IT 公海(香港資訊科技同路人)主題 Brainstorm大會

第一屆. 29 May 2020 - 1 June 2020

主題： 如何提升 Telegram Group / Channel Administrator 安全程度?

網路科技日益進步，不法份子經常在網路上盜用他人身份作出不當行為。作為本港資訊科技業界的一份子，我們致力提希望能提升大眾對於網絡安全的認知。因為，本周我們以網路安全作為主題，希望引起大眾討論及關注，在日後能更有效地保護個人資料。

在編寫、討論及或結論等等的會議過程中，任何與會者均以學術研究的前提下展開相關討論; 當中並沒有鼓勵、鼓吹及煽動、構成、引導或誘導他人作出任何違法行為。任何人以此文本的任何名義作一切違法及或犯罪的行為均與任何與會者無關。

在此感謝所有熱心義工及參與討論之人士。

討論內容整理

問題拆解

Telegram group/ channel administrator 面對的安全問題可分為三點：

- Keep anonymous (保持匿名)
- Secure data (保護資料)
- Emergency delete (緊急刪除)

常見錯誤

常見的錯誤（詳細內容及解決方法參見附件1 ）可分為6大層面，包括：

- 身份隔離
- 硬件安全
- 軟件安全
- 網絡安全
- 資料安全
- 人為漏洞/滲透性攻擊

建議解決方法

- 針對常見錯誤加強教育
- 修改目前Telegram Client 推出更符合安全標準的版本
  - 參照常見錯誤的解決方法，在部分安全設定更改預設值 / 關閉安全度低的選項
  - 可加入multiple profile 等功能
  - 但技術要求及開發成本較高
- 針對需求推出用以管理group/ channel 的開源系統
  - 此點有關於安全性，信任問題的爭議討論

1. 身份隔離

抗爭的過程中難免會遇上不少「別有用心」的人士意圖或企圖入侵你的手機。 因此作為群組管理員，又應該如何避免呢？

• 社運帳戶及私人帳戶分開
• 加密檔案
• 不要與他人共用手機
• 不錄音、不錄影、不影相
• 使用匿名 SIM 卡

2. 硬件安全

盡力確保你的個人硬件安全，當中包括:

• 盡量不要使用「中國品牌」的硬件
• 把重要設備留在安全的地方，切勿帶往高危地方
• 使用防偷窺螢幕防護貼
• 將 SIM 卡加密
• 切勿隨便使用街上提供的 USB 線; • 或 不要使用來路不明的 USB 存儲器或電線

3. 軟件安全

盡力確保手機上的安全做法如下:

• 不安裝中國的「流氓軟件」
• 不要打開 「全球定位 (GPS)」服務
• 正確的手機私隱設定
• 不要連接公共 Wi-Fi (包括政府 Wi-Fi)
• 定期更新軟件

4. 網絡安全

網絡安全是現今社會缺一不可的意識之一，其中建議方法:

• 使用「雙因素認證」(Two-Factor-Authentication, 2FA)
• 使用更好的密碼格式作為密碼
• 使用 VPN 及或 TOR

5. 資料安全

除了你手機的安全設定之外，也要注意你的個人資料或儲存的敏感資料，亦可能沒有做好保護而被別人盜取後，輕易讀取。防護措施包括:

• 開設硬碟加密
• 使用更好的密碼格式作為密碼
• 定期清理手機內存
• 關閉 itunes 或 Android 開發人員功能(Debug mode)
• 切勿「越獄」(jail-break) 或及刷取權限等破壞手機安全行為

6.「社交工程」漏洞/滲透

「社交工程」是常見的針對個人社交的層面上，進行資料套取。建議保護方法如下:

• 保持警覺，時刻注意人身安全
• 任何場合，切勿透露任何個人資料
• 不要打開任何可疑的連結(網址)、檔案或任何縮短的網址
• 在不同的網上平台使用不同的密碼
• 不要使用太多的「口頭禪」，以免被別人找到了個人的相近點

