張貼日期：2021/07/29

【資安攻擊預警】強化通訊軟體Line安全性建議，供參考運用。

主旨：【資安攻擊預警】強化通訊軟體Line安全性建議，供參考運用。

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202108-0112
  - 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，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，以降低機敏資訊遭外洩之風險。技服中心提供防護建議以強化通訊軟體Line安全性，供各機關參考運用，詳見建議措施。另重申，為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。
- 影響平台：
  通訊軟體Line
- 建議措施：
  檢視Line帳號安全性，請執行下列步驟：
  1. 請至Line app主頁→設定(齒輪)→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。
  2. 請至Line app主頁→設定(齒輪)→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點檢視【登入中的裝置】。
  3. 請至Line app主頁→設定(齒輪)→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，並執行第4點。
  4. 請至Line app主頁→設定(齒輪)→我的帳號，將【允許自其他裝置登入】設定為關閉。

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20210729_01

Last update: **2022/08/08 09:58**