



網絡安全攻略

手機應用程式安全貼士



安裝流動保安軟件

- 手機平台危險度其實比電腦更高
- 選擇知名度高的流動保安軟件
- 安裝前多做功課，多看不同的用戶評價，以及不同人仕編寫評測
- 保安軟件必須由程式原作者官方網站、蘋果 Appstore 或 Google Play Store 下載
- 避免選擇不知名廠商平價手機



只從可靠來源下載應用程式

- 市面上每一個手機平台都有一個正式的 App 下載市場

- 蘋果 Appstore



- Google Playstore



- Microsoft Windows Phone Store



- Android App 可分開下載 APK 安裝，國內亦有多個 App 助手，可幫你下載及安裝不同 Apps，但 APK 是否還安全則成疑問
- 獨立下載 APK 時，也應只從原作者官方網站下載較為安全

留意應用程式及 程式更新所需權限

- 每次下載新 App 前，最好先了解應用程式所需要的權限
- 更新時如 App 權限有所更改，亦應考慮權限變更是否有必要，再行決定是否更新



保護流動操作系統

- 必須設定啟動密碼
- 設定在非活動狀態時間內自動鎖定
- 更新操作系統至最新版本
- 盡量啟用遠端清除功能
- 加密敏感內容
- 在不需使用時將 Wifi 及藍芽功能關閉
- 別隨便安裝不知名、來歷不明軟件或遊戲
- 別 Root 機或 Jail-Break 操作系統



安全的網上 社交網絡活動



我在Facebook做什麼？

- 分享個人狀態
- 分享相片及影片
- 分享目前位置
- 分享朋友家人資訊
- 分享個人喜好
- 分享婚姻狀態
- 分享個人資訊如學歷及工作，甚至電話地址等等



誰在看你的Facebook Profile ?



- 黑客或者別有用心的賊人，可以透過以上你分享的資訊，推斷你的生活習慣，甚至發掘你的私隱
- 網絡欺凌事件，都可能是因用戶所分享的資訊作引起
- 使用社交網站，必須小心自己有否透露過多個人資料

提高網絡安全意識

- 網上交友必須小心謹慎，切勿向不認識的人透露過多個人資料
- 跟網友見面更應保持警惕，任何跟錢財有關的事宜都必須格外小心，外出時個人安全更加務必注意
- 小心設定好社交網站內的私隱設定
- 留意社交網站對私隱相關條例的更新
- 社交網站跟第三方網站的連接最好少用為妙，必須使用時，也必須確定你的個人資料，不會因為這些應用程式或網站而外流



使用雲端服務的良好作業

小心了解雲端平台上 檔案分享的相關設定



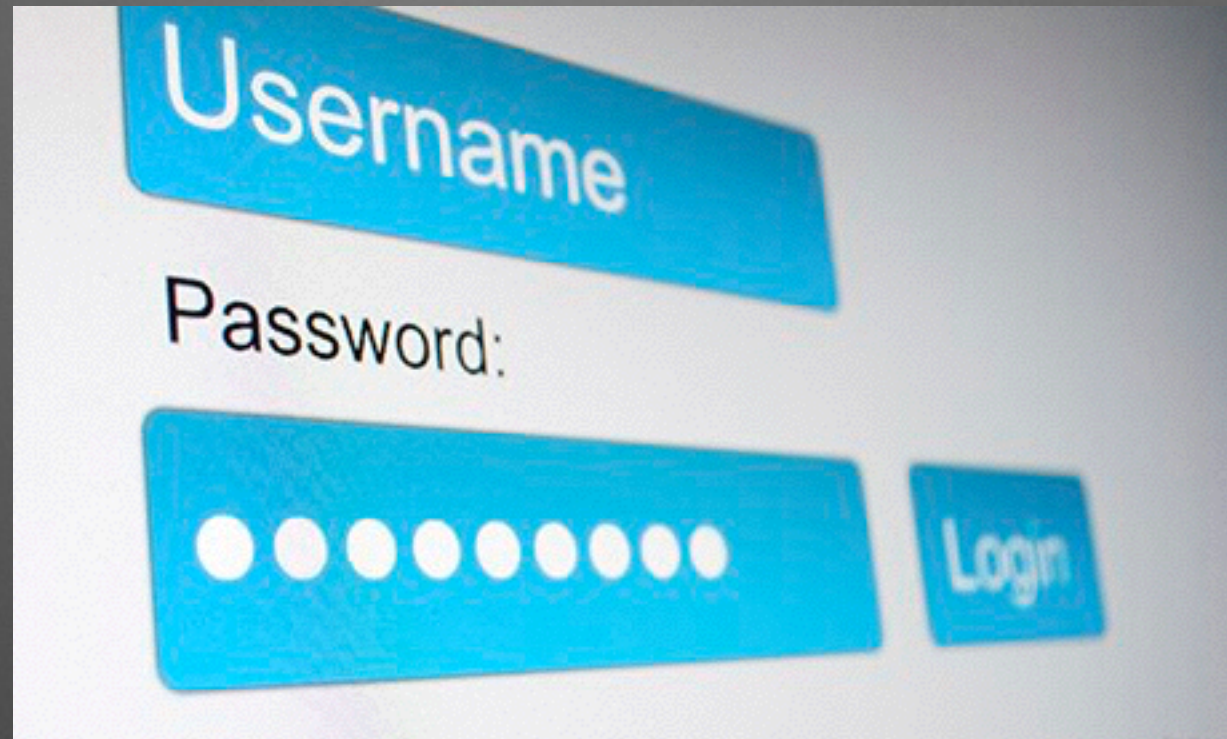
- 雲端平台的儲存服務其中一大賣點是：分享檔案十分方便
- 但這個功能亦很容易導致機密文件外泄，用戶必須詳細了解相關設定，在分享前確保設置恰當的權限
- 有部份雲端平台，設有分享自動過期的功能，建議大家最好使用這方法作出分享
- 如使用密碼分享，必須使用強密碼
- 所謂「強密碼」（Strong Password），一般是指包含英文大、小寫、數字和符號的8位以上密碼，才不易被破解 (例：ILuv2PlayB@dm1nt()n)
- 如使用 URL 分享，請留意有否被轉發而導致內容外泄

加密敏感資料



- 如果你會在雲端服務儲存敏感資料，最好使用第三方加密軟件，先將檔案加密，再作上存
- 這作法可以將雲端服務被黑客入侵或檔案外泄時，損失減至最少

雲端服務密碼管理



- 為雲端服務選用嚴謹密碼
- 在不同雲端服務及網站，使用不同之密碼
- 定期更改密碼
- 可使用密碼管理軟件產生的強密碼



保護家居網絡裝置





無線寬頻路由器
互聯網攝影機(IP Cam)
智能電視(SmartTV)
網路連接儲存設備
(Network Attached Storage)

買回來後記得更改密碼！

家居網絡安全須知

- 最好 SSID 也改甚至 Hidden
- 關閉不必要功能
- 不必使用時，將它們統統關掉，或設定時間制
- 經常保持操作系統更新
- 對外分享及管理功能，最好有需要時才開啟，其他時間都保持關閉
- 切勿隨便更新第三方 Firmware
- 定期更改密碼！





完