網路使用與手持式裝置的安全探討

講師　　呂守箴

大綱

- 網路使用的個資防護
  - 社群網站的詐騙手法與防範
  - 如何清除電腦裡不應該留存的資料
- 手機與平板式電腦的安全問題
  - 使用LINE聊天應注意的簡訊詐騙
  - 如何防範與安裝防毒APP
- 問題與討論

網路使用
的
個資防護

只要使用網路就有風險

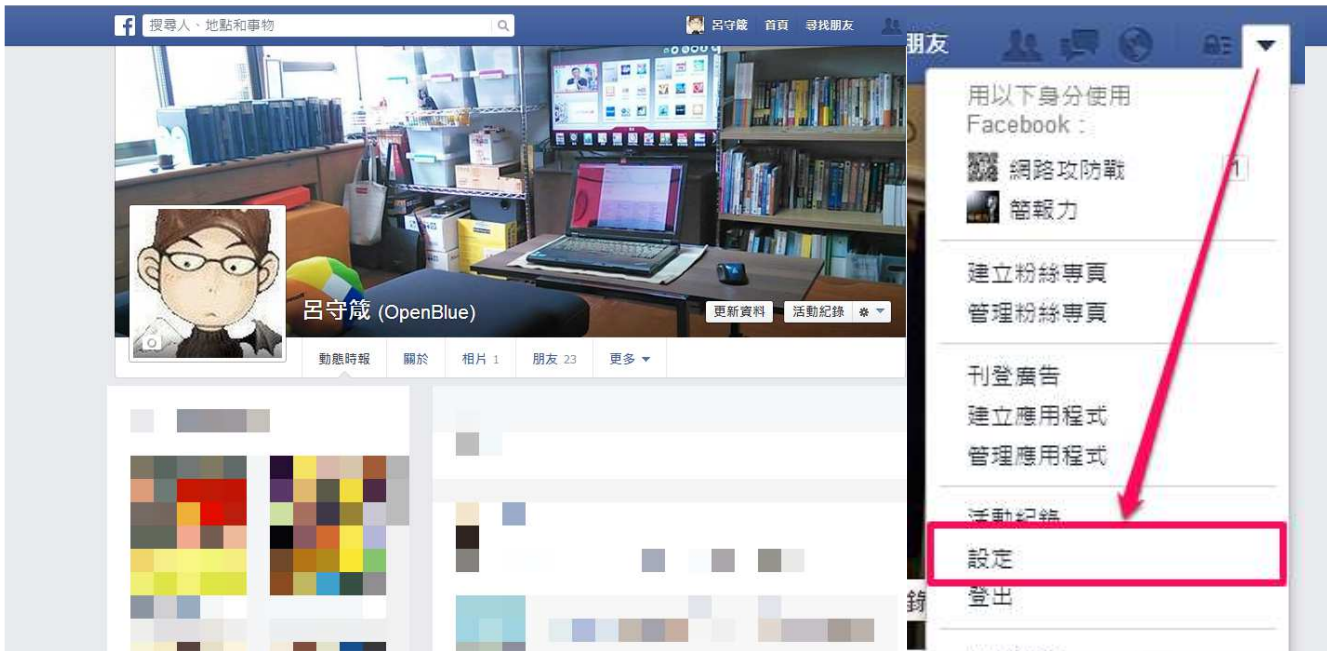
- 出門時一定要帶的東西@@
- 不管使用哪種裝置(電腦、手機、平板)只是使用網路(有線、無線、3G)就有可能連到惡意網站、下載到惡意程式。

手機防護

- 當使用者越來越仰賴iPhone、Android等智慧手機、平板電腦，單位的安全防護網將會面臨有別於傳統的新風險。
- 不只要防範鎖定手機伺機入侵的木馬和惡意程式，還得預防**遺失手機而導致資料外洩**的風險。
- 伴隨著手機進入單位的3G網路，更是輕易**跳過內網管制**的防線。傳統的防護網已經逐漸瓦解，單位必須正視行動應用帶來的新風險，才能有效鞏固防護網。

Facebook的帳號安全

- 點選首頁右上角，選『設定』



Facebook的帳號安全

Facebook的帳號安全

登入通知

當有人從你不曾使用過的電腦或手機進入你的帳號時，我們可以通知你。請選擇寄送通知方法：

- ☑ 電郵地址
- ☑ 簡訊 / 推送通知

儲存 取消

登入許可

☑ 要求 1 個安全密碼，讓我從未知的瀏覽器進入我的帳號 [?]

