公務機密宣導

使用即時通訊軟體洩密案例

案例說明

一、案例1

〇〇市政府雇員A被控將聯合稽查時間和對象，以直接或間接透過中間人方式，洩漏給電子遊戲場和養生館業者，法院審理後，判張女2年徒刑，得科罰金，緩刑4年。

基隆地方法院判決書指出，A任職於〇〇市政府期間，將市府聯合稽查時間和對象，逾百次透過LINE傳送訊息給中間人B、C、D和E，再由4人分別洩漏給10多家電子遊戲場業者。

A傳送之訊息LINE訊息，有如告知中間人稽查某間足體養生館時間，或直接傳送給電子遊戲場業者「提醒今天晚上要去你家要記得喔、等等我要去你家、星期五20號晚上要去你家喝咖啡但不是我去」等訊息，洩漏聯合稽查時間，讓業者得以事先準備，以免遭裁罰。

（新聞來源：2022/10/10中央通訊社）

案例說明

二、案例2

〇市政府傳出洩密案，臨時員工F負責處理民眾檢舉信件時，明知規定不得透露檢舉來源、民眾個資等，竟將信件內容貼到共有20人的工作群組內，導致檢舉人個資、檢舉內容均曝光。經內部人員通報後遭法務部廉政署查獲，檢方認為F涉嫌洩密，但考量其無前科、犯後坦承，予以緩起訴處分。

F任職單位表示F負責1999案件之分派業務，為利分文時效，並確認是否為該科業務，始將內容截圖至科內群組，卻因一時不察，將檢舉人資訊一併揭露。

事發後已請政風室辦理法令宣導課程，並於各會議場合加強保密及個資維護宣導，且於新進員工報到時提供保密及廉政倫理規範宣導資料，以避免再度發生類似情事。

（新聞來源：2021/8/19聯合新聞網）

案例分析

一、資訊傳遞

1. 資安風險控管之關鍵點為**「資訊傳遞」**。若能做到一律不以即時通訊軟體傳輸涉及機密性、資訊安全及隱私事項之公務資訊，原則上就不可能會有透過即時通訊軟體傳輸或外洩的機會。

2. 公務人員線上進行公務討論聯繫時，應注意**資訊安全與通訊內容之機密性**。

3. 公務人員利用行動裝置從事公務討論時，應進行**資料備份與加密防護**，並**注意該裝置遺失或廢棄時之資料處理**。

案例分析

二、通訊軟體的公務群組管理

1. 通訊軟體的公務群組管理，應由群組管理者（如：組長）**本於管理權限進行群組成員之加入或退出之審核**。因此，若不具有加入群組資格、或所任職務與該群組之公務目的無涉者，就無法進入該群組而有後續接觸公務資訊的機會，藉以降低公務資訊外流的風險。同時亦應注意授權的必要性，避免加入群組者過多。

2. 即時通訊軟體（例：Telegram、LINE等）日趨普及，雖可提升公務聯繫效率，但也不可輕忽其資訊安全風險。

3. 尤其在**任何公開**之新聞群組、論壇、社群網站或公布欄中，應特別注意**不可透漏任何與公務機密相關之細節**！

改善及策進作為

一、若確有需求，應改用安全性更高之即時通訊軟體，並謹慎使用：

1. 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非屬我國管轄，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，洩密風險日益升高。
2. **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開發之揪科（Juiker）APP 作為替代。
3. **在未轉換更安全之相關軟體前，各機關應妥善維護管理LINE等通訊軟體之帳號，**且**應該謹慎並有限制範圍地使用**，才能避免重要公務資訊不輕易外洩、確保各項機密資訊的安全。

改善及策進作為

二、加強公務機密宣導事宜，深植機關同仁之資訊安全觀念：

1. 即時通訊軟體能夠提供工作上即時互通的便利性，卻缺乏加密保護的功能，使用者往往亦對這些軟體或智慧型行動裝置本身的潛在資安危機**缺乏警覺**。
2. 機關可結合機關各項會議及活動時機，宣導同仁應注意資安風險，培養其保密及資安意識，盡可能降低洩密風險，並應提醒同仁以 LINE 等即時通訊軟體傳送公務訊息或資料前，**務必再三確認欲傳送之訊息或資料是否適切及必要，所傳遞之對象是否正確，且不得傳送機密及重要公文**。
3. 同時，公務人員因職務知悉或持有相關資訊時，**切勿公開談論內容，或為私用而影印、掃描公文，甚至將訊息外流**！

