LINE來 LINE去，LINE出問題

／鍵盤 007

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！

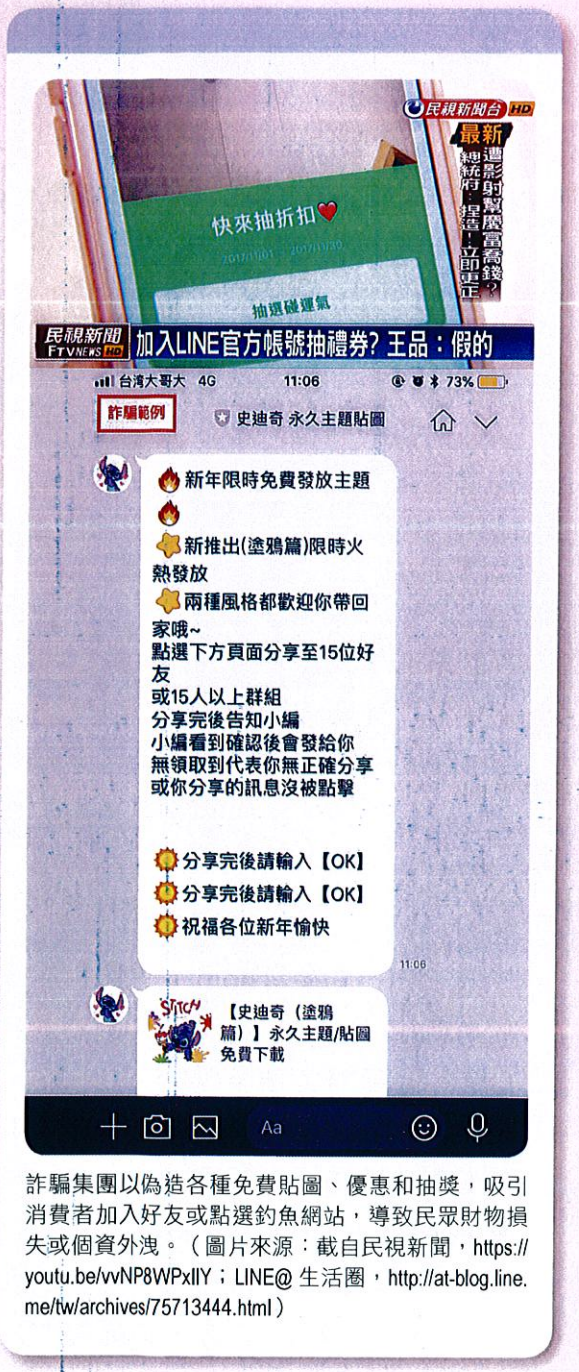
LINE 近期議題

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。

LINE 最常遇到的態樣，當屬詐騙集團竊取個資及財務等問題。趨勢科技所屬「資安趨勢部落格」曾指出詐騙集團善於偽造「瘋傳 7-11 限時發送 100 元禮券」、「FamilyMart 送全家千元禮券」等等詐騙帳號，吸引民眾加入好友或點選釣魚網站連結。據趨勢科技防詐達人調查，臺灣前 15 大 LINE@ 詐騙帳號受害品牌店家，以臭跩貓詐騙貼圖排名第一，共有將近 150 組詐騙 Line@ 帳號；而被發現的詐騙帳號中，1/2 為假貼圖，1/4 則透過假冒如星巴克、王品、中油、全聯、7-11、全家等店家假優惠名義引誘消費者上鉤。

其他通訊軟體，像是 WhatsApp、Instagram 等亦存在類似資安風險，例如 iThome 亦指出 WhatsApp 於 2018 年 10 月才修復一項漏洞，該漏洞允許使用者於視訊通話時，讓駭客有機會操控手機程式。

此外 LINE 也成為假訊息散布平台，長輩、朋友間都用 LINE 轉傳不實消息，例如「菌類不能和茄子一起吃」、「柿子加優酪乳會中毒」等，另 107 年 9 合 1 大選之前，LINE 更成為攻擊各候選人的大平台，常有人轉傳「韓國瑜造勢現場發走路工 1,500 元」、「陳其邁辯論會帶耳機」等攻訐候選人不實訊息。



