保護自己的數位便捷生活

資安與我

廖仁宏

國立高雄師範大學

講者介紹

職業訓練專門科

廖仁宏

專門為您抓漏掉的技能

活動中心 C５０１教室

程式設計　軟體工程　介面裝潢

07-8210171 高雄前鎮

講者介紹

廖仁宏

- 現職-勞動部勞動力發展署高屏澎東分署職業訓練師
- 曾任-軟體程式設計師、軟體研發工程師、軟體技術顧問、高職教師

專長與可授課程

- Back-end programming(ASP.net Core MVC)
- Front-end programming(JavaScript、jQuery、Angular)
- Responsive web design(Bootstrap)
- Database design and implement(MS SQL Server)
- System analysis and system design(UML)
- Web application design and development
- 網頁設計乙丙級、電腦軟體應用乙丙級、電腦軟體設計丙級技術士檢定

證照

- 網頁設計乙級
- 電腦軟體應用乙級
- 電腦軟體設計丙級
- 網頁設計丙級
- 電腦軟體應用丙級
- 電腦硬體裝修丙級
- 會計事務丙級
- 雲端APP程式應用人員認證

其他

- 2020年勞動部推動人工智慧專案評獎-創新提案獎
- 指導軟體設計職類選手獲第49屆全國技能競賽分區賽南區金牌
- 2016年度勞動部勞動力發展署 最佳訓練師資獎
- 中華民國專利 "反向路徑確認動態來源繞送方法" 發明第 I 351855號

