桃園市瑞埔國小 教師研習
資安宣導活動

宣導單位：瑞埔國小教務處
宣導日期：107年5月09日

什麼是資訊安全?

資訊安全的現況

一

駭客利用假郵件、假連結、假網頁、假APP、假WIFI等方法，針對敏感資訊的單位量身訂製攻擊手法

二

駭客攻擊目標常鎖定政府施政之重要部門(如:保防、特勤、外交、兩岸事務)或金融機構

三

勒索軟體竄起，且蔓延至行動裝置

四

惡意連結簡訊、通訊軟體詐騙訊息...等攻擊增加，行動裝置病毒更氾濫，費用詐欺成為新威脅

資安最弱的一環

利用資安最弱的一環攻擊：人

隨著防護產品的佈建，對惡意攻擊的嚇阻可達一定的成效。

但是”人”的因素，往往是資安環節最弱的一環

人的因素

扯！違規單洩個資 檢舉人名、電話全都露

用APP軟體追劇，看片同時個資同步看光光

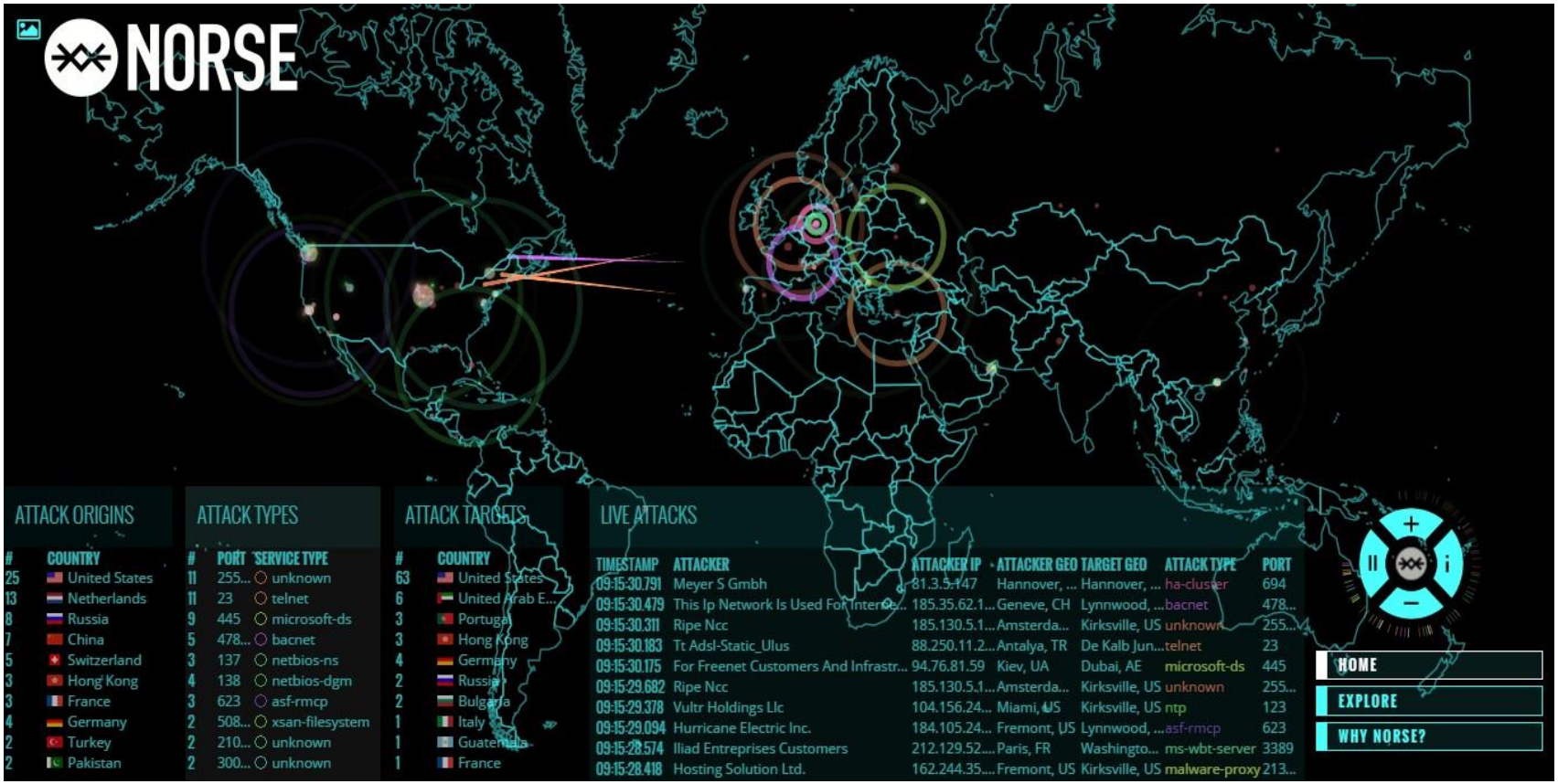
「衣芙日系」個資遭駭　客戶被詐505萬

「衣芙日系」被駭 個資外洩事件

一	網站遭駭客入侵，盜取客戶資料，轉賣給詐欺集團
二	詐騙集團竄改網站客服中心的電話，因此買家打電話，會轉到假的客服中心
三	人員謊稱訂單錯誤要重新操作，進而行騙
四	四個月下來，多達38人被騙，得手505萬

Facebook 癱瘓！伊斯蘭駭客 Lizard Squad 聲稱發動攻擊

2015年1月27日下午，全球的 Facebook 出現大當機，將近一個小時的時間不只 Facebook 無法登入，就連 Instagram 也跟著癱瘓。就在癱瘓同時，知名駭客 Lizard Squad 在 Twitter 上寫下留言，聲稱這起事件是他們幹的。



真假網址?!