附件 2. 第一日與會會議記錄 (重點) • 會議提出的議程問題

- **Avoid being identified (phone, name, ip etc)** (如何避免身份洩露 **?)**

- **Protect data after being targeted** (如何在被發現身份後，保護個人(所有) 資料 **?)**

- **Damage control after being arrested** (如何在被捕後，保證人身資料安全及正當地使用 **?)**

• 問題 **1 – Avoid being identified** 的討論

▪ 與會者列出相關問題 (整合與節錄)

問題類型	問題要點
身份隔離	1. 沒有在安全情況下，把拍下的相片直接上載至群組 2. 「個人帳戶」與「私人帳戶」容易混淆或不清楚 3. 使用個人電話號碼開設帳戶
硬件安全	1. 與他人使用同一部手機 2. 使用「中國品牌」的硬件 3. 沒有使用防偷窺螢幕防護貼 4. 手機 SIM 卡沒有加設密碼保護

軟件安全	1. 電腦安裝及或使用中國的「流氓軟件」 2. 打開了手機的「推送通知」及或 「全球定位 (GPS)」服務 3. 使用網頁版的 Telegram， 但瀏覽器安裝及或使用「中國製造」的 plugin (外掛程式)
網絡安全	1.Telegram 上沒有使用「雙因素認證」(Two-Factor- Authentication, 2FA) 2.忽略了 Telegram 的私隱設定 (privacy setting) 3.使用了「弱密碼」作為密碼 4.沒有使用虛擬私人網絡 (Virtual Private Network, VPN) 及或 TOR (匿名通信軟件) 5.VPN 沒有「停止開關」(Kill Switch) 導致洩露了 IP 位址 及或 DNS (Domain Name System) 6.亂按陌生連結， 例如: 縮短網址 (shorten link)

資料安全	1. 沒有進行「硬碟加密」(Disk Encryption) 2. 手機使用的密碼太弱 3. 沒有定期清理手機內存空間
人為漏洞/滲透性攻擊	1. 分享連結及或圖片時，不小心洩露了 ID (fbclid/igshid) 2. 在「公海」群組內曝露了個人資料 3. 在不同的網上平台使用相同的密碼 4. 個人說話的「口頭禪」

附件 2.(續) 第一日與會會議記錄 (重點)

- 與會者列出相關問題的初步解決方案 (整合與節錄)

問題類型	解決問題要點
身份隔離	1.使用獨立的手機把相片上傳 2.購買外國的 SIM 卡，使用匿名 SIM 卡登記電郵及或帳戶(用作收發短訊或認證) 3.不使用私人手機及或與他人共用手機 4.不錄音、不錄影、不影相 5.檔案使用加密等方式隱藏，必需經後期製作才可輸出
硬件安全	1. 不要使用「中國品牌」的硬件 2. 把重要設備留在安全的地方，切勿帶往高危地方 3. 使用防偷窺螢幕防護貼 4. 將 SIM 卡加密

軟件安全	1. 不安裝中國的「流氓軟件」 2. 不要打開「推送通知」及或 「全球定位(GPS)」服務 3. 定期更新軟件 4. 正確的手機私隱設定
網絡安全	*1.* *第一日議後待議 2. 使用更好的密碼格式作為密碼 3. 使用 VPN 及或 TOR *4.* *第一日議後待議
資料安全	1.開設硬碟加密 2.使用更好的密碼格式作為密碼 3.定期清理手機內存 4.關閉 itunes 及或 Android debug mode 5.切勿「越獄」(jail-break) 或及刷取權限等破壞手機安全行為
人為漏洞/滲透性攻擊	1. *第一日議後待議 2. *第一日議後待議 3. 在不同的網上平台使用不同的密碼 4. 不要使用太多的「口頭禪」，以免在其他社交平台上又有類 近的言語，被別人找到了個人的相近點

附件 3. 第二日與會會議記錄 (重點)

• 與會者提出的問題與討論 (節錄) ▪ * **Day-2** 新增的解決方法

問題類型	**Day-2** 提出的解決問題要點
身份隔離	**1.**使用獨立的手機把相片上傳 (**已更換為第 6 點**) **2.**購買外國的 SIM 卡，使用匿名 SIM 卡登記電郵及或帳戶(用作收發短訊或認證) **3.**不使用私人手機及或與他人共用手機 **4.**不錄音、不錄影、不影相 **5.**檔案使用加密等方式隱藏，必需經後期製作才可輸出 **6.***將社運帳戶及私人帳戶分開使用 (e.g. 不要使用 VPN 連線至銀行戶口)

