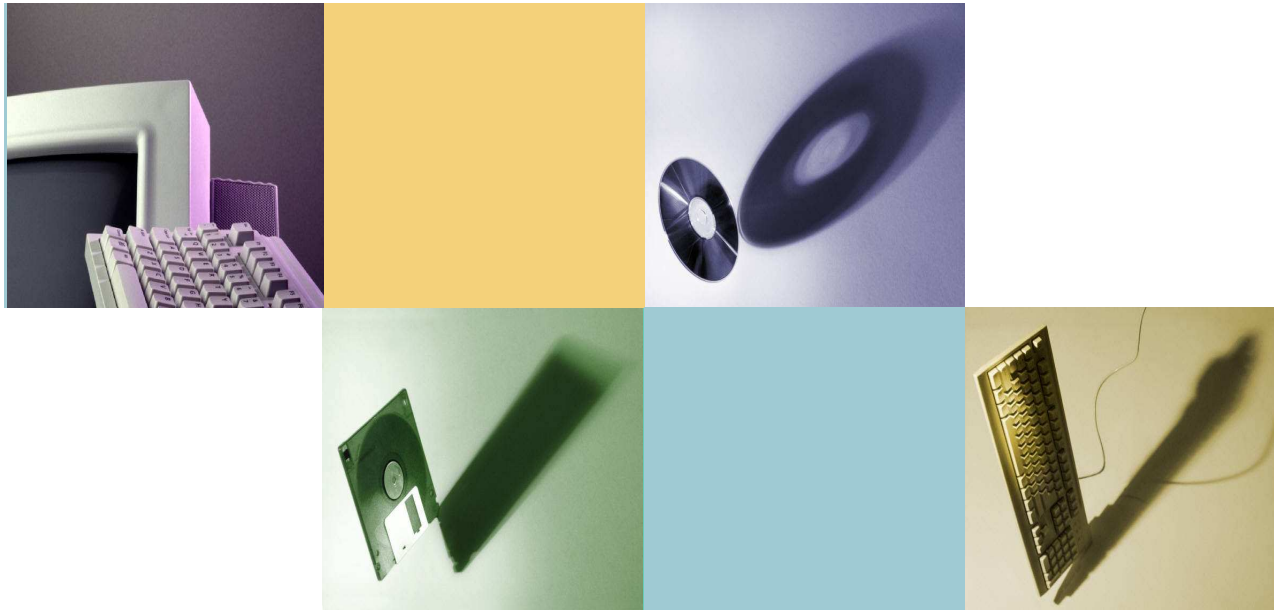


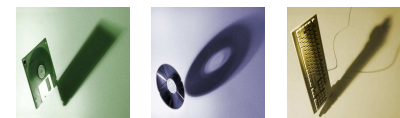
瞭解與您相關的電腦個資保護



宜蘭區網中心 曾國旭

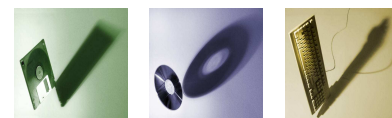
大綱

- 個人資料保護介紹
- 資安法令宣導
 - 刑法第2編第36章，妨害電腦使用罪
 - 個人資料保護法介紹



您有以下這些行為嗎

- 拷貝正版光碟…？
- 學校網路非法下載影音…？
- 提供MP3下載…？
- P2P軟體下載音樂…？
- 部落格張貼版權音樂…？
- 複製他人著作…？
- 網頁用他人拍的照片…？



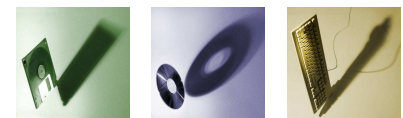
校園資訊安全事件案例

- ○○大學選課系統學生帳號遭盜用…
- ○○大學網頁照片侵權判賠罰金…
- ○○大學學生模仿性愛照外流事件…

其實，

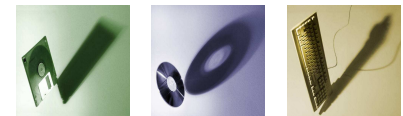
這些都是資訊安全認知不足的疏失造成…

特別是個人資料保護…



個人資料保護實際案例

- 詐騙集團以假網頁、木馬程式側錄等方式蒐集套取民眾個資...
- 透過Google輸入特定的關鍵字，可以找到「訂單詳細資料」，包括聯絡人姓名、身分證字號、電話、地址、電子郵件...
- 學生在校內遺失USB記憶卡，內有該學生與女友親密的照片...
- 將手機交予電話服務商維修，遭技術人員發現內有私密照片，將其複製與友人分享，被人上載網路流傳...