國立高雄師範大學

01 何謂資訊安全

資訊安全有哪些要素？
何謂ISMS？何謂 ISO 27001？何謂PDCA？
資訊安全有哪些種類？

02 資安威脅介紹

電腦病毒、木馬程式、蠕蟲，一堆名詞要先搞清楚！
我該怎麼防範惡意程式？
駭客是什麼？如何進行攻擊？如何預防？

03 網路交易安全概念

何謂加密與解密？如何運作？
認識SSL、SET及FXML等機制。
在這個網路交易盛行的時代，你一定要懂得自我保護。

04 網路普及帶來的衝擊

資訊大到無法負荷所引發的資訊焦慮，如何帶來資安風險？
網路謠言與假訊息有哪些手法？
有哪些網路犯罪的方式？
暗網是什麼？有哪些威脅？

05 資訊素養與倫理

資訊居然還有素養？！有哪些？內涵為何？
何謂PAPA原則？

06 個人資料的保護

什麼是個人資料保護法？它很重要嗎？
什麼資料該被保護？真的有辦法保護嗎？
隱私權是什麼？你對隱私權的認知真的對嗎？

07 校園資訊安全教育

家長與教師該是什麼角色？
學生有哪些自我保護的責任與方法？
具備基本的資安素養才是根本之道！

國立高雄師範大學

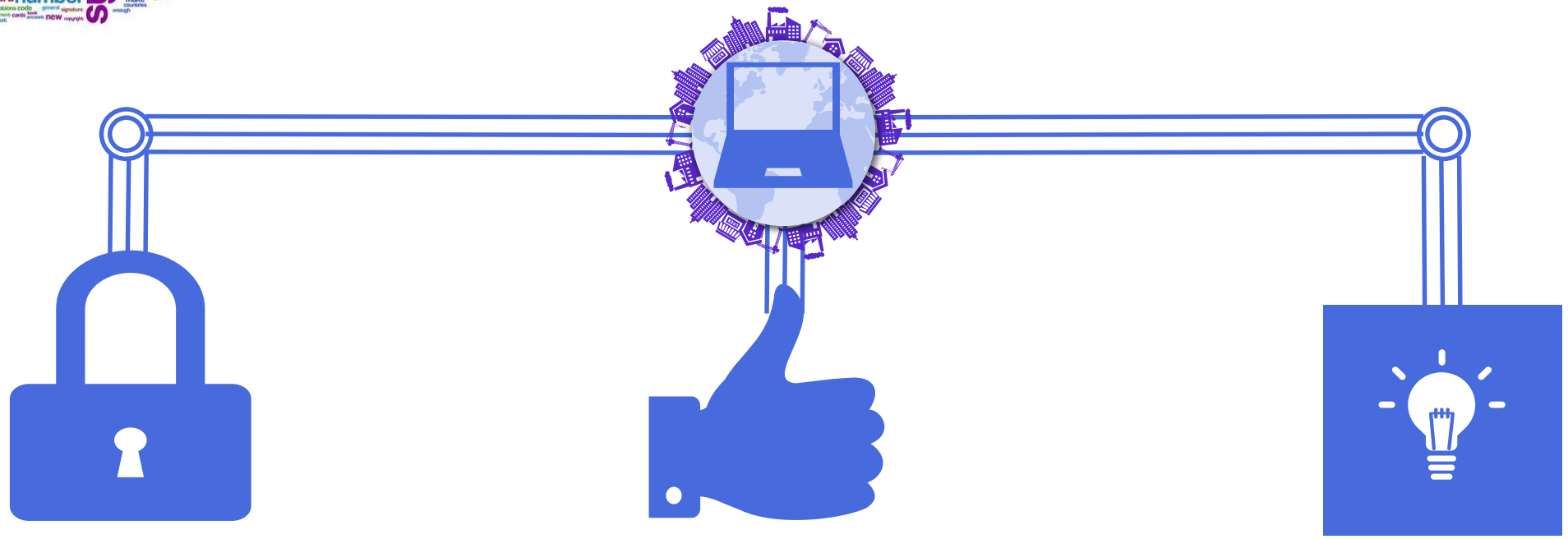
何謂資訊安全

What is Information Security？

保護自己的數位便捷生活

資訊安全三要素

國立高雄師範大學



機密性(Confidentiality)

任何機密資訊未經授權皆無法被看到。要保障所有的訊息由對的人、在對的時間、用對的裝置、於對的地點上被存取。

完整性(Integrity)

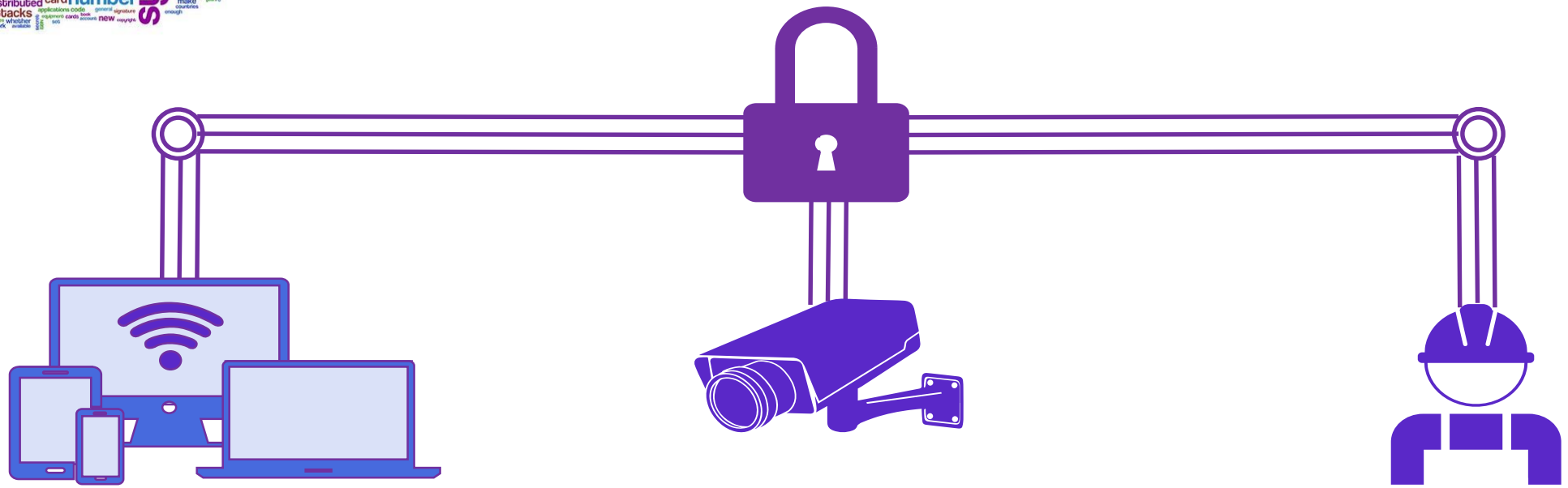
在傳輸、儲存資訊或資料的過程中，資訊或資料未被篡改，維持資訊內容的正確與完整。

可用性(Availability)

