



智慧財產權、資訊安全 、個人資料保護宣導

教務處資訊網路中心 報告人：謝景順



法律及法規的遵循 — 著作權法及相關知識



The screenshot displays the official website of the Intellectual Property Office (IPO) of the Economic Bureau. The header includes navigation links such as '網站導覽', '常見問題', '意見信箱', '雙語詞彙', '專業人士', 'English', and '中文'. Below the header, there are tabs for '便民服務', '公告資訊', '國際事務', '認識智慧局', and '政府資訊公開'. The left sidebar contains a list of services including '資料檢索', '案件申請', '法規資訊', '大陸著作權相關法令及重要資訊專區', '著作權修法專區', '著作權集體管理團體相關資料', '著作利用及授權資訊', '音樂著作集體管理團體管理資訊整合查詢', and '契約範本及相關說明'. The main content area is titled '著作權知識+' and lists several topics: '著作權基本觀念', '著作權合理使用', '政府機關著作權', '電腦伴唱機著作權', '營業場所著作權', '校園著作權', '網路著作權', and '公播版影片著作權'. The last three items are highlighted with a red rectangular box.

經濟部
智慧財產局
Intellectual Property Office
INTELLECTUAL PROPERTY OFFICE

網站導覽 常見問題 意見信箱 雙語詞彙 專業人士 English 中文

便民服務 公告資訊 國際事務 認識智慧局 政府資訊公開

現在位置 | 首頁 > 著作權 > 著作權知識+

著作權知識+

- ▶ 著作權基本觀念
- ▶ 著作權合理使用
- ▶ 政府機關著作權
- ▶ 電腦伴唱機著作權
- ▶ 營業場所著作權
- ▶ 校園著作權
- ▶ 網路著作權
- ▶ 公播版影片著作權

法律及法規的遵循 —

教師於課堂上播放影片用於教學，方式有二：

1. 運用教室e化視聽設備播放

- 涉及視聽著作對特定多數人（公眾）公開上映行為。
- 是否屬於「公播版」或「教育版」的影片光碟？若否，則應注意取得著作財產權人之授權。

2. 運用電腦網路系統播放

- 涉及視聽著作的「公開傳輸」行為
- 若著作權人已授權公開傳輸，則不必另外取得授權。但如果著作權人並未授權公開傳輸的話，應取得著作權人同意。

→ 否則必須符合著作權法合理使用規定，以免侵害他人著作財產權

→ 著作權法第55條「合理使用」之三要件者：得於活動中公開口述、公開播送、公開上映或公開演出他人已公開發表之著作。

- ◆ 非以營利為目的、
- ◆ 未對觀眾或聽眾直接或間接收取任何費用、
- ◆ 未對表演人支付報酬

數位學習平台(iLMS)之權責單位

■ 數位學習平台

- 上傳平台之教材內容，由教學與學習發展中心負責管理及宣導。
- 平台可用性、安全性維護，由資網中心負責。

■ 104學年度統合視導，委員提出之建議：

針對教師上傳至數位學習平台之教材內容，校內業管單位應訂定上傳內容檢核機制，以確保上傳教材符合智慧財產權之規定。

法律及法規的遵循 — 個資保護及相關知識

- 一、101年10月「個人資料保護法」公布實施。
- 二、102年9月本校通過「**個人資料保護管理要點**」。
- 三、103年8月21日教育部明令要求，各私立專科以上學校必須訂定「**個人資料檔案安全維護計畫**」。
- 四、104年9月本校正式導入「**個資保護管理制度(PIMS)**」。
- 五、105年8月5日教育部正式發布「**教育體系資通安全暨個人資料管理規範**」。

個人資料蒐集、處理與利用的關鍵概念

目的 + 必要
合法
(法律要件)