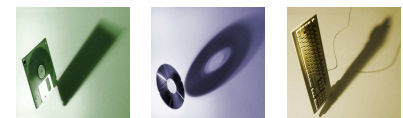


個人資料外洩的原因

- 來自外部的威脅
- 人為疏失造成的資料外洩
- 保管不當
- 安全認知不足

使用者對於資訊安全防護認知的不足
可能造成極大的資料外洩代價…

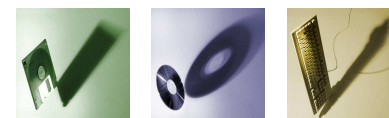
您，真的沒有外洩個資？



何謂社交工程

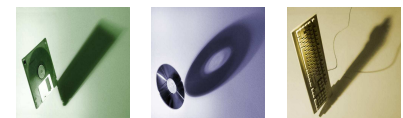
所謂「社交工程」，就是詐騙！

透過電話、電子郵件等方式偽裝身份
誘騙您上勾受騙…



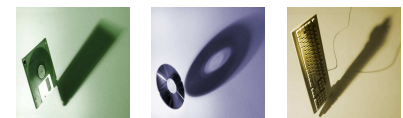
常見的社交工程手法

- 打電話
- 電子郵件隱藏電腦病毒
- 網路釣魚
- 偽裝工具程式
- 即時通



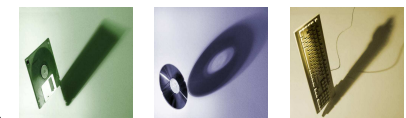
社交工程攻擊步驟

- 首先取得一個攻擊目標的背景資訊
- 向目標騙取資訊
- 再利用這些資訊向其他人欺騙
- 重覆這些步驟致達到最後目標



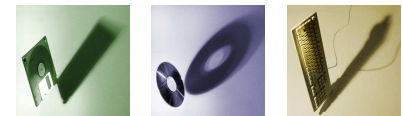
防範社交工程的正確觀念

- 認識常見社交工程攻擊的可疑徵兆
- 遵守組織安全政策與程序
 - 確認對方的身分
- 通報作業



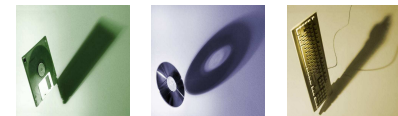
常見的惡意程式電子郵件

- 利用「社交工程」伎倆的電子郵件詐騙攻擊
- 常見的惡意程式電子郵件型式
 - 利用色情標題誘騙收件人開啟郵件
 - 內容看似一般網路轉寄郵件
 - 惡意程式郵件也會將檔案隱藏在.zip檔
 - 附檔名.bat可能是惡意程式執行檔
 - 附檔名.lnk可能是惡意程式網頁連結



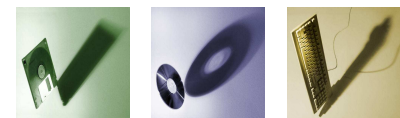
電子郵件的相關安全防護

- 除了不要點擊連結與隨意開啟附檔外，您應該曉得的安全防護還包括：
 - 關閉自動下載圖片
 - 關閉預覽視窗，啟用預覽視窗等同「開啟郵件」！
- 不要自動回覆讀信回條
- 考慮設定以純文字格式讀取郵件
 - 電子郵件如果是HTML格式，因HTML可以撰寫ActiveX，所以您只要瀏覽電子郵件，就觸發ActiveX執行！（有些惡意程式是利用ActiveX功能來執行的）



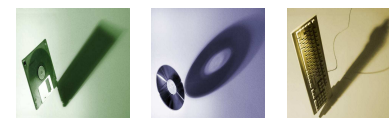
轉寄郵件需留意的事項

- 轉寄郵件可能外洩個資
 - 轉寄郵件洩漏個人資料
 - 曝露收件者的郵件信箱
- 轉寄郵件的**正確操作**認知
 - **刪除轉寄郵件標頭文字**
 - **使用密件副本**功能保護收件人郵件信箱資料