讓系統隨時處於可工作狀態，資訊服務不因任何因素而中止，資料必須可即時並可靠地提供。

衍生-三個安全性要素

國立高雄師範大學



不可否認性(Non-repudiation)

確保無法否認於系統上完成的操作。

- 信用卡線上刷卡。
- 存錢、領錢、轉帳。
- 證券交易。

存取控制(Access Control)

依照身分給予適當權限，任何人都必須有適當且合理的授權。

- 有授權不代表可以一直使用。
- 人為因素難防範
- 作業疏忽甚至有意為之。

鑑別性(Authenticity)

能辨識資訊使用者的身分且確保數位身分有合理妥當的驗證。

- 帳號、密碼。
- 憑證（實體、軟體）。

保護自己的數位便捷生活

資訊安全管理系統

國立高雄師範大學

資訊安全管理系統(Information Security Management System, ISMS)

系統的目的在於保護資訊資產的機密性、可用性及完整性。

透過有系統地分析和管理資訊安全風險方法，利用專業的控制手段，將資訊安全風險降到可接受的範圍內，即使遭受攻擊，仍能維持系統的基本運作能力。

ISO 27001

一套國際通用的資安管理系統標準，中文全名為「資訊科技-安全技術-管理系統-要求事項」

台灣《資通安全管理法》規定，不論是A、B、C級的公務機關或特定之非公務機關，必須在2年內取得台版CNS 27001或ISO 27001認證。

PDCA流程

建構ISMS的流程準則

計畫 Plan

建立管理資訊安全風險的目標及改進資訊安全系統的相關政策、控制措施。

執行 Do

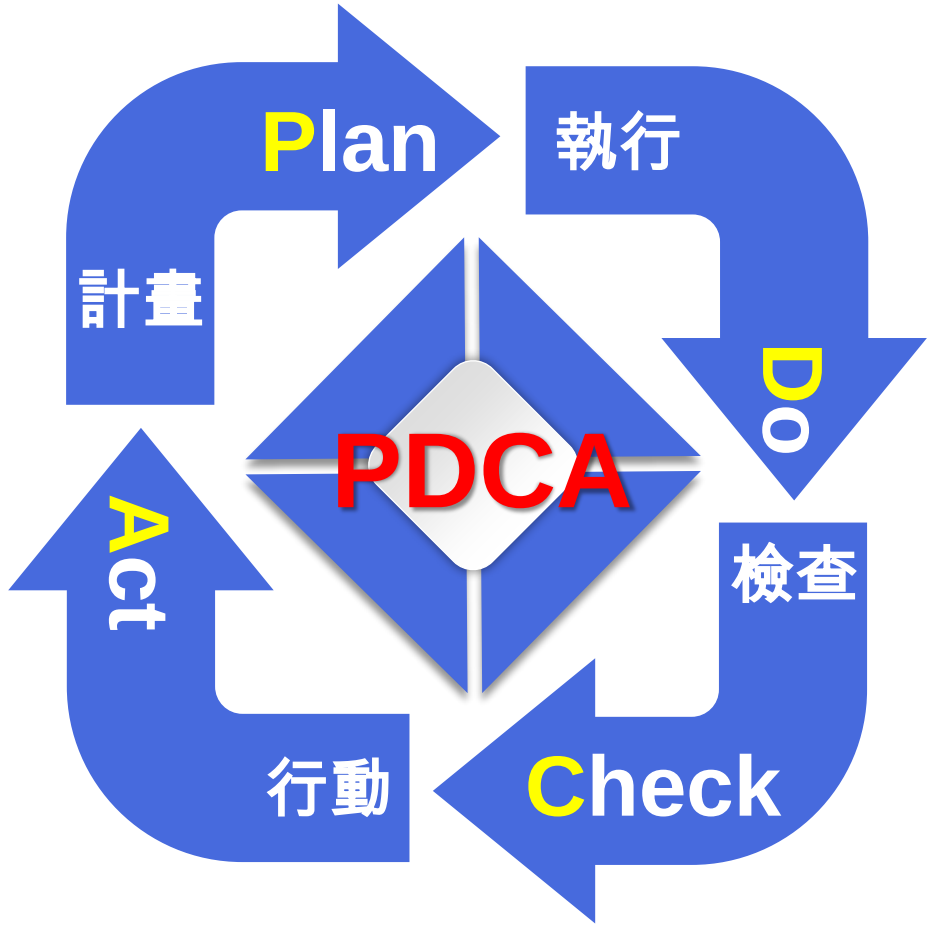
建立管理資訊安全風險的目標及改進資訊安全系統的相關政策、控制措施。

檢查 Check

建立管理資訊安全風險的目標及改進資訊安全系統的相關政策、控制措施。

行動 Act

建立管理資訊安全風險的目標及改進資訊安全系統的相關政策、控制措施。