1. 明確瞭解蒐集個人資料之特定目的為何？
2. 所蒐集之資料有必要性。
3. 必須具備允許蒐集之法律要件。

※ 非具必要性之資料，由當事人自由提供
~ 個資法第15條、第19條 ~

個人資料**利用**之意涵及合法性

利用行為**意涵**為何？

1. 公開或揭露
2. 將資料提供給當事人以外之第三人
3. 業務上非處理性質之使用

如何**合法利用**個人資料？

1. 必須在**特定目的內利用**個人資料
2. 不得逾越必要範圍(必要性考量)
3. 只有在個資法第16條或第20條規定之例外情形，才能作**特定目的外利用**(法律要件)

非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

違反個資法的法律責任 — 民事

- 對非公務機關請求權依據

私立學校所負民事責任為「**舉證責任倒置**」——能**證明**其無故意或過失者，始能免除賠償責任。

- 舉證責任倒置：**由被告舉證**。
- 如何證明？ ➡ 訂定個人資料檔案安全維護計畫，並落實執行，證明已善盡維護之責。

違反個資法的法律責任 — 刑事(行為人)

§41 (違反蒐集、處理、利用及國際傳遞要件)

違反第6條、
第15條、第16
條、第19條、
第20條第1項
規定，或中央
目的事業主管
機關依第21條
限制國際傳輸
之命令或處分

非意圖營利

足生損害
於他人

意圖營利

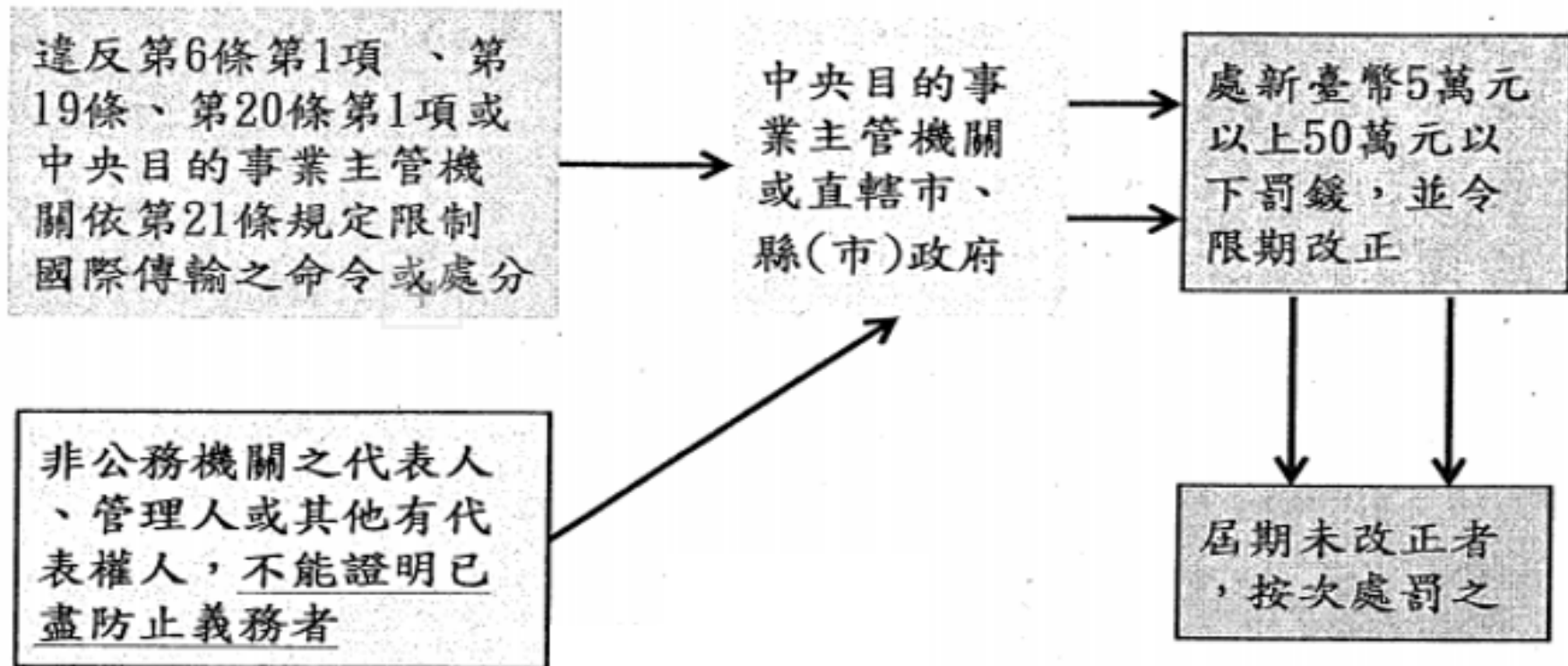
處2年以下有期徒刑、
拘役或科或併科新臺幣
20萬元以下罰金
(告訴乃論)