硬件安全	1. 不要使用「中國品牌」的硬件 2. 把重要設備留在安全的地方，切勿帶往高危地方 3. 使用防偷窺螢幕防護貼 4. 將 SIM 卡加密 5. *切勿隨便使用街上提供的 USB 線/不要使用來路不明的 USB 存儲器或電線
軟件安全	1. 不安裝中國的「流氓軟件」 2. 不要打開「推送通知」及或 「全球定位(GPS)」服務 3. 定期更新軟件 4. 正確的手機私隱設定 5. *不要連接公共 Wi-Fi (包括政府 Wi-Fi)

網絡安全	1. *開啟 2FA (**Day-2 議後決議**) 2. 使用更好的密碼格式作為密碼 3. 使用 VPN 及或 TOR *4*. 第二日仍議後待議
資料安全	1.開設硬碟加密 2.使用更好的密碼格式作為密碼 3.定期清理手機內存 4.關閉 itunes 及或 Android debug mode 5.切勿「越獄」(jail-break) 或及刷取權限等破壞手機安全行為

人為漏洞/滲透性攻擊	1. *保持警覺，時刻注意人身安全 (**Day-2** 議後決議) 2. *任何場合，切勿透露任何個人資料(**Day-2** 議後決議) 3. *不要打開任何可疑的連結(網址)/檔案/任何縮短的網址 4.在不同的網上平台使用不同的密碼 5.不要使用太多的「口頭禪」，以免在其他社交平台上又有類 近的言語，被別人找到了個人的相近點 6. 6.

附件 3.(續) 第二日與會會議記錄 (重點)

• 事件分享與討論

▪ 有一位與會者提及，當年有人使用了 Web 版 (Telegram ?) 使用了 VPN 及 Tor network，並且使用了 bitcoin 交易，結果毒販頭子直接去買家家中交收。

• 問題 **2 - Protect data after being targeted** 的討論 ▪ 與會者提出的問題與討論 (節錄)

問題/問題分類	解決方法
資料保護 (Secure data)	1. 自動化刪除訊息 2. 使用非實名購買 (非合約) 手機及或行動網絡數據 (mobile data) 卡 3. 定期掃描手機是否安裝了來路不明的應用程式
資料刪除處理 (Emergency delete)	1. 刪除任何與抗爭不相關的資訊 2. 除去群組管理員權限
匿名身份 (Keep anonymous)	1.利用 Telegram Bot (機械人) 接收資訊 2.不要使用 (Telegram ?) call 3. 自動化刪除訊息 4. 不要洩露任何可識別個人身份的資料

附件 4. 第三日與會會議記錄 (重點)

- 與會者提出的問題與討論

會議議題/問題/問題分類	內容
展開新 IT project	▪ 有與會者討論展開新 project ▪ 有與會者表示寫 client 是比較容易「更易改善安全設定」
資料加密	▪ 討論資料加密問題
管理 Telegram	▪ 討論使用 User-bot 去管理 Telegram group 等 ▪ 新的管理 (建議) 方法: ▪管理員控制 Web service/forward bot ▪ 管理員需要相信 (可依靠?) 的 (網絡?) 主機 ▪ 需要較難去編輯 (edit) 或轉發(forward) ▪Web service/forward bot 管理 telegram channel • ▪ ·需要 user-bot 建立 channel • ▪ ·或有機會違反了 telegram TOS (Terms of Service) • ▪ ·若 Telegram 封鎖該帳戶將會影響相關的 channel

會議議程問題 _____	• 有與會者表示，若在不更換系統情況下，會議議程差不多完成 • 有與會者表示，希望是次會議的思路是「提升安全及全面推廣」
怒剷 Telegram 方法	• 有與會者表示，若在不信任 Telegram 的情況下，倒不如直接 uninstall telegram
Tor 亦非可完全信任	• Exit node 問題