Facebook
fbme-setting-protection-system.hol.es/login.htm
facebook
注意網址！
Facebook 登入
臉書假官網
惡意竊取帳密個資

新型態社交工程威脅-手機簡訊

詐騙集團手上已經握有一份超過十萬人的名單（包含姓名、手機號碼），透過簡訊發送功能，把你的姓名加上一串隨機問候語，還有一個惡意鏈結，包裝後用簡訊方式寄送給所有名單上的使用者。收到的人不疑有他（上面有你的名字，看起來很像是朋友傳來的簡訊），點擊簡訊裡的惡意鏈結，會自動下載惡意程式 APK 檔，手機就會「中毒」！

公共 Wi-Fi 駭客是這樣用的

駭客行動四部曲

一	讓人們主動連接到偽造的網路中
二	竊取他們的姓名、電子郵件帳號密碼
三	竊取他們的職業、愛好以及困擾(出售資料)
四	點選忘記密碼→至電子郵寄信箱截獲密碼

免費WIFI的風險

- 曾經有媒體報導一位女子在麥當勞門前舉牌抗議，表示其使用公開WIFI上網被銀行帳戶被轉走了2000元，那麼究竟是誰通過免費WIFI伸出了他的黑手呢？

- 例如：駭客通過搭建一個與公共WiFi很相近的名字，比如，模仿星巴克（Starbucks），搭建一個名為Starbucks01的WiFi熱點，不用登錄密碼，你就會在完全沒有察覺的情況下將掉落陷阱。

免費的真的免費嗎?

- 前行政院長張善政說，手機設定免費Wi-Fi就連結，有風險，手機不應設定免費Wi-Fi「閉著眼睛就連」，這設計不好，至少不要到處都可連

如何規避免費WiFi風險

一	謹慎使用公共場合的WiFi。要選擇也是官方機構提供的而且有驗證機制的WiFi，最好在連接之前與工作人員確認。
二	儘量使用僅需密碼或手機號碼+簡訊驗證方式的公共WIFI，如碰到需要提供更多的資訊進行註冊，那你就應該注意了。
三	使用公共場合的WiFi時，儘量不要進行網絡購物和網銀的操作，避免重要的個人敏感信息遭到泄露。
四	養成良好的WiFi使用習慣，手機會自動連接相同名稱的WIFI，所以在公共場合把WiFi調成鎖屏後不再自動連接，以保證手機不連接上來路不明的WIFI。
五	對於網路銀行、購物網站、社交軟體、支付寶、電子郵件等重要應用，定期更新密碼。

手機感染電腦 方式 -- 總結

惡意程式

Google play

1.使用者下載惡意APP

3.惡意程式竊取密碼;開啟麥克風竊錄環境音

4.被竊資料傳到手機

中毒電腦

2.使用者進行充電,手機惡意程式感染電腦

5.透過手機將資料傳到駭客的FTP

駭客

智慧型手機安全防護

- 手機設置密碼鍵盤鎖等防護措施。
- 不點選來路不明連結網頁。
- 不用相同帳密登入不同網站。
- 安裝手機防護軟體(如Avast、Dr.Web、AVG.....等)。
- 手機避免下載或安裝來路不明之安裝程式(非Google Play或App Store之軟體)。
- iPhone及iPad等iOS設備建議不要進行JB(越獄)操作
- 儘量避免離開視線或交由陌生人操作
- 充電儘量使用座充變壓器，避免連接電腦
- 不任意點選來路不明的簡訊超連結。
- 不理會陌生人的訊息(如LINE、Facebook...等)。

智慧型手機安全性設定-LINE

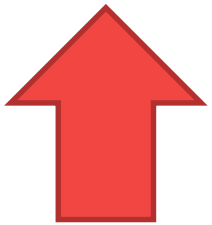
1. 關閉「公開ID」功能。
2. 若無使用電腦版 LINE，應關閉「允許自其他裝置登入」。
3. 定期更改密碼，設定換機密碼。
4. 關閉手機通訊錄「自動加入好友」、關閉「允許被加入好友」。
5. 開啟「阻擋訊息」，阻擋非來自好友之訊息。
6. 社群網站、軟體或免費信箱不使用同組帳號密碼。
7. 不在公用電腦登入LINE。
8. 不任意授權LINE 遊戲讀取你和好友的個人資料。

手機感染電腦-充電引起！

一	某單位向S業者申請技術支援
二	防毒有偵測到”偷密碼惡意程式”，但是清除或重灌後還是持續出現
三	現場發現多隻惡意程式 偷取IM密碼
四	推論是USB 感染，但是客戶確認沒有使用USB 隨身碟
五	確認有人借用電腦充電(手機USB連到電腦)

追查手機

- 手機:android 系統
- 檢驗最近三個月下載的App
- 發現有三個程式會與USB溝通
- 分析後確認存在有惡意行為的APP



抓到兇手了！手機中毒傳給電腦

如何防範網路勒索

國小資訊組

綁架惡意程式之危害-如何預防

- 備份檔案
- 對電子郵件、網站和應用程式（APP）保持戒心
- 使用防毒程式
- 時時安裝更新
- 絕不付贖金

兒少安全上網~師長的叮嚀


祝大家上網安全
安全上網