處5年以下有期徒刑，
得併科新臺幣100萬元
以下罰金
(公訴罪 §45)

44§公務員加重其刑二分之一

違反個資法的法律責任 — 行政(非公務機關及負責人)

§47、§50（違反蒐集、處理、利用及國際傳遞要件）



校園落實執行個資保護的好處

- 教學及行政單位應落實執行個人資料蒐集、處理、利用、保管、銷毀等標準程序，當不幸發生個資外洩或其他違法事件時，
 - (1) 可以查出個資外洩管道適時防補，
 - (2) 可向主管機關或法院證明，已盡防止義務，沒有故意或過失責任
 - (3) 避免被行政裁罰及民事損害賠償責任
- 統合視導之個資業務訪視委員曾提及，其最感興趣稽核的單位，包括：註冊、招生、輔導、校友、推廣、資訊中心等。

資訊安全威脅 - 駭客思維的改變

- 炫耀技能，駭入系統修改網頁資料
- 駭入系統，竊取機密資料、獲取主控權
- 駭入特定主機，側錄系統管理者帳號/密碼。
- 運用殭屍病毒程式(蠕蟲病毒)，控制大量僵屍電腦(botnet)，攻擊特定主機可用性(DDoS攻擊)。(使用者的電腦成為犯罪者的幫兇)
- 使用「進階持續性滲透攻擊」(Advanced Persistent Threat，簡稱APT攻擊)竊取目標系統上之資料。配合零時差漏洞攻擊(因為廠商尚未釋出修補程式，漏洞將讓廠商及一般受害者手忙腳亂。)
- 使用釣魚方式，配合釋出之木馬程式，觀察使用者的反應處理時間，再決定下手對象。
- 針對特定主機，竊取弱點掃描報告/網路架構資料，再評估下手目標。
- 植入惡意程式(勒索軟體)，將資料全數加密，藉機勒索金錢。