資安是一個管理的過程，不是一項技術導入過程，所以資安的維護不單單是資訊人員的責任，而是每個參與其中的人，否則整個組統都會受到威脅。所以資安人員要時時建立使用者的資安概念及良好的資訊素養與使用習慣。

保護自己的數位便捷生活

資訊安全的種類

國立高雄師範大學

硬體安全

包含對硬體環境的掌握及設備管理，例如建築物安全、天然災害、火災、人為破壞等控制。

- 滅火設備
- 耐火絕緣材質
- 防水及漏水保護
- 電力系統(發電或不斷電)
- 備份及備援(同地、異地)
    - 完整、差異、增量

軟體安全

包含資料軟體安全和通訊管理的安全性。

- 感染病毒
- 被入侵
- 被斷網

資料安全

因為資訊犯濫而造成的資料安全問題，也成為資訊使用者最擔心的問題。

- 被竊取、盜用或遺失
- 嚴謹的密碼設置
- 多方的安控方式
- 資料的加密
- 良好的使用習慣

國立高雄師範大學

資安威脅介紹

The Threat of Information Security

惡意程式

國立高雄師範大學

惡意程式 (Malicious Code)，泛指所有不懷好意的程式碼。

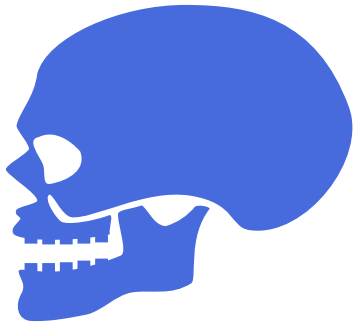
電腦病毒
Computer Virus

蠕蟲
Worm

垃圾郵件
Spam

特洛伊木馬
Trojan Horse

勒索軟體
Ransomware



間碟程式
Spyware

邏輯炸彈
Logic Bombs

無檔案病毒
Fileless Malware

著名的病毒

國立高雄師範大學

01

經典老毒

米開朗基羅、兩隻老虎、台灣No.1…

02

全球重大經濟損失經典毒

疾風、紅色警戒、WannaCry…

03

當年討論度很高

彩虹橋木馬

保護自己的數位便捷生活

惡意程式防範

國立高雄師範大學

定期備份

安裝(更新)防毒軟體

勿下載及安裝來路不明軟體

注意國際重大資安事件

軟體定期更新(漏洞填補)