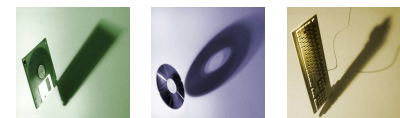


轉寄郵件可能產生的違法情況

- 以為自己善意轉寄告知，但**傳達的可能是完全錯誤訊息**
- **散播錯誤的醫療知識、食品**
- 未經證實轉寄惡行，**可能變成毀謗從犯**
- 肆意轉發他人版權著作(圖、文、影音)，**可能違反著作權法...**

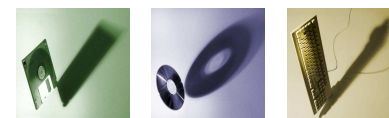


再次提醒您，
不要隨意開啟郵件附檔，
包括像Word、Excel檔案
都可以利用VBA撰寫程式碼，
亦可能為惡意程式檔案！



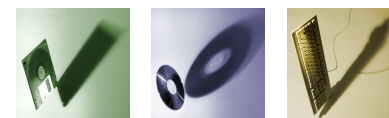
網路釣魚Phishing

- 利用偽造的網頁作為誘餌，詐騙使用者洩漏如帳戶密碼等個人機密資料
- 釣魚網頁畫面與官方網站相同(或類似讓人無法辨別)，但其實這個網址並非官方網站
 - 以相似的字元來偽裝網址，例如：以數字的0來替換英文的O；以數字的1來替換英文的l



防範網站惡意程式的正確認知

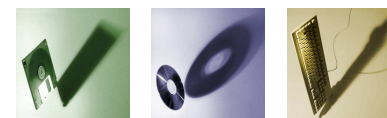
- 惡意程式陷阱皆是利用使用者好奇心誘騙開啟，因此千萬不要因為好奇心肆意開啟連結
- 當點選連結後出現「您將前往的網頁可能含有惡意程式」等類似訊息文字，代表該連結為網站外部連結，並可能為一惡意程式執行檔，應立即取消連結的執行
- **留意圖示連結、文字連結等實際的網址URL**，實際連結的網址可能和畫面上顯示的網址不同。可將滑鼠游標停留在圖示連結、文字連結上，由畫面左下方顯示的實際連結網址，確認畫面顯示的是否為偽連結網址



清除電腦上所留的登入資料

- 以使用Internet Explorer瀏覽器為例
 - Internet Explorer中提供了「自動完成」功能，該功能主要是方便使用者記住曾經在瀏覽器中輸入先前輸入的網址、表單及密碼等訊息。

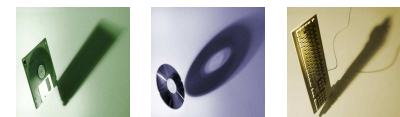
電腦上的暫存檔案，
也可能洩露您曾經做過的操作…



常見的P2P程式

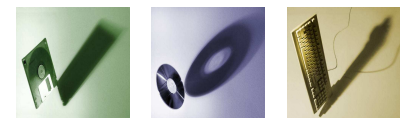
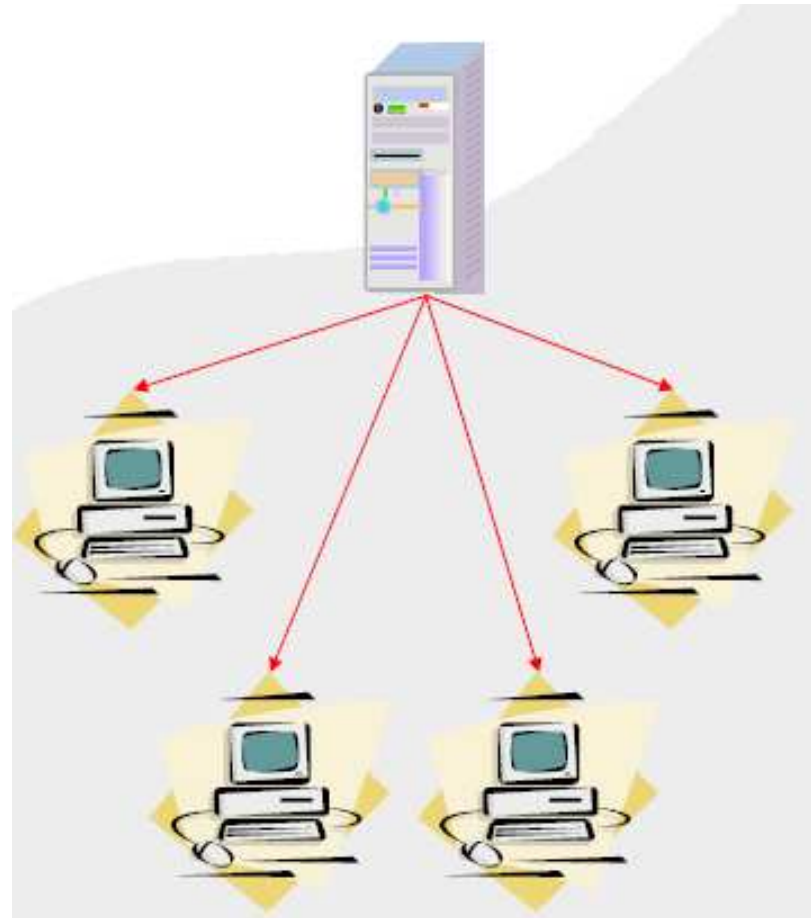
- 即時通訊軟體
- eDonkey
- eMule
- Foxy
- BitTorrent / BitComet
- Clubbox / GOGOBOX
- Kuro/ ezPeer