資訊安全威脅 - 世界經濟論壇的2016年全球風險報告

世界經濟論壇（WEF）的全球風險報告將風險分成 環境、經濟、社會、地緣政治與科技等五大範疇，評估所有風險發生的「可能性」以及「影響性」。

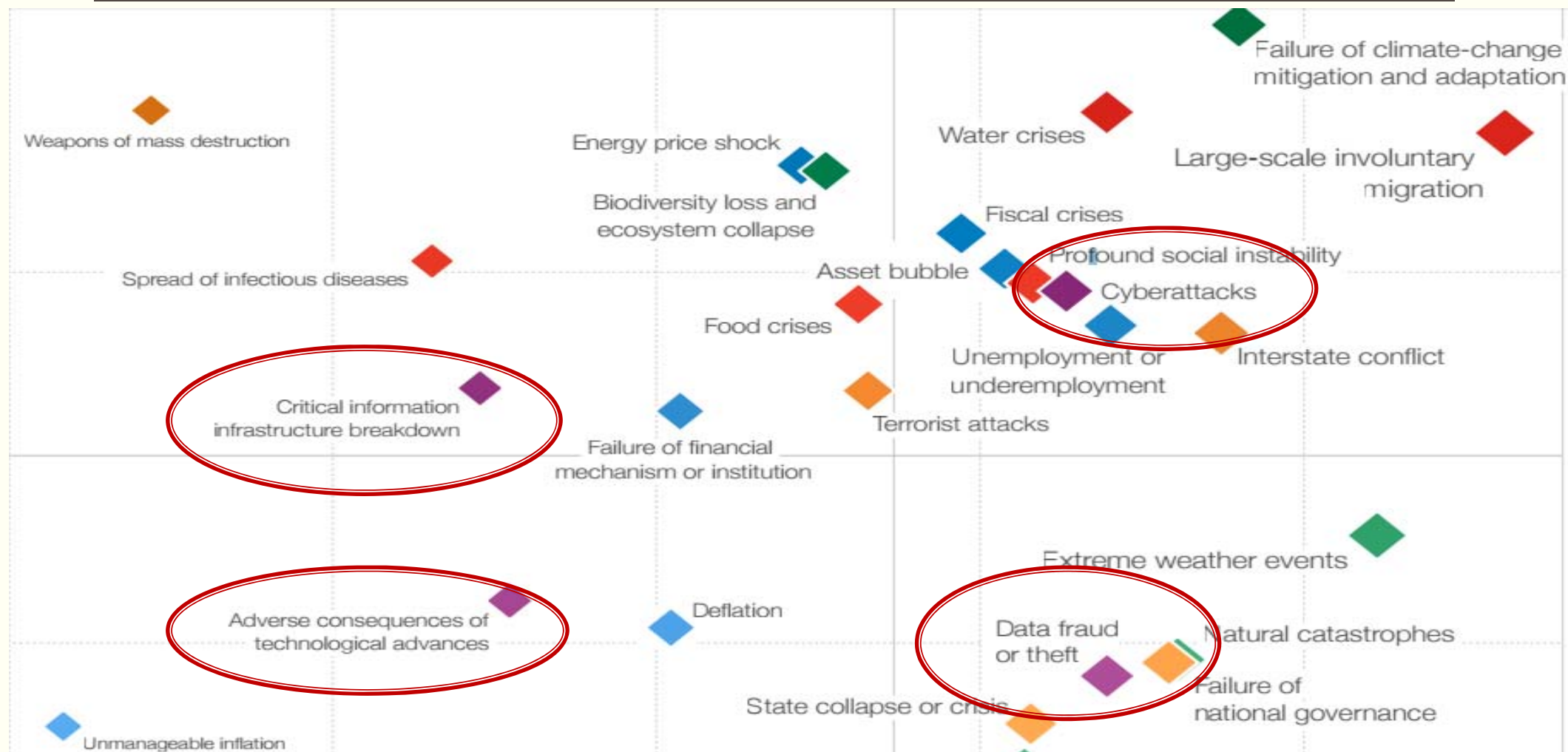
Top 10 risks in terms of 發生機率

- 1 大規模難民移民
- 2 極端氣候
- 3 氣候變遷調節與適應失靈
- 4 國家衝突
- 5 自然災害
- 6 國家治理失靈
- 7 失業
- 8 數據造假與偷竊
- 9 水資源危機
- 10 非法貿易

Top 10 risks in terms of 衝擊性

- 1 氣候變遷調節與適應失靈
- 2 大規模殺傷性武器
- 3 水資源危機
- 4 大規模難民移民
- 5 能源價格衝擊
- 6 生物多樣性喪失與生態系統崩潰
- 7 財政危機
- 8 傳染病大規模擴散
- 9 資產泡沫
- 10 社會動盪

資訊安全威脅 - 世界經濟論壇（WEF）2016年科技風險



資訊安全威脅 - 2016 科技風險驟增

- 自2015年開始，科技風險愈來愈受重視，2016年企業和國家最關心的科技風險(Technological Risks)，前四名依序是
 - 大規模網路攻擊 (Large-scale cyber attacks) 、
 - 資料詐騙和資料偷竊(Incident of data fraud/theft) 、
 - 關鍵基礎建設中斷 (Breakdown of critical information infrastructure and network) 、
 - 科技進步帶來的不良後果(Adverse consequences of technological advances)