改善及策進作為

三、定期檢測智慧型行動裝置防駭防毒效能：

1. 智慧型行動裝置功能日益完善，且因攜帶方便，使用者對於LINE、Facebook Messenger、 WeChat等即時通訊應用程式之使用頻率及依賴性增加，遭受資安威脅之機率亦隨之升高。
2. 因此**智慧型行動裝置亦應安裝及定時更新防毒防駭軟體**，並審慎維護管理自己的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。

改善及策進作為

三、定期檢測智慧型行動裝置防駭防毒效能：

3.行政院國家資通安全會報技術服務中心近期發現駭客鎖定通訊軟體LINE發動攻擊活動，用戶相關內容遭擷取外流，爰發布「漏洞/資安訊息警訊」，就強化**通訊軟體LINE安全性**提出建議：

(1)建議**勿使用即時通訊軟體討論公務或傳輸機敏資訊**，傳輸**檔案均應加密**，且**處理公務之設備不得安裝有資安疑慮之產品**，以降低機敏資訊遭外洩之風險。

改善及策進作為

三、定期檢測智慧型行動裝置防駭防毒效能：

(2)為檢視Line帳號安全性，請至「**LINE app主頁→設定(齒輪圖示)**」各項下執行下列步驟:

a.**隱私設定**→檢視訊息加密功能【Letter-Sealing】是否開啟；
若未開啟，請立即開啟。

b.**我的帳號**→檢視【允許自其他裝置登入】設定是否開啟；
若有開啟，請執行第3點↓。

c.**我的帳號**→檢視【登入中的裝置】，是否有陌生裝置登入；
如有陌生裝置登入，表示此帳號遭駭風險高，請先截圖留存畫面，將該陌生裝置登出後，並執行第4點↓。

d.**我的帳號**→將【允許自其他裝置登入】設定為關閉。

資料來源：

1.法務部廉政署-公務機密宣導案例-公務機密維護-錦囊第6號_LINE 不當轉傳致洩密
https://www.aac.moj.gov.tw/media/74484/%E6%A9%9F%E9%97%9C%E6%A9%9F%E5%AF%86%E7%B6%AD%E8%AD%B7plusplus%E9%8C%A6%E5%9B%8Aplus%E7%AC%AC6%E8%99%9F_line%E4%B8%8D%E7%95%B6%E8%BD%89%E5%82%B3%E8%87%B4%E6%B4%A9%E5%AF%86.pdf?mediaDL=true

2.清流月刊-中華民國109年3月號「通訊軟體用在公務上好不好」
https://www.mjib.gov.tw/FileUploads/eBooks/7ceda1184b2b4d01b522fbde956fd2bf/Section_file/bd5a3a9ddef04379955fdbb999963415.pdf

3. 苗栗縣政府政風處-7月宣導–〈公務機密宣導-通訊軟體洩密〉
https://webws.miaoli.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvNDE2L3JlbGZpbGUvOTc0NS80MjUxOTEvZjM3YTQ5ZTItNDc4MS00NTQwLTkxNmQtNjcyZDAzMGNiZTZjLnBkZg%3d%3d&n=5YWs5YuZ5qmf5a%2bG57at6K23LemAmuioiui7n%2bmrlOa0qeWvhig35pyI5Lu9KS5wZGY%3d&icon=.pdf

4.行政院國家資通安全會報技術服務中心- 2021年7月28日漏洞/資安訊息警訊
http://webnas.bhes.ntpc.edu.tw/wordpress/archives/22667

5.中央通訊社─基市府雇員涉洩密稽查 判刑2年
https://www.cna.com.tw/news/asoc/202210100090.aspx

6.聯合新聞網-桃園市府新工處傳洩密 民眾檢舉信、個資遭承辦人貼LINE群組曝光
https://udn.com/news/story/7321/5684086

——花蓮縣政府政風處關心您！