分享加速式檔案下載



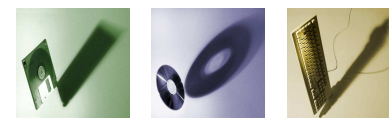
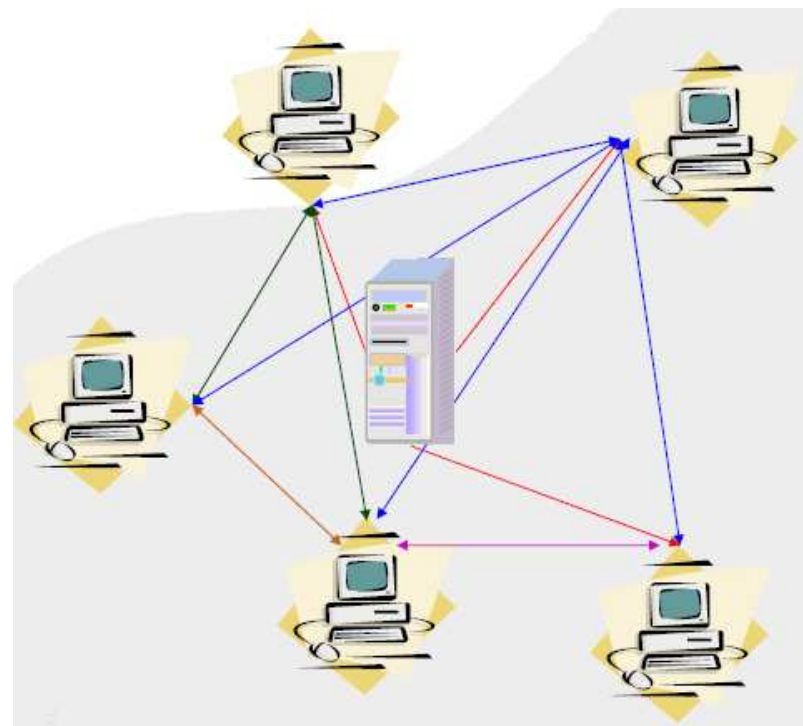
傳統伺服器下載

- 使用者由伺服器下載檔案，越多使用者同時下載檔案時會因頻寬分用，下載檔案速度會變慢



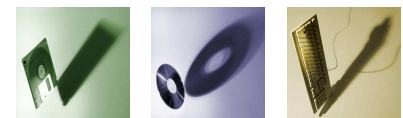
P2P網路下載

- 每一個使用者同時擔任提供檔案角色，某一檔案越多人下載時，下載檔案速度會因檔案分段切割越多，速度越快

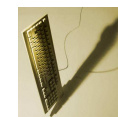
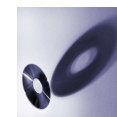


使用P2P軟體可能衍生的問題

- 任意使用各種P2P軟體下載盜版軟體、電影與音樂等
- 使用不當造成電腦內資料外洩
- P2P網路上散播的惡意程式造成電腦中毒
- 佔用區域網路連外頻寬

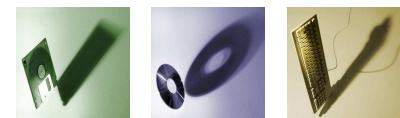


Q & A



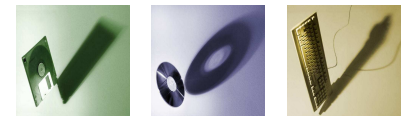
刑法妨害電腦使用罪

- 第358條：無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而**入侵他人之電腦或其相關設備者**，處**三年以下有期徒刑、拘役或科或併科十萬元以下罰金**
- 第359條：**無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄**，致生損害於公眾或他人者，處**五年以下有期徒刑、拘役或科或併科二十萬元以下罰金**