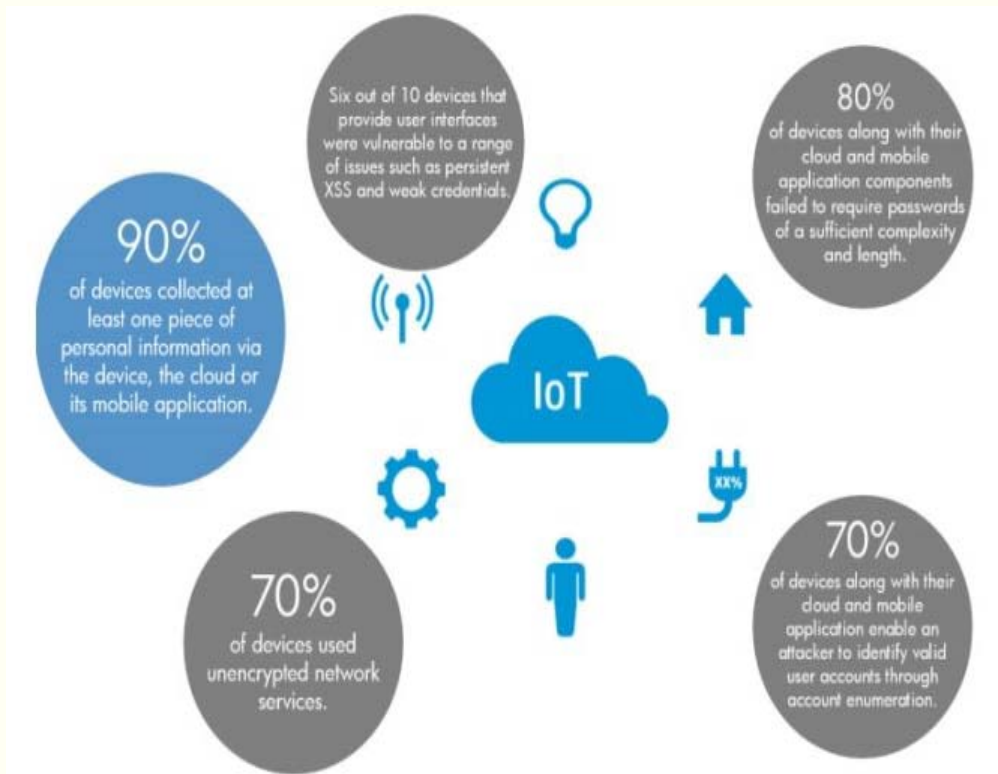
- 例如：第一銀行的提款機盜領案

資訊安全威脅 -科技風險 (續)

- 國與國之間的互動和競逐，**各國紛紛建立自己的網軍**，用各種手法發動網路攻擊，希望藉此達到各自目的，如資料外洩取得機敏資料，或是關鍵基礎設施的中斷達到癱瘓國家運作等。
- 許多人對社群軟體和行動裝置高度依賴，改變了既有的生活習慣，如低頭族已經是全球現象。讓許多**中國山寨App**有機可乘，仿冒成熱門App誘騙使用者下載。
- **勒索軟體(Ransomware)**惡意軟體，利用各種作業系統漏洞，達到綁架資料、像使用者勒索金錢的目的
- 美國蘋果公司為了確保**使用者隱私**，大力抵抗美國聯邦調查局（FBI）要蘋果公司協助提供使用者個人資料的要求，但蘋果公司的作法仍是少數，**大多數企業，其實都擋不住政府跟企業要人民資料的壓力**。（華為、小米、阿里巴巴、騰訊？）
- 在資料保護上，像是**物聯網（IoT）和數位金融**的應用也面對更大的資安挑戰。

資訊安全威脅 – 科技風險 (物聯網裝置)