詐騙集團以偽造各種免費貼圖、優惠和抽獎，吸引消費者加入好友或點選釣魚網站，導致民眾財物損失或個資外洩。（圖片來源：截自民視新聞，https://youtu.be/vvNP8WPxIIY；LINE@ 生活圈，http://at-blog.line.me/tw/archives/75713444.html）

LINE 潛藏風險

總結上述各項議題，我們得知 LINE 本身存在許多資安風險，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

1. 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。

2. 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。

3. 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。

4. 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

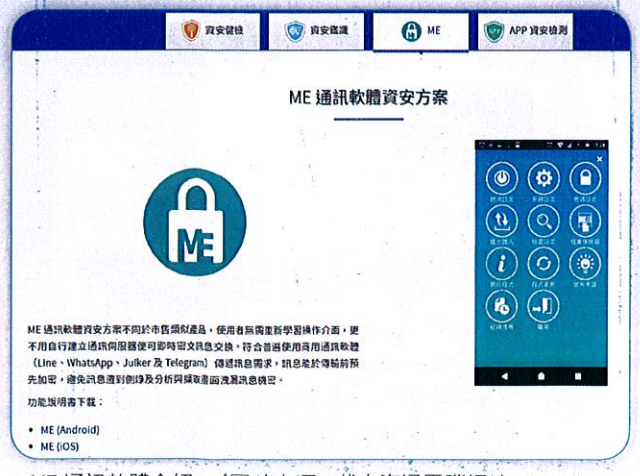
1. LINE 可隨意轉貼及點選任何網址，若是該網址潛藏惡意代碼，手機極可能被植入惡意程式，導致機敏資訊遭竊。

2. 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。

風險防制

一、安裝訊息加解密軟體

若 LINE 群組人員欲傳送公務資料，請務必安裝第三方加解密軟體，例如資通電腦與國家中山科學研究院研發之「ME 通訊



ME 通訊軟體介紹。（圖片來源：截自資通電腦網站，https://www.ares.com.tw/products/ncsist/?_ga=2.250067718.1418945601.1549964666-605880405.1549964666#lineme）

軟體」，透過該軟體對訊息、檔案加密後，再以 LINE 傳送，避免訊息誤傳或訊息遭他人擷取之資安疑慮。

二、「LINE」群組中建立管理人員

透過設定群組管理人，可統籌管理群組成員，必要時可將不適合人員踢出群組，以確保該群組談話內容不外流。

三、持續更新 LINE 版本

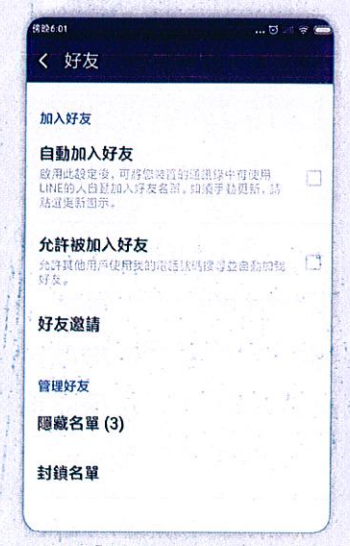
LINE 近年持續進行「資安漏洞回報獎金計畫」，用於挖掘軟體漏洞等各項缺失，並於後續版本中修補漏洞，故當 LINE 跳出新版本（電腦版）要求更新時，務必持續更新，避免遺留漏洞給駭客趁機攻擊。