發送安全代碼：

- 發送簡訊至 0931
- 使用代碼產生器 [?] 移除
- 當你沒有隨身攜帶手機時，取得代碼以使用

儲存 取消

Facebook的帳號安全

通訊軟體

iOS

LINE

開發人員 NAVER Japan

開啟 iTunes 以購買和下載 Ap

Facebook

開發人員 Facebook, Inc

開啟 iTunes 以購買和下載 Ap

Android


中午12:52
設定
一般
安全性
隱私設定
動態時報與標籤
封鎖
通知
手機簡訊
追蹤者
應用程式
廣告
交易付款


中午12:52
安全設定
簡訊登入通知
電子郵件登入通知
登入許可開啟
登入許可代碼
第三方驗證器
信賴的聯絡人
信賴的聯絡人是每當你無法存取帳號時，可以安全地幫你恢復存取權的朋友。
應用程式密碼
認可的裝置 17
有效的連網。 11


中午12:52
設定
一般
安全性
隱私設定
動態時報與標籤
封鎖
通知
手機簡訊
追蹤者
應用程式
廣告
交易付款


中午12:53
你的人際關係鏈
誰可以看到我的東西？
誰可以查看你往後的貼文？
公開
限制你設定和「朋友的朋友」以及「公開」分享貼文的分享對象？
誰可以與我聯絡？
誰可以傳送交友邀請給你？
朋友的朋友
誰可以搜尋我？
誰可以使用你所提供的電子郵件找到你？
朋友
誰可以經由你提供的電話號碼搜尋你？
朋友
你希望其他搜尋引擎連結到你的動態時報嗎？
是

手機軟體定位：iOS

iOS **Android(不提供)**

手機軟體定位：Android

iOS(不提供) **Android**

手機與
平板式電腦
的
安全問題

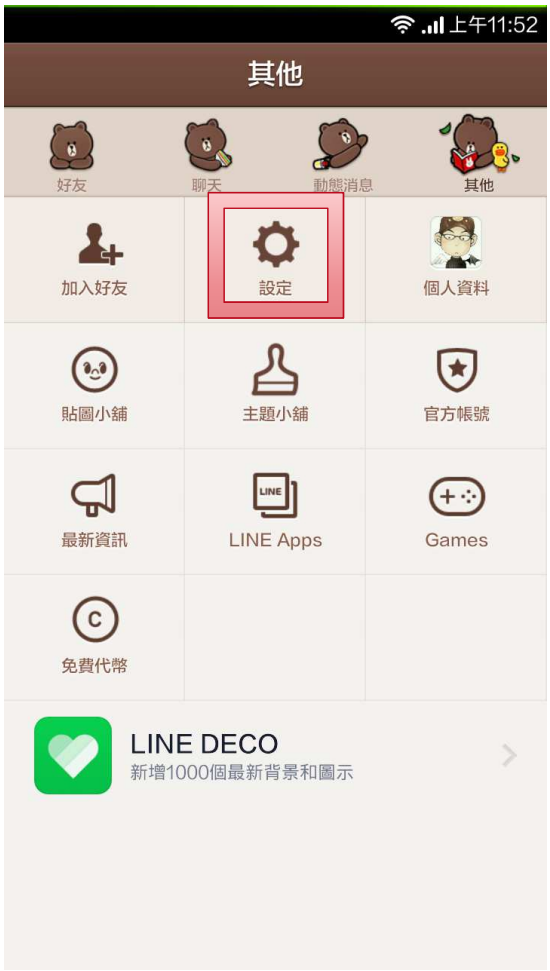
貪圖LINE免費貼圖卻洩漏個資？

- 既然免費為什麼不可以？
- 主要是收集使用者的 LINE ID 或電話號碼藉此發送”其它廠商”的廣告訊息。
- 被亂加入廣告群組，發送”無聊、色情、促銷”的簡訊通知。

評估風險再決定使不使用！

- 應該這麼說，這是一個跨國的企業、
- 韓國的公司、日本發行、台灣代理。

- 並非完全不能使用Line，而應該是說想用這種通訊軟體，就必須知道它的風險。
- 了解它所造成的影響再根據自己能接受的風險(被側錄、過濾、詐騙簡訊、違法貼圖)，再決定使不使用。
- 如同前一陣子討論公務機關到底開不開放使用MSN、雅虎奇摩即時通等通訊軟體一樣，需要事先評估資安風險。
- 註：Line 有提供『電腦版(桌面版)』可以安裝，也須評估資安風險。




晚上09:09
我的帳號
設定電子郵件帳號
設定已完成
電話號碼
+886 931 633
換機密碼
設定已完成
Facebook
解除
連動中的應用程式
允許自其他裝置登入
開啟本功能後，您將能自LINE的電腦版或WIN8版登入。