根據Gartner的估計，2020年全球將安裝260億台的物聯網裝置

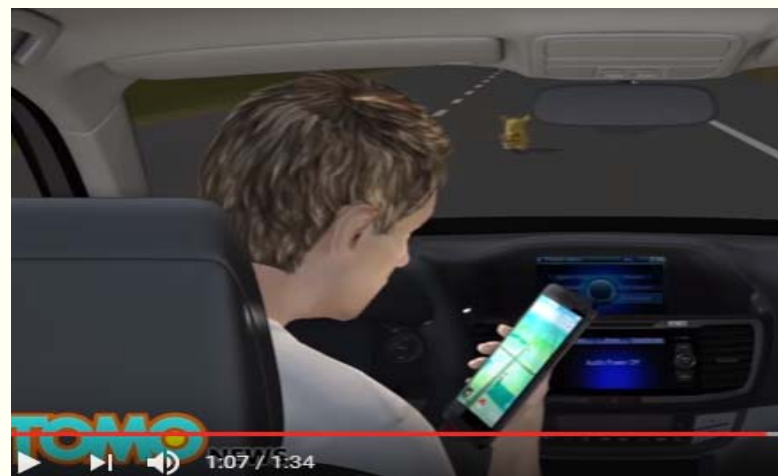
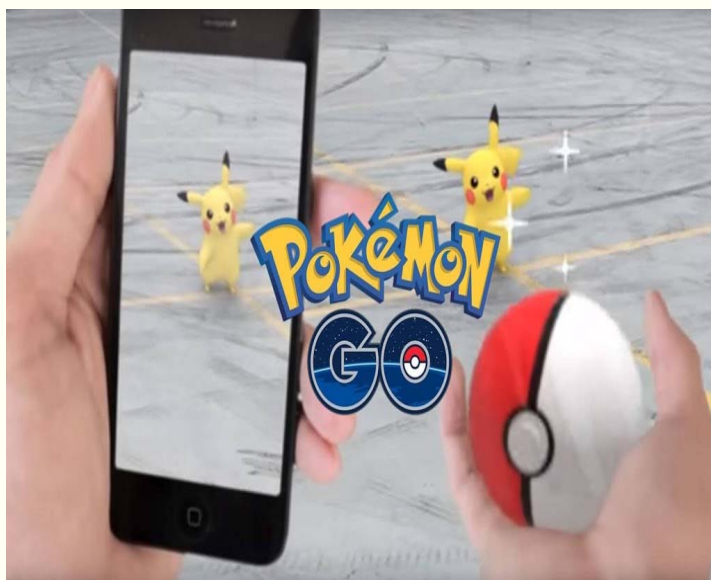


HP最近公布一份物聯網研究報告指出高達**7成的物聯網裝置含有安全漏洞，可能洩露使用者個人資訊**(名字、電子郵件、家中地址、生日、信用卡或健康資訊)

- 裝置缺乏密碼安全性、加密機制、使用者存取控制
- 相關的雲端與行動程式未含有足夠的存取保護機制
- 資料傳輸過程未進行加密保護

資訊安全威脅 — 科技進步帶來的不良後果

沉迷於任何遊戲
帶來的不良後果。



對校內教職同仁的資訊安全建議

- 本校校務資訊系統整合，採單一帳號登入(SSO)作法，其最大的資訊安全風險即為登入密碼強度(複雜度)不足，密碼強度(字數、大小寫字母、數字、符號)，並定期更改。
- 千萬小心透過「社交工程」、「網路釣魚」方式所造成的資安威脅。
- 教師宜審慎檢查在各式平台或系統所設定之資料存取權限，切勿成為「疑似侵犯智財權」或「疑似個資外洩」的當事人。
- 教師在教學、輔導或招生時，應合法地蒐集、處理、利用、傳輸個人資訊。對含有(敏感)個資之文件、電子檔、隨身碟、傳輸、儲存與處置等，應採取安全措施。
- 任何校園內之智財、個資、資安問題或事件，請直接反應給資網中心同仁。