

臺東縣新興國民小學105年

資訊安全與智慧財產權宣導



教導處 關心您



尊重智慧財產權 人人有責

Please respect intellectual property rights

著作權四不一沒有

不要在網路上隨便免費下載音樂、影片、軟體
不要將他人文章、音樂、影片、軟體隨便轉寄
不要將他人的文章、照片隨便張貼或移花接木
不要將他人的流行歌曲或音樂拿來在部落格使用
沒有合法授權的著作不要在網路上販賣



▶ 違反個資法的罰則

民事責任

- ◎每人每一事件可求償 5 百元～ 2 萬元。
- ◎同一件事，最高可求償 2 億元。

刑事責任

- ◎最高可處 2 年以下有期徒刑、拘役或科或併科新臺幣 20 萬元以下罰金。
- ◎意圖營利，可加重求處 5 年以下有期徒刑，得併科新臺幣 1 百萬元以下罰金。

行政處罰

- ◎最高可處新臺幣 5 萬元以上 50 萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰。

資訊處理作業時應注意事項



- 密碼不可在便利貼在附近
- 人離開電腦要鎖定螢幕或登出
- 人離開桌面，敏感性紙本要先收好，不可隨便置於桌面
- 密碼不可太過簡單，最好有多組輪流定期更換
- 公務電腦一定要有資安防護軟體
- 不要在公務電腦安裝非法軟體，以造成系統漏洞
- 紙本敏感性資料，繕打錯誤或不用時一定要碎掉，不可變成資源回收品

密碼安全設定



- 密碼強度不足，使你危機四伏
- 剖析不良的密碼設定方式
- 密碼安全設定原則

密碼強度不足，使你危機四伏



- 簡單來說，帳號就像我們住的房子，而密碼就是大門的門鎖，如果帳號沒有設定密碼，就像未上鎖的大門，陌生人都可以輕易的進出，對安全造成極大隱憂！

密碼被暴力破解的實驗統計結果



| 密碼 長度 | 英文字母 (26 字元) | 英文字母+數字 (26+10 字元) | 英文字母大小寫 (52 字元) | 含特殊符號字元 (96 字元) |
|----------|-----------------|-----------------------|--------------------|--------------------|
| 4 | 0 | 0 | 1 分鐘 | 13 分鐘 |
| 5 | 0 | 10 分鐘 | 1 小時 | 22 小時 |
| 6 | 50 分鐘 | 6 小時 | 2.2 天 | 3 個月 |
| 7 | 22 小時 | 9 天 | 4 個月 | 23 年 |
| 8 | 24 天 | 10.5 個月 | 17 年 | 2287 年 |
| 9 | 21 個月 | 32.6 年 | 881 年 | 21 萬 9000 年 |
| 10 | 45 年 | 1159 年 | 45838 年 | 2100 萬年 |

千萬要避免的密碼設定方式



- 密碼與帳號相同
- 使用生日、身分證字號、英文名字等個人資料
- 使用公司、部門、單位名稱
- 使用與系統管理相關專有名詞（如admin、password等）
- 不設定密碼（空白密碼）
- 使用簡單字元組合（如1234、abcd、111111等）

密碼安全設定原則



- 不使用懶人密碼
- 長度與複雜度
- 密碼無明顯含義
- 避免重覆
- 定期更新

手機上網安全



- 手機實體安全防範
- **APP** 使用風險與安全建議
- 享受社群網路服務同時保護個人資料

幾個基本的手機實體安全小撇步



- 設定手機密碼保護手機
- 使用**PIN**碼保護手機**SIM** 卡
- 記下你的手機唯一識別碼 (**IMEI**)
- 安裝搜尋手機軟體

記下你的手機唯一識別碼 (IMEI)



- 每一個手機都有一個獨立的手機序號列，稱之為 **IMEI** 碼，相當於行動電話的身分證號碼。
- 通常可以在手機上輸入 *#06# 後即可以查詢自己手機的 **IMEI** 碼。
- 請記下你的手機 **IMEI** 碼，當你的手機被偷或遺失時，這組號碼是電信公司向警察單位查詢尋獲手機或贓機的辨識號碼，通常在失竊手機報案時，警察也會詢問你的 **IMEI** 碼。

APP 使用風險



- 智慧型手機、平板電腦等行動設備其實也是一種電腦，有處理器、記憶體與儲存空間，可以安裝各種軟體，能夠上網、玩遊戲和瀏覽影音等，因此也像一般電腦一樣可能存在惡意程式竊取你的資料，或偷偷執行其他動作。

手機病毒的危害



- 導致使用者資訊遭竊
- 傳播非法訊息
- 使手機無法運作

手機受病毒感染的癥狀



- 當你發現以下癥狀時，你的手機可能已經遭到惡意程式或病毒的感染了！
 - 電話帳單金額沒有任何理由地暴增。
 - 手機簡訊與電子郵件信箱的寄件備份中，出現你不曾寄出過的訊息或電子郵件。
 - 手機使用介面（如桌布、主題、手機桌面的擺設方式）突然自行改變。

只在信譽良好的網站中下載APP



- 建議只在像是Apple APP Store或Google Play Store 等作業系統業者所提供的APP交易平台下載。
- 避免透過手機的瀏覽器下載APP程式，因為從未知或不可靠的來源下載的程式有可能就是惡意程式。

安裝手機防毒軟體



- 手機也可以像電腦一樣安裝防毒軟體，當你透過安裝APP時，它會自動掃描檔案的安全性，避免惡意軟體竄入手機。
- **Sophos Mobile Security (Android系統)**