上午11:54
聊天・語音通話
預覽貼圖
您選擇的貼圖將在送出前放大顯示。
以Enter鍵傳送
設定後，按下Enter鍵即可傳送。
頁面顯示設定
自動變化顯示方向
聊天室頁面的顯示方向可設為直向 / 橫向固定
圖片的傳送畫質
標準
再度自動傳送
無法傳送的訊息於一定時間過後，將會再度自動傳送。
刪除所有聊天記錄
刪除聊天室內的檔案
開啟語音通話功能
若您關閉本功能，將無法接聽來電；
也無法接收未接來電的訊息。


上午11:54
好友
自動加入好友
實行日期：-
通訊錄的好友將自動加入好友名單。
如需手動更新，請點選更新圖示。
允許被加入好友
若其他用戶的通訊錄內有您的電話號碼，您將會自動被加入
該用戶的好友名單內。
隱藏名單
封鎖名單
ID
openblue
公開ID
公開後，其他用戶可利用ID找到您。


下午04:06
隱私設定
密碼鎖定
若您忘記密碼，必須先刪除LINE，再重新安裝。
請留意：您過去的聊天記錄將會被全數刪除。
公開ID
阻擋訊息
開啟本功能後即可阻擋不是來自好友的訊息。
更新行動條碼
刪除所有聊天記錄

LINE 防毒軟體：

iOS

- 因 APPLE 公司軟體管控政策，所以**不提供**！

Android

來電辨識與封鎖：

iOS **Android**

- 因 APPLE 公司軟體管控政策，所以**不提供**！

其實最好不要用(可惜大多數人辦不到)，那麼要用就要先學保護自己的方法。

- Line 台灣官方「問題反應表」：
- https://line.naver.jp/cs/zh-hant/

- 說明：
- Line帳號被盜的情況頻傳，甚至衍生出詐騙案件，經過刑事局和Line公司協調之後，基於打擊犯罪的共同目標，即日起民眾可以透過Line問題反應表的連結，就可以立刻請求 LINE 公司處理，同時讓被害人拿回原帳號。

Android作業系統平台

- Android 是一種以Linux為基礎的開放式原始碼作業系統。
- 它由Google公司收購後與開放手持設備聯盟開發和主導。
- 目前尚未有統一的中文名稱，常見為：安卓、安致、安桌椅等稱呼。
- 安全問題：
  - Android 作業系統：例如：版本衝突、核心程式漏洞等
  - Android Market (Google Play)線上應用程式商店：例如：不安全、竊聽程式等。

行政院消費者保護會
Consumer Protection Committee, Executive Yuan

進階搜尋

關於我們 政策與法令 消費資(警)訊 申訴調解 教育宣導 疑難解答 諮詢窗口 主題服務 資訊服務 相關連結

首頁 > 消費資(警)訊 > 消費資(警)訊

消費資(警)訊

公布智慧型手機資安檢測結果！(行政院消費者保護處)

日期：103-07-07

為維護消費者權益，行政院消費者保護處（下稱行政院消保處）針對HTC New One、Samsung Note 3、Sony Xperia Z等三款暢銷智慧型手機進行資安測試，測試結果發現HTC New One具有4項資安缺失(2項高風險，2項低風險)、Samsung GALAXY Note 3具有3項資安缺失(1項高風險，2項低風險)、Sony Xperia Z具有6項資安缺失(2項高風險，4項低風險)，經行政院消保處通知業者已請業者全數改善完畢。

在現今人手一機的時代，您了解智慧型手機內內建智慧型軟體的隱私是否會遭有心人士竊探嗎？行政院消保處為了解智慧型手機內建搭載軟體之安全性，市購HTC New One、Samsung Note 3、Sony Xperia Z等三款智慧型旗艦手機，並委託國內唯一具專業資安測試能力的財團法人資訊工業策進會資安科技研究所進行檢測，檢測標準則參照國際知名資安組織所發布常見的行動裝置十大資安漏洞(「OWASP Top 10 Mobile Risks」)之測試內容為主，檢測標準則參照國際知名資安組織「OWASP Top 10 Mobile Risks」與「SANS: CWE/SANS TOP 25 Most Dangerous Software Errors」之測試內容為主，測試結果發現該3款手機具有如下資安疑慮缺失(詳細檢測結果如附表)：

(一) HTC New One：

1、手機上之筆記應用程式資料缺乏更嚴謹的保護措施，造成機敏資料有外洩之虞。高風險部分：使用者筆記內容以明文儲存且讀取權限設置不當，造成機敏資料有外洩之虞。

2、「Wi-Fi熱點」與導航應用程式密碼以明文方式儲存與傳輸，可能遭到竊取，用以上網。低風險部分：導航應用程式Ndrive註冊時，使用者帳號密碼以明文方式傳輸及應用程式「Wi-Fi熱點」密碼以明文方式儲存。