勿點擊來路不明連結

培養正確的使用習慣

隨時注意電腦狀況

其時很多時候是自己打開門大喊「歡迎光臨」

駭客 & 怪客

國立高雄師範大學

駭客(Hacker)，指的是非法入侵他人電腦系統、竊取資料甚至破壞及竄改等。

白帽、灰帽、黑帽、藍帽、藍帽、激帽

思考：駭客是壞人嗎？

國際駭客組織

Anonymous

常見駭客手法

鍵盤側錄

零時差攻擊

網路釣魚

郵件炸彈

中間人攻擊

阻斷式攻擊
DoS、DDoS

入侵網站

網站掛馬攻擊

殭屍攻擊

密碼噴灑

資料隱碼攻擊

DNS伺服器攻擊

跨站腳本攻擊(XSS)

駭客威脅及防範

國立高雄師範大學

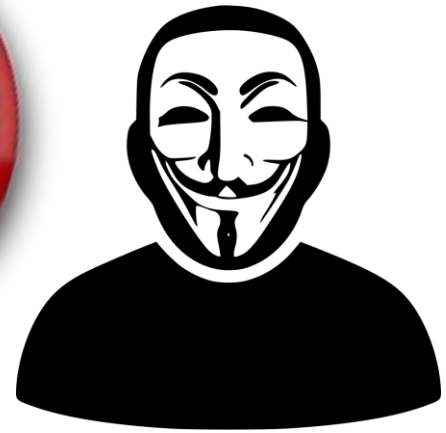
防火牆　防火牆只能阻擋外部的入侵

入侵偵測及防護系統　主動式的防護

虛擬私有網路VPN　利用權限管理網路

帳號與密碼的使用　有效的密碼規範

駭客的防範必須多管齊下才有較佳的效果，但若遇到真正有心的人士，仍會被攻破。



國立高雄師範大學

網路交易安全概念

Transection Security of Internet

保護自己的數位便捷生活

網路交易安全概念

國立高雄師範大學

資料的加密與解密示意

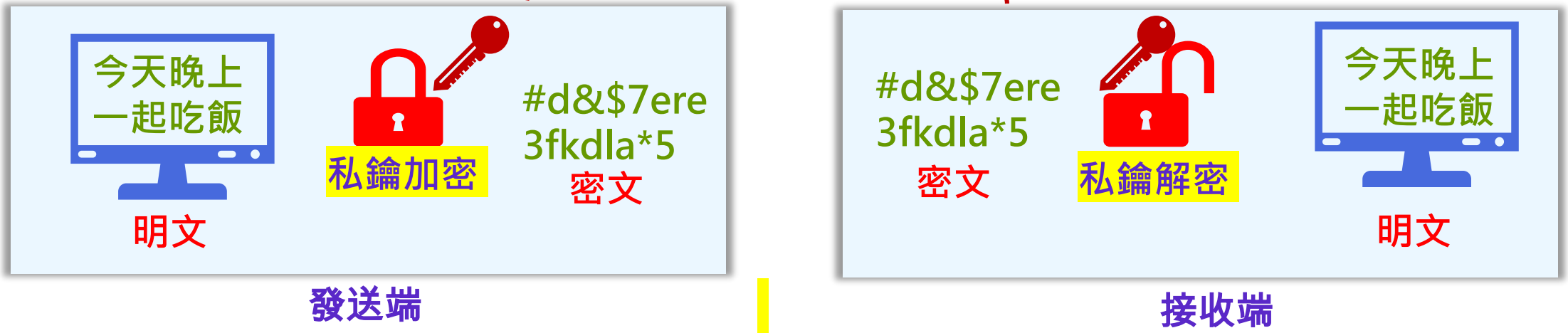
資料加密的作用是將**可被讀取的資訊進行某種規則的保護**，確保即使被人擷取到資料也無法得知內容為何，而接收的人再**依據規則解開保護**，即可讀取正確的資訊。

網路交易安全概念

1. 私密金鑰加密法(對稱式加密法)