享受社群網路服務要保護個人資料



- 隨著社群網路滲透率提高，智慧型手機夾帶的3G行動上網優勢，降低了使用者對於社群網路服務的使用時間及地點上的限制，使得利用智慧型手機或平板電腦使用社群網路成為趨勢。
- 在缺乏充分的資安認知情況下用手機玩社群網路服務，很容易讓自己或親朋好友的重要資訊及隱私被竊取或曝光！

手機的社群網路應用個資保護



- 只接受你認識的朋友邀請
- 謹慎思考要張貼哪些資訊
- 幫朋友打卡與**Tag** 前，先取得同意
- 定期檢視你的隱私權設定

電子郵件威脅



- 夾帶病毒及惡意程式
- 社交工程
- 垃圾郵件

夾帶病毒及惡意程式



- 電子郵件是傳播電腦病毒、蠕蟲、木馬程式.....等惡意內容的常見管道。
- 若收件者不慎開啟夾帶有惡意程式的電子郵件，不但有可能造成
 - 系統資料毀損
 - 成為殭屍電腦而任由駭客擺佈其電腦
 - 造成整個內部網路服務的癱瘓
 - 部分電腦病毒甚至會關閉掃毒引擎，造成防毒功能失效等。

釣魚郵件



- 釣魚郵件的常見模式為網路詐騙者發送帶有偽冒網站超連結的電子郵件，引誘不知情者前往該山寨版的網站並輸入自己的帳號與密碼，因為山寨版網站的外觀與實際的官方網站十分相像，也讓其有機會剽竊受騙者的帳號密碼。

電子郵件安全小撇步



- 安裝防毒軟體，不安裝來源不明的軟體
- 更新軟體修補程式
- 不要啟用郵件的預覽窗格
- 辨識釣魚郵件四大重點

安裝防毒軟體



- 電腦安裝防毒軟體為最基本的病毒防護措施，除安裝防毒軟體外，並應下載及使用最新的病毒碼。

更新軟體修補程式



- 電腦系統與軟體通常在推出後，軟體開發業者會根據使用者所反映的意見，針對軟體的功能、效能、系統安全漏洞或錯誤等進行加強與修正，然後推出更新的軟體版本。
- 通常，軟體在進行更新之後在運作上會更為順暢，或者因為新功能的強化，使軟體變得更加好用。

注意郵件提供者的警示標語

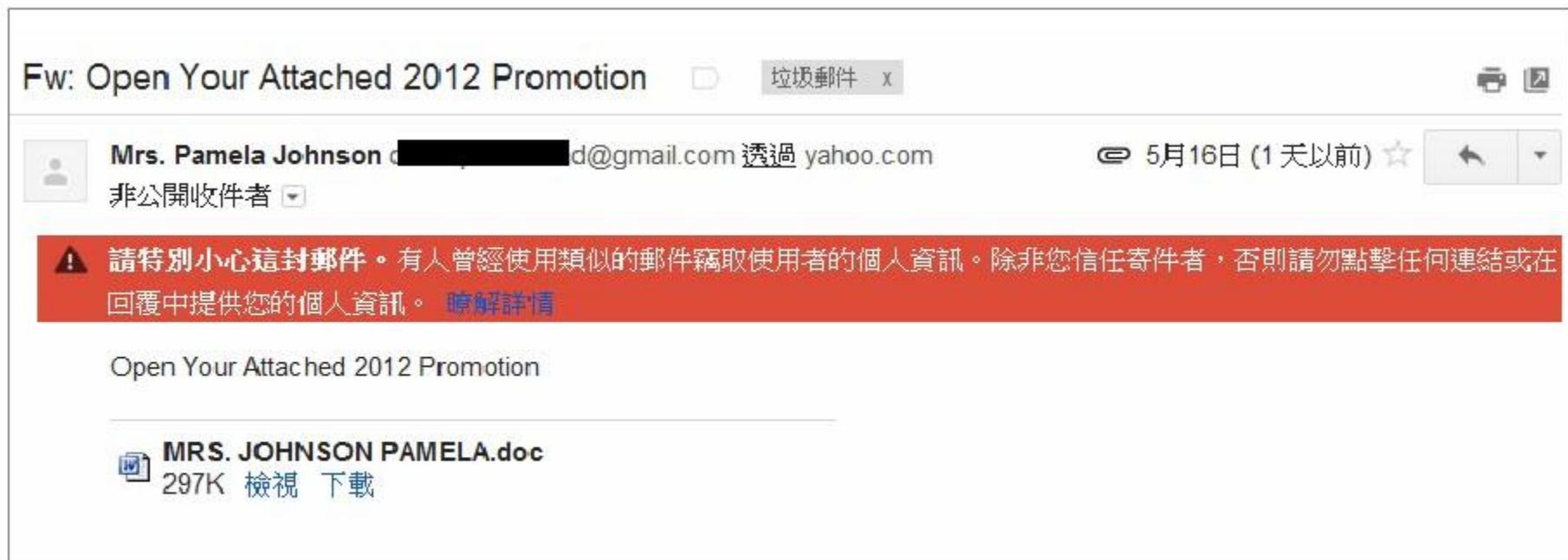


圖15. Gmail 電子郵件中標示警告標語圖例 (製圖：NII 產業發展協進會)

使用安全有效的防護產品



- 確保個人電腦維持在安全的狀態，除自身需具備充足的資訊安全觀念，亦建議安裝防護軟體並隨時更新，更加提昇安全性。