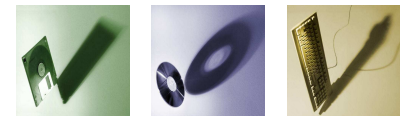
刑法妨害電腦使用罪(續)

- 第360條：無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金
- 第361條：對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一



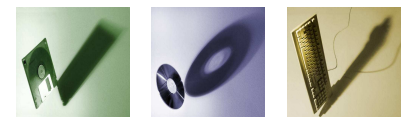
刑法妨害電腦使用罪(續)

- 第362條：製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金
- 第363條：第358條至第360條之罪，須告訴乃論



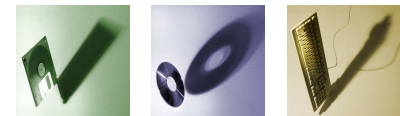
個人資料保護法

- 共六章，56條
 - 第一章：總則(第1條至第14條)
 - 第二章：公務機關對個人資料之蒐集、處理及利用(第15條至第18條)
 - 第三章：非公務機關對個人資料之蒐集、處理及利用(第19條至第27條)
 - 第四章：損害賠償及團體訴訟(第28條至第40條)
 - 第五章：罰則(第41條至第50條)
 - 第六章：附則(第51條至第56條)



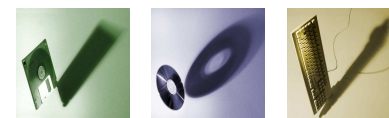
個人資料保護法(續)

- 立法目的與精神
 - 為**規範個人資料之蒐集、處理及利用**，以**避免人格權受侵害**，並促進個人資料之合理利用，特制定本法(第1條)
- 什麼是個人資料？
 - 指**自然人**之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料



個人資料保護法(續)

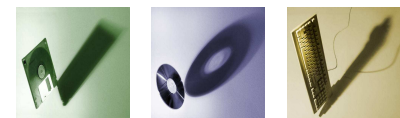
- 範圍與主體普遍化
 - 新版個資法將舊法規範的對象從原來醫療、電信、大眾傳播、金融等8大行業擴大至**所有公民營機關**，將過去不適用電腦處理個人資料保護法的行業(如網路零售業)，**不限行業、自然人、法人或其他團體(含境外)**，全部納入規範



個人資料保護法(續)

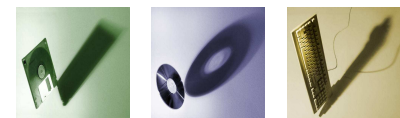
- 強化行為規範

- **特定目的**：個人資料之蒐集、處理或利用，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯
- **公開及專人維護**：應將所蒐集、處理及利用之個資類別、檔案名稱、保有之依據及目的，保有機關名稱及聯絡方式加以公開，並指定專人維護
- **告知及書面同意**：向當事人蒐集個人資料時，應明確告知當事人蒐集機關的名稱、目的、個資類別、個資利用的期間、地區、對象及方式、當事人得行使之權利及方式等，並取得當事人之書面同意



個人資料保護法(續)

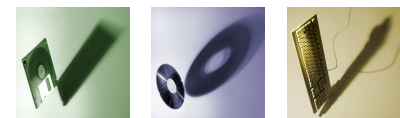
- 特種個資蒐集、處理及利用之例外情況
 - 有關**醫療、基因、性生活、健康檢查、犯罪前科**之個人資料，**不得蒐集、處理或利用**。但有下列情形之一者，不在此限
 - 法律明文規定
 - 公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施
 - 當事人自行公開或其他已合法公開之個人資料
 - 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料(範圍、程序及其他應遵行事項之辦法，由中央目的事業主管機關會同法務部定之)



個人資料保護法(續)