如果有第三人也有這把鑰匙呢？

兩邊使用同一把鑰匙



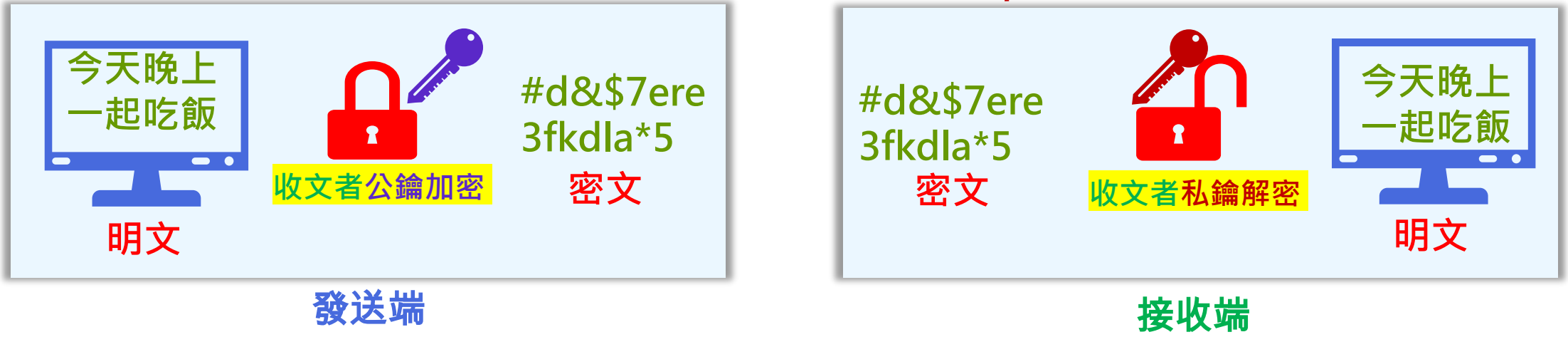
我們擁有同一把上鎖及開鎖的鑰匙

網路交易安全概念

2. 公開金鑰加密法(非對稱式加密法)第一種用途

確保資料機密

兩邊使用不同鑰匙



用接收者的公鑰加密，用接收者的私鑰解密

網路交易安全概念

2. 公開金鑰加密法(非對稱式加密法)第二種用途

確保資料來源正確

兩邊使用不同鑰匙

今天晚上
一起吃飯
明文

發文者私鑰加密

#d&$7ere
3fkdla*5
密文

發送端

#d&$7ere
3fkdla*5
密文

發文者公鑰解密

今天晚上
一起吃飯
明文

接收端

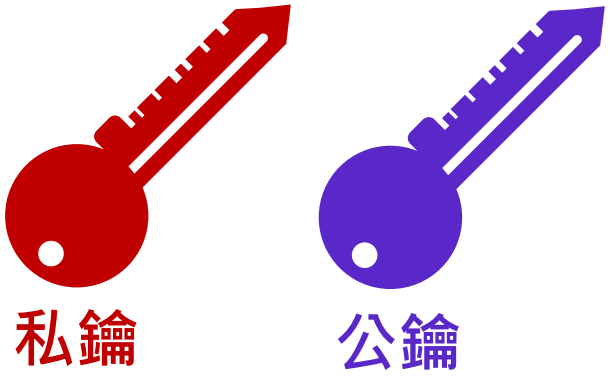
