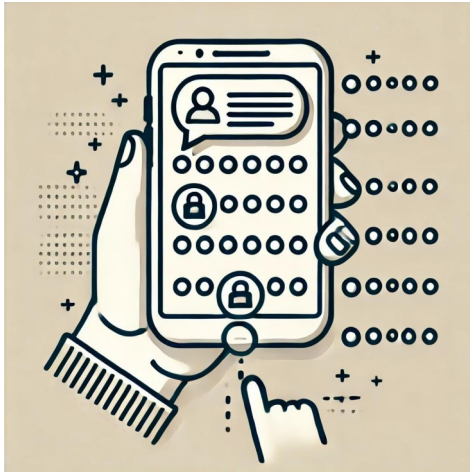




LINE 不當轉傳致洩密風險分析及因應措施

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。甚有媒體報導警政署表示即時通訊應用軟體（LINE、Facebook、Messenger）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，讓其安全性備受爭議。

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皆於智慧型手機開立一個 LINE 群組，透過 LINE 傳送嫌犯照片、即時資訊，並下達攻堅指令。然而至現場攻堅時，發現空無一人，原來嫌疑犯早已獲知消息，提早逃逸。經調查係群組成員在轉傳訊息時「手滑誤觸」其他友人頭像，致搜索訊息輾轉流傳，最終傳到詐騙集團手中，導致行動提前曝光，功敗垂成。

問題分析

1. 機關缺乏對新型設備及軟體之洩密風險評估及預警機制，未建立相關防範措施。
2. 未停用 LINE 等即時通訊軟體利用手機號碼自動加入陌生人好友的功能，也未定期清理陌生聯絡人。
3. 機關對智慧型手持裝置防制洩密宣導不足，同仁對智慧型裝置的洩密方式認知不足。
4. 因傳訊快速便利，忽略即時通訊軟體無法有效加密或刪除訊息的事實，低估洩密風險。
5. 公私務器材混用，聯絡人資訊未明確區隔，增加洩密風險。

改善及策進作為

1. 落實資訊安全稽核及獎懲制度，定期檢查同仁資安保密執行情形，以提升保密警覺性。
2. 定期清查及檢測智慧型行動裝置的資安防護狀態，並安裝與更新防毒防駭軟體。
3. 落實公務機密宣導，深植資訊安全觀念，避免使用即時通訊軟體傳送敏感或機密訊息。
4. 推動智慧型手持裝置公私用途明確區隔，避免混用導致洩密。
5. 建議機關使用如工研院開發的「揪科（Juiker）」通訊軟體，以替代國外商用軟體。
6. 禁止破解或越獄公務智慧型手持裝置，防範資安風險。

結語

公務機密維護已進入 E 化時代，唯有透過有效管理及持續宣導教育，提升資安意識，才能保障民眾及機關權益。