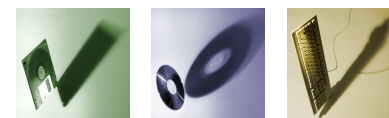
- 損害賠償及團體訴訟

- **公務機關違反個資法規定**，致個人資料遭不法蒐集、處理、利用或其他當事人權利者，**負損害賠償責任**。但損害因天災、事變或其他不可抗力所致者，不在此限
- **被害人不易或不能證明其實際損害額時**，法院得依侵害情節，以**每人每一事件新台幣五百元以上二萬元以下計算**。如**同一原因事實造成多數當事人權利受侵害事件**，賠償金額**最高以新台幣二億元為限**。但若該原因事實所涉利益超過新台幣二億元者，以該所涉利益為限



個人資料保護法(續)

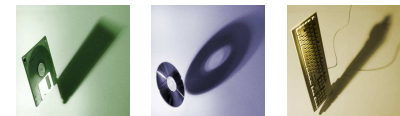
- 非公務機關違反個資法規定，致個人資料遭不法蒐集、處理、利用或其他當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限
- 損害賠償請求權，自請求權人知有損害及賠償義務人時起，因二年間不行使而消滅；自損害發生時起，逾五年者，亦同



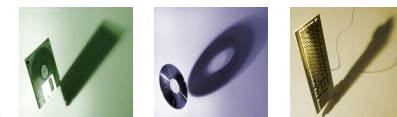
個人資料保護法(續)

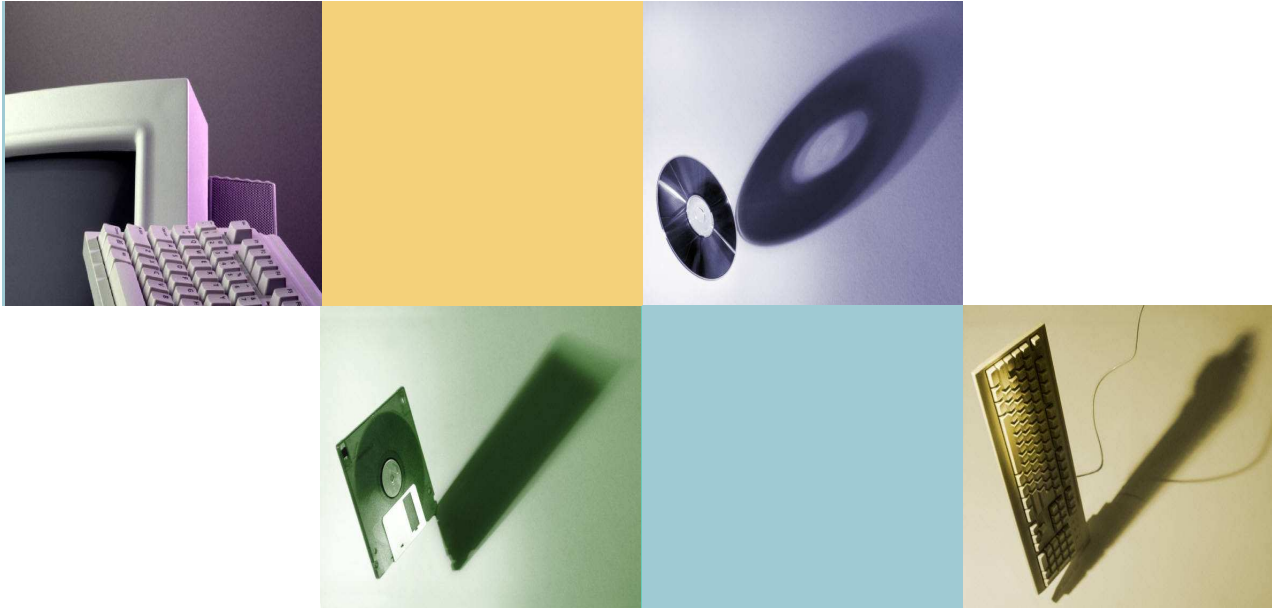
• 罰則

- **公務機關違反個資法相關規定**，足生損害於他人者，處**二年以下有期徒刑**、拘役或科或併科**新台幣二十萬元以下罰金**。意圖營利犯前項之罪者，處**五年以下有期徒刑**、拘役或科或併科**新台幣一百萬元以下罰金**
- **公務員假借職務上之權力、機會或方法**，犯本罪者**加重其刑二分之一**
- **非公務機關違反個資法相關規定**，由中央目的事業主管機關或直轄市、縣市政府處**新台幣五萬元以上五十萬元以下罰金**，並令限期改正。未改正者，按次處罰之。代表人、管理人或其他有代表權人，應受同一額度罰金



Q & A





THANKS !