

智慧型手機所面臨之資安風險

隨著科技進步，智慧型手機已可提供上網功能，而且使用上比起個人電腦更方便。個人電腦面臨的資安風險及威脅，智慧型手機一項也不缺。但由於智慧型手機使用者年齡涵蓋範圍極廣，所以資安風險意識之建立更為不易。綜觀智慧型手機面臨資安風險之來源，包含智慧型手機硬體及韌體、外加行動應用 App 及使用者上網習慣等。

近年來，媒體報載智慧型手機系統內建軟體及行動應用 App 未經使用者同意，卻已啟用手機功能或者蒐集手機內存資料後，回傳至手機製造商、服務提供者或第三方之情形時有所聞；更甚者，於硬體植入後門，進行資料蒐集並回傳廠商。

在技術上，智慧型手機之硬體、軟體及韌體都有可能將其內存資料外洩，甚至回傳至特定伺服器，但多數消費者卻渾然不知，或是忘記當初安裝行動應用 App 時所同意 App 可以使用的權限項目及範圍。因此，手機資安風險議題亦包括手機製造商或 App 提供者是否提醒、告知及揭露軟體的使用權限等資訊，讓消費者有選擇 SAY NO 的權利與機會。

消費者於選購智慧型手機、安裝行動應用 App 及連上網際網路時，都應提高資安風險意識。如選購經資安認證的手機，安裝 App 時確認其使用權限及可能被蒐集的資料，僅連接熟悉、有保障的 Wi-Fi AP 等。只要提高警覺就能將資安風險降低，才不會因為疏忽，將個人資料或機敏資料，傳到手機製造商或 App 提供者，甚至第三方的手中！

～ 轉載自國家通訊傳播委員會網站～