（二）Samsung GALAXY Note 3：

1、手機上之筆記應用程式資料缺乏更嚴謹的保護措施，造成資料有外洩之虞。高風險部分：使用者筆記內容以明文儲存且讀取權限設置不當，造成機敏資料有外洩之虞。

2、應用程式網路加密連線機制缺乏更嚴謹的驗證機制，可能導致使用者連線至惡意網站而遭到攻擊。低風險部分：應用程式以SSL加密連線至網站時，未驗證憑證是否簽發給連線網站，可能使應用程式因故被導向至釣魚網站時。

手機APP(應用程式)開發商

- Android 作業系統是完全免費開放的，任何廠商都可以不經過Google和開放手持設備聯盟的授權隨意使用。
- 之後推出 Android Market (Google Play)線上應用程式商店，使用者可在該平台上尋找、購買、下載及評分。
- 第三方軟體開發商和自由開發者則可以在Android Market (Google Play)上不需事先審核並自由發佈其開發的免費或付費APP應用程式。

手機防護：Android

- 解決策略：
- **不安裝** “來路不明” 的小遊戲或軟體
- 移除不需要或不常用的小遊戲或軟體
- 安裝 Android 防護程式
- 採用 ASEF針對惡意APP分析檢測

Android 防毒軟體

- 智慧型手機功能日益強大，就像是隨身帶著走的小型電腦。
- 功能越多、效能越強，加上手機內存有大量個人相關資訊，後果就是惡意軟體的出現。加上Android系統的開放態度，能夠安裝非Google Play應用程式集裡的程式，使得惡意軟體更容易隨著程式侵入手機/平板。
- Google雖然在Android 4.2之後新增了驗證應用程式功能，在安裝時能夠自動掃描檔案，但似乎偵測率不佳，還是需要依賴第三方程式來幫忙。

行動安全防護 – 全民版

iOS **Android**

iOS 作業系統平台

- iOS是由蘋果公司獨家開發的封閉式作業系統。
- iTunes是一款媒體播放器的應用程式，用來播放以及管理數位音樂和與視訊檔案。
- QuickTime是由蘋果電腦所開發的一種多媒體架構與程式。
- 安全問題：
  - iOS 作業系統：例如：版本衝突、核心程式漏洞等
  - App Store 線上應用程式商店：例如：不安全、竊聽程式等。

手機防護：iphone /iPad

- 解決策略：
- **不安裝**“來路不明”的小遊戲或軟體
- 移除不需要或不常用的的小遊戲或軟體
- 安裝iOS防護程式
- 使用“原裝”不要越獄或破解

iphone最容易感染的環境：
1. 越獄(JB, Jailbreak)過
2. 安裝了 SSH 且沒有更改預設密碼
3. 喜好在  App Stone搜尋安裝軟體

APP 軟體更新

- 不管是”Android”還是”iOS”作業系統，由於APP軟體都會有瑕疵，會引起當機、中毒、漏洞，所以都需要做 APP 軟體更新。
- Android 透過→Google Play 來更新。

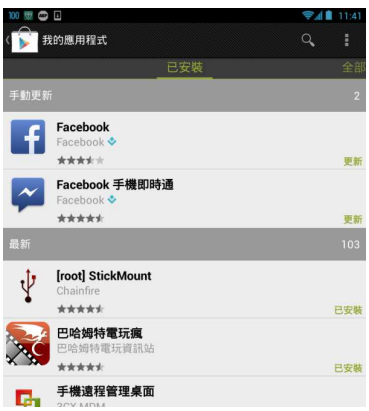
- iOS 透過 → App Store 來更新。

APP 軟體更新

Android

- 點選

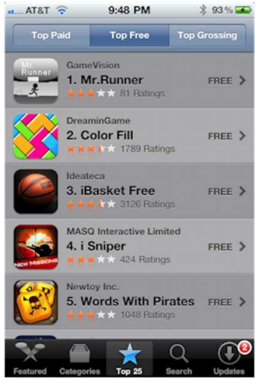
- 下載”更新”



iOS

- 點選

- 更新”Updates”



結論

- 網路使用的個資防護
  - 社群網站的詐騙手法與防範
  - 如何清除電腦裡不應該留存的資料
- 手機與平板式電腦的安全問題
  - 私人手機成行動安全管理的問題
  - 2大手機系統平台的安全性
  - 如何防範與安裝防毒APP
- 問題與討論

- 講師： 呂守箴
- E-Mail：shoujen@gmail.com

- 網路攻防戰：
- 部落格：http://anti-hacker.blogspot.com
- FB粉絲團：https://www.facebook.com/NetWarGame
- G+專頁：https://plus.google.com/u/0/118062628172252352420

- Youtube影片頻道：http://www.youtube.com/user/openblue
- 網路直播頻道：http://zh-tw.justin.tv/openblueTV