用發送者私鑰加密，用發送者公鑰解密

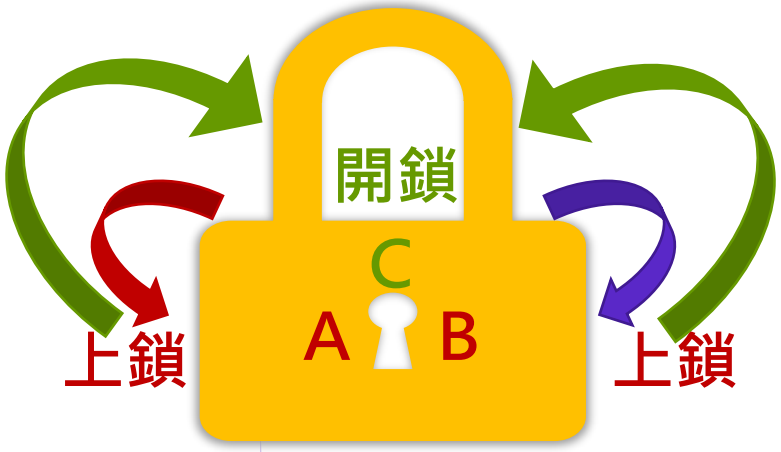
公開金鑰加密法舉例說明

國立高雄師範大學

遊戲規則

1. 這是一把特製的鎖，必須使用特製的鑰匙才能打開。
2. 紅色鑰匙要上鎖時只能往左轉到Ａ，紫色鑰匙要上鎖時只能往右轉到Ｂ。
3. 兩把鑰匙在開鎖時都可以把鎖孔轉中間到Ｃ。
4. 紅色就是**私鑰**，**不會**在網路上傳遞，紫色是**公鑰**，**會**在網路上傳遞。



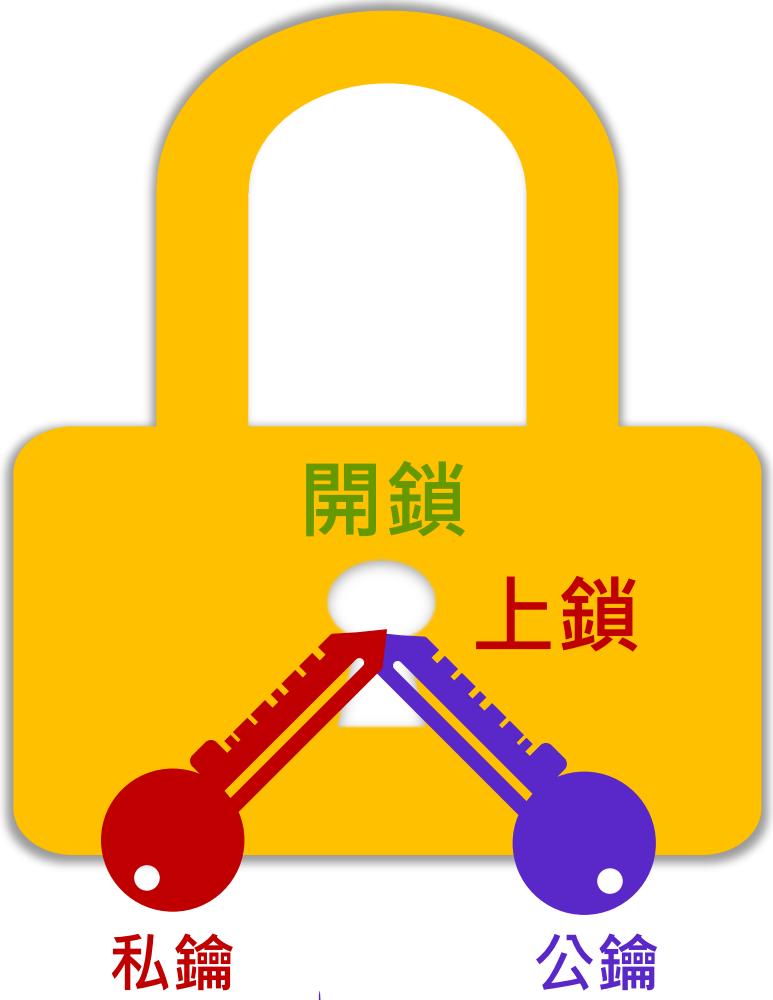


確保資料的機密

1. 由收件者寄出一把公鑰和鎖頭給寄件者。
2. 寄件者將信放入盒子裡，用收件者的公鑰把鎖頭鎖起來。
3. 將已上鎖的盒子寄給收件者。
4. 收件者利用私鑰把鎖打開，讀取盒子裡的信件。

