外洩的風險，也增加其朋友的風險與困擾。為避免這種情況發生，每位使用者都應提高對安全性的敏感度，對於來路不明的手機程式不要亂安裝，若要下載應用程式，也應選擇合法的官方網站。另外，下載APP軟體前一定要先看過使用者評價，確認其安全性後再下載；如收到來路不明的簡訊，也不要打開，要立即將它直接刪除；而接受朋友傳送過來的檔案時，也必須再三確認是否為其本人，如非本人請不要隨意接受檔案。只有在使用上多一分警覺心，才能避免重要資料損毀，或造成其他方面難以估計的損失。 （摘自清流月刊）