# 公務機密維護宣導

## ~「公務機密維護：Line 來 Line 去，資安別賴掉」

近年由於行動通訊的發展，智慧型手機的普及率越來越高，根據臺灣網路資訊中心所公布的 2014 年臺灣寬頻網路使用調查結果顯示：國內行動上網人數已達 1,260 萬人。財團法人資訊工業策進會創新應用服務研究所 FIND 團隊的調查，推估全臺行動族群計有 1,432 萬人，且同時持有智慧型手機及平板電腦的人口則有 527 萬人。

近年間 Line 變成國人手持式行動裝置上首選的即時通訊軟體，它不僅是年輕人溝通的工具，甚至變成政治人物親民、愛民、戮力政務的象徵，任何政府機關好像沒有用 Line，就是落伍、不認真。

但是 Line 用於公務上真的安全嗎？以往發生在即時通訊軟體上的詐騙案就已層出不窮，小到如前往超商買遊戲點數，大到要對方去銀行轉帳，詐騙手法不斷翻新。先前又發現某刑大大隊長的 Line 帳號遭盜用，被拿來要求朋友買遊戲點數；也有人誤把色情影片或個人行程傳到公務群組。

使用 Line 多年經驗的小潘也看到這則新聞，於是就在師生下午茶約會中跟司馬特老師討論這個議題。司馬特老師聽完小潘的問題，喝口咖啡表示，使用即時通訊軟體所面臨的資訊安全問題，可分成幾個層面來看，包括帳號、身分認證以及訊息內容。所有開放式系統為了讓使用者能為它編寫應用程式，都會將它的系統架構、功能開放出來；既然把門打開，有心人士難免就會進來，這是不可避免的宿命，尤其在網路世界，門禁幾乎是不設防的狀態，即使像微軟這麼大的公司，它的 Windows 系統也是經常有病毒、駭客出沒。

目前市面上的智慧型手機，除了 Apple 是自己專屬的作業系統外，其餘的手機廠商，不管是 Android 系統或者是 Windows Phone 系統，都屬於開放式架構，因此，手機業者一旦選上它，就已具備被入侵的缺陷，這是它先天上的不足。既然先天已經不足，後天就不能再失調，即時通訊軟體的訊息係透過網路傳送，而病毒、駭客都會經由網路進來，所以帳號密碼要選用複雜度高的，而且要定期更換才不容易被破解。若

遇有異常對話，應先做身分認證，身分認證若在即時通訊軟體上無法確認，就應透過電話的方式進行。

Line 來 Line 去的資訊安全議題，應該置重點於內容上；內容包括了群組成員的對話及傳遞的資訊內容。無線通訊是透過訊息在空氣中傳遞，既然以空氣為介質，當然無法避免有心人士的非法截取。試想，如果警方在攻堅時，用 Line 公告攻擊發起的時間，萬一訊息被歹徒接收了，會有什麼後果？

每個人在即時通訊軟體上可能擁有很多群組，這麼多的群組，如果把機密訊息發錯群組，又會造成什麼後果呢？這可不像我們在聊天時，發現講錯地方，補一句「打錯了」就沒事的。即時通訊軟體一旦發出就收不回，機密資訊一旦發錯群組，就被看光光了。最重要的是傳送檔案的問題，由於 Line 是日本公司發展的軟體，伺服器在國外，所以我們不知道傳送檔案的路徑是什麼，在這麼遠的過程中，萬一被有心人士從某個伺服器中截取，而這個檔案又具機密性，則對國家造成的損失，可能難以估計。

小潘聽到這裏，又有了新的問題，效率跟安全可不可以兼得呢？

效率跟安全當然要同時考量，為了避免檔案遭洩漏，政府機關在使用即時通訊軟體傳送檔案時，應訂定機密等級，限制沒有機密等級的資料才能透過即時通訊軟體來傳送，具有機密性的檔案本來就要依規定傳送，資訊安全還是高於一切。

小潘這時恍然大悟，政府跟企業最大的不同在於它處理的事務，很多都跟國家、人民的安全有關；行政的效率固然重要，但是，不能只為了追求效率而忽略安全，畢竟，沒有了資訊安全，再高的效率都沒有用。

摘自清流月刊104年6月號 （作者為科技大學資訊管理系講師）