四、安裝防毒軟體

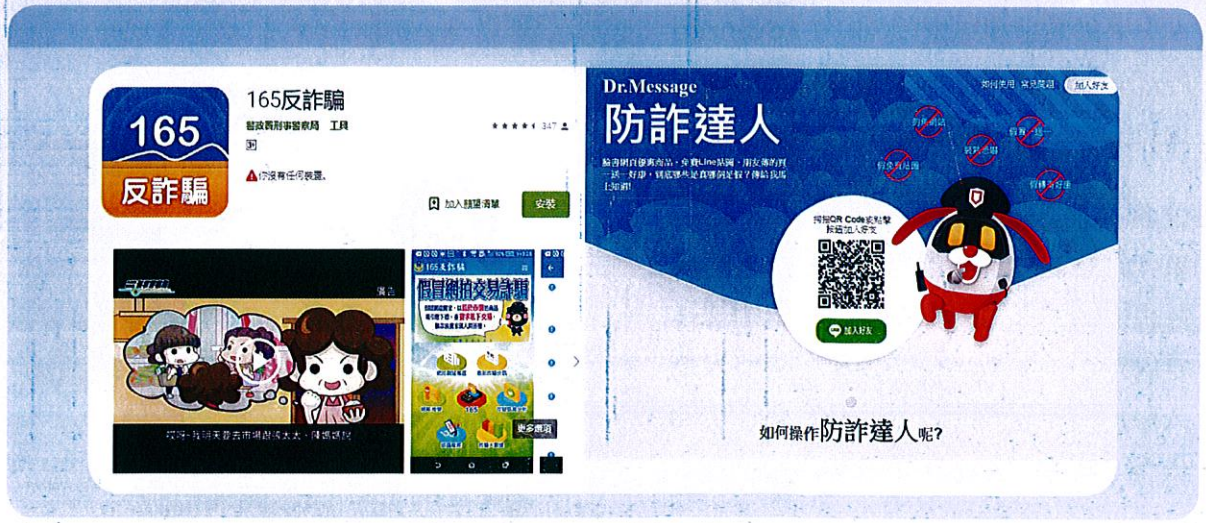
由於 LINE 可傳送各項超連結網址、檔案、圖片等，甚至許多使用者亦安裝 LINE 電腦板，往往給駭客可趁之機，誘騙使用者下載檔案、開啟連結，最終再植入木馬程式。因此若加裝防毒軟體，就可讓防毒軟體進行初步篩選，降低中毒機會。

五、不隨便加好友、加官方帳號

不隨意加陌生人為好友，可點選 LINE「設定」中的「好友」設定，關閉「自動加入好友」、「允許被加入好友」功能，即可避免被色情業者、陌生人士誘騙。另網路上常常充斥各種假官方帳號，建議可利用「趨勢防詐達人」、「刑事局 165 APP」，先查證該帳號是否為「官方正版」後再加入。



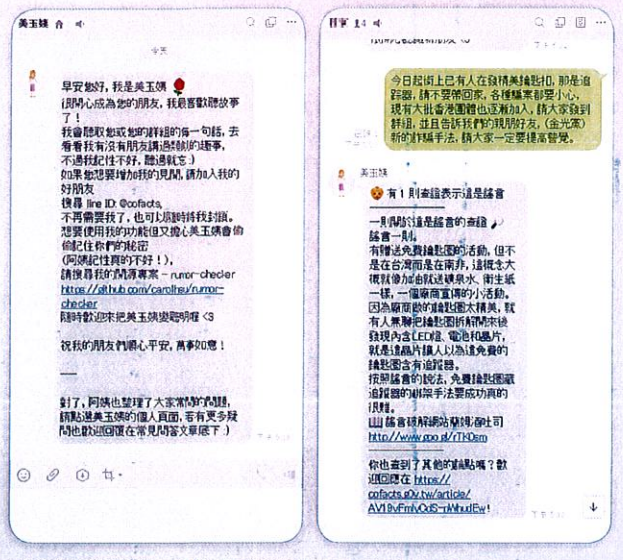
LINE「好友」設定。



刑事局 165 反詐騙 APP 和趨勢防詐騙達人。（圖片來源：Google Play，https://play.google.com/store/apps/details?id=tw.gov.cib.app.fraud165&hl=zh_TW；趨勢科技防詐騙達人網站，https://www.getdr.com/）

假訊息防制

雖然坊間已有不少假訊息查證平台，像是 LINE 帳號「真的假的」、網站「MyGoPen」等，但迄今最方便、最受歡迎的查證管道，當屬「美玉姨」LINE 聊天機器人。使用者僅需將「美玉姨」加入聊天群組，即可以提問方式丟出訊息，讓「美玉姨」直接查證該訊息是否真實；惟「美玉姨」系採擷取使用者訊息並傳送至資料庫查詢運作方式，公務群組若加入「美玉姨」恐有資料外洩之虞。



LINE「美玉姨」及謠言查證結果。

結論

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，我們也要明白使用 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。

公務機關透過 LINE 增進行政效率的同時，務必考量 LINE 的安全性。圖為臺北市政府針對 LINE 之使用，所訂定的參考指引。（圖片來源：臺北市政府資訊局，https://doit.gov.taipei/News_Content.aspx?n=6CB3401DAD37F659&s=3284900CC421A8E1）