公務機密維護宣導--「Line 來 Line 去，Line 出問題」

根據根據 iThome 於 107 年 3 月間的報導，LINE 用戶已突破 1,900 萬，每天使用 LINE 進行語音通話人數也突破 700 萬，毫無懸念地，LINE 已成為臺灣最主要的社群通訊軟體。舉凡學生喜歡用 LINE 溝通，老師用 LINE 教學分享、指導課業，公務機關亦起而效尤，隨手建立公務群組，藉此橫向連繫、有效溝通。但是每天使用的你，知道它也存在一些「黑歷史」嗎？每天 LINE 來 LINE 去到底會不會出事？其他通訊軟體像是 WhatsApp、Instagram 會不會比較安全？這些疑問從來就沒有消停過！

東森新聞於 2018 年 11 月 29 日報導「手誤傳錯群組，潘姓員警被依過失洩密罪送辦，檢方給予緩起訴處分」，內容陳述 2017 年間偵辦擄人勒贖案的潘姓員警，原本要傳「偵辦進度報告」給負責調閱監視器的同事，卻誤傳到反年金改革的群組「台灣憤怒鳥」，該案檢方於 2018 年給予緩起訴處分，需繳交公庫 3 萬元。另外 LINE 最常遇到的態樣，當屬詐騙集團竊取個資及財務等問題；此外 LINE 也成為假訊息散布平台。

LINE 潛藏風險可約略將之分為「操作風險」及「軟體風險」，分述如下：

一、操作風險

(一)如前述案例所載，使用者於公務上可能同時與多群組人員聯繫，稍有不慎，易誤傳公務相關文件予不相干第三人，即使 LINE 具備「訊息回收」功能，也難得知第三人是否已知悉內容。

(二)許多人使用 LINE 未了解軟體具備之功能，像是 LINE 聊天室的「相簿」、「儲存至 Keep」功能等，可將檔案上傳雲端，若不善用而隨意儲存在手機目錄、相簿內，一旦

手機誤植木馬軟體等，手上資料恐遭外洩。

(三)LINE 若設定不當，允許陌生人加為好友，讓有心人士有可趁之機，偽冒熟識、家人，誘騙點選連結進行 APT（Advanced Persistent Threat）攻擊或交付資料等，均可能引發資安風險。

(四)公務機關人員為求跨部會聯繫提升效率，往往建立許多群組，群組成員間彼此也未必熟識；又尚未在 LINE 群組裡指定管理者時，任何成員均可邀請他人進入該族群內；倘若誤加入非此公務相關人員，將滋生公務資料外洩疑慮。

二、軟體風險

(一)LINE 可隨意轉貼及點選任何網址，若是該網址潛藏惡意代碼，手機極可能被植入惡意程式，導致機敏資訊遭竊。

(二)LINE 建置雲端資料庫能儲存用戶或群組對話內容及檔案，但若 LINE 公司遭駭客入侵，即可能洩漏用戶或群組之檔案及對話內容，即使循司法調查管道，亦因 LINE 屬國外公司而增加偵辦難度；此外，使用者在通訊過程中亦存在遭 LINE 公司側錄對話內容之風險，故以國安角度考量，確實不宜在機敏公務上使用。

因應風險防制有 5 點：安裝訊息加解密軟體、「LINE」群組中建立管理人員、持續更新 LINE 版本、安裝防毒軟體及不隨便加好友、加官方帳號。

LINE 在臺灣儼然成為生活不可或缺的一部分，公務機關也常藉此開設公務群組，期以「行動辦公室」增進行政效率，然而在享受便利的同時，我們也要明白使 LINE 所必須承擔的資安風險，盡可能不要在 LINE 上處理公務，倘仍須處理公務，務必考量 LINE 使用上的安全性。您可透過安裝加解密軟體、調整 LINE 操作等預防方式，在最低的風險下，方能享受 LINE 帶給我們的便利。

~~ 節錄自 2019/3 月號-清流雙月刊 ~~ 政風室 關心您