



【數位時代防護術-「LINE 不當轉傳致洩密」】

【no.2】

壹、前言

隨著智慧型手持裝置日益普及，資通網絡升級與即時通訊軟體大行其道，資訊運用除了更加便利外，更伴隨著令人擔憂之資安事件及機密外洩等問題。熱門通訊軟體中，不論是 LINE、Facebook Messenger、WeChat 等，其通訊安全性都備受質疑，甚有媒體報導警政署表示即時通訊應用軟體有其便利性，但都是民間研發的商業軟體，政府機關不能管控，難防洩密。加以邇來媒體報導使用該等軟體諸多被駭、詐騙、洩密及誤傳事件，讓其安全性備受爭議。此等資訊安全情事屢見不鮮，值得機關加以防範與管制。

貳、案例摘要

刑事局某外勤隊日前與多個縣市警方共同偵辦一起詐騙集團犯罪案，行動前所有專案成員都在智慧型手機上開立一個 LINE 的群組，用 LINE 傳送嫌犯照片、即時資訊、並下達攻擊指令。惟至現場攻擊時，發現空無一人，原來嫌疑犯等人早已獲知消息，提早一步逃離。經調查發現，該次搜索行動採用時下流行的 LINE 傳送訊息，因使用群組發送，群組中某些負責情報蒐集成員在轉傳訊息時「手滑誤觸」其他友人頭像，致搜索行動訊息被轉傳，輾轉流連最後傳到詐騙集團手中，導致整個搜索行動提前曝光，致該不法集團成員先行逃匿，功敗垂成。

參、問題分析

- 一、機關缺乏對於新型設備、軟體之洩密評估風險及預警，LINE、Facebook Messenger、WeChat 等即時通訊軟體帳號被盜、洩密、誤傳訊息之新聞時有所聞，機關未建立相關預警機制。
- 二、未停用 LINE 等即時通訊軟體利用行動電話號碼自動加入陌生人為好友的功能，亦未定期刪除或封鎖 LINE 等即時通訊通訊錄之陌生人。
- 三、機關對智慧型手持裝置防制洩密之宣導不足，機關同仁對於智慧型手持裝置洩密方式不甚清楚。
- 四、貪圖傳訊快速便利，忽略即時通訊軟體無法加密或刪除所發訊息，低估該等軟體洩密風險。
- 五、公、私務器材物品混用不分，智慧型手持裝置通訊錄之聯絡人亦公私不分。

肆、改善及策進作為

- 一、落實資訊安全稽核檢查作為
為使資訊安全保密工作更臻完善，除了加強教育宣導之預防工作外，辦理督導考核亦是重要的一環；期透過稽核、檢查過程中發掘優、缺點，以落實資訊安全保密執行工作。
- 二、定期清查或檢測智慧型行動裝置防駭防毒效能
智慧型行動裝置之功能已趨近於電腦，由於其攜帶方便之特性，使用者對於 LINE、Facebook Messenger、WeChat 等通訊軟體使用頻率及依賴性增加，遭受資安威脅之機率亦更高，故對於智慧型行動裝置應比照電腦定期辦理資訊稽核，並加裝及定時更新防毒防駭軟體，以及審慎維護管理 LINE 等通訊軟體之帳號，避免機密資料外洩或遭受惡意程式攻擊的危機。
- 三、確實落實公務機密宣導事宜，深植資訊安全觀念
目前智慧型行動裝置使用率極高，但是使用者對於智慧型行動裝置潛在之資安危機普遍缺乏警覺，尤其以 LINE 等即時通訊軟體傳送公務訊息或資料時，如能提供同仁瞭解智慧型行動裝置可能存在之資安漏洞，方能明瞭弱點進行強化與修補。是以，各機關得彙整相關公務機密法令規定、洩密違規案例，以及可能導致洩密管道與因素，並結合機關各項會議及活動，有計畫有系統的利用各種時機向同仁宣導，使每一同仁均能瞭解相關法令規定。
- 四、使用安全性更高之即時通訊軟體
LINE、Facebook Messenger、WeChat 等通訊軟體屬於國外公司研發之軟體，其電腦主機與管理權限皆不屬我國管轄，且上述軟體使用人數破億，商機極為龐大已成為駭客覬覦的目標。若機關有即時通訊需求，建議使用安全性更高，使用者較少之即時通訊軟體，如我國工業技術研究院研發的開發之揪科 (Juiker) APP 作為替代，惟在未轉換更安全之相關軟體前，建議各機關妥善維護管理 LINE 帳號。
- 五、以公務用或私用之用途區隔智慧型手持裝置
使用公務用智慧型行動裝置，應避免私人用途及連結不明網站或下載不明之程式或軟體；傳送訊息時，應再三確認收件者對象及內容是否正確，避免誤傳，內容涉及隱私、機敏資料，應盡量避免使用即時通訊軟體傳送。