即使公鑰在傳輸過程中被盜取或複製，也打不開這個鎖，因為只有私鑰可以打得開。

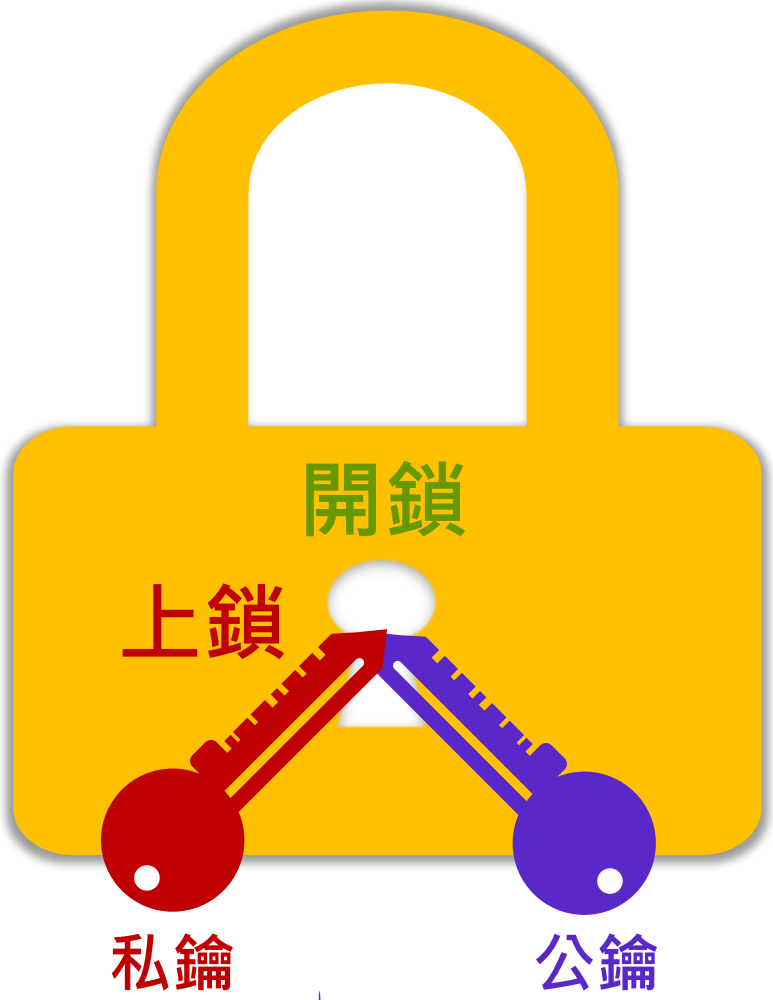
由於私鑰並未在網路上傳遞，因此不會被盜取或複製，也就是只有收件者有辦法將其打開。



確保資料來源正確

1. 寄件者先把公鑰寄給收件者。
2. 寄件者將信放入盒子裡，用寄件者的鎖頭和私鑰把鎖起來。
3. 將已上鎖的盒子寄給收件者。
4. 收件者利用寄件者的公鑰把鎖打開，讀取盒子裡的信件。

使用寄件者的公鑰若可以將鎖打開，因寄件者當初是用私鑰上鎖，代表這個盒子一定是寄件者送來的。但這樣沒辦法保證資料的機密性。



如何確保資料機密及來源正確

1. 由收件者寄出一把公鑰和鎖頭給寄件者。
2. 寄件者將信放入盒子裡，用寄件者的鎖頭和私鑰把鎖起來。
3. 再將這個盒子放入另一個盒子裡，並用收件者的公鑰把鎖頭鎖起來。
4. 將已上鎖的盒子寄給收件者。
5. 收件者利用私鑰把自己的鎖頭打開。

   (只有收件者私鑰能打開收件者公鑰上鎖的鎖頭，因此確保機密性)
6. 收件者利用寄件者的公鑰把寄件者的鎖頭打開。

   (若能將鎖打開，因此鎖是用寄件者私鑰上鎖，則一定是寄件者送的，確保來源正確)

保護自己的數位便捷生活

這些熟悉的陌生名詞

國立高雄師範大學

數位簽章

數位憑證

SSL

SET

FXML

國立高雄師範大學

網路普及帶來的衝擊

The Influence of Internet Popularity

保護自己的數位便捷生活

網路普及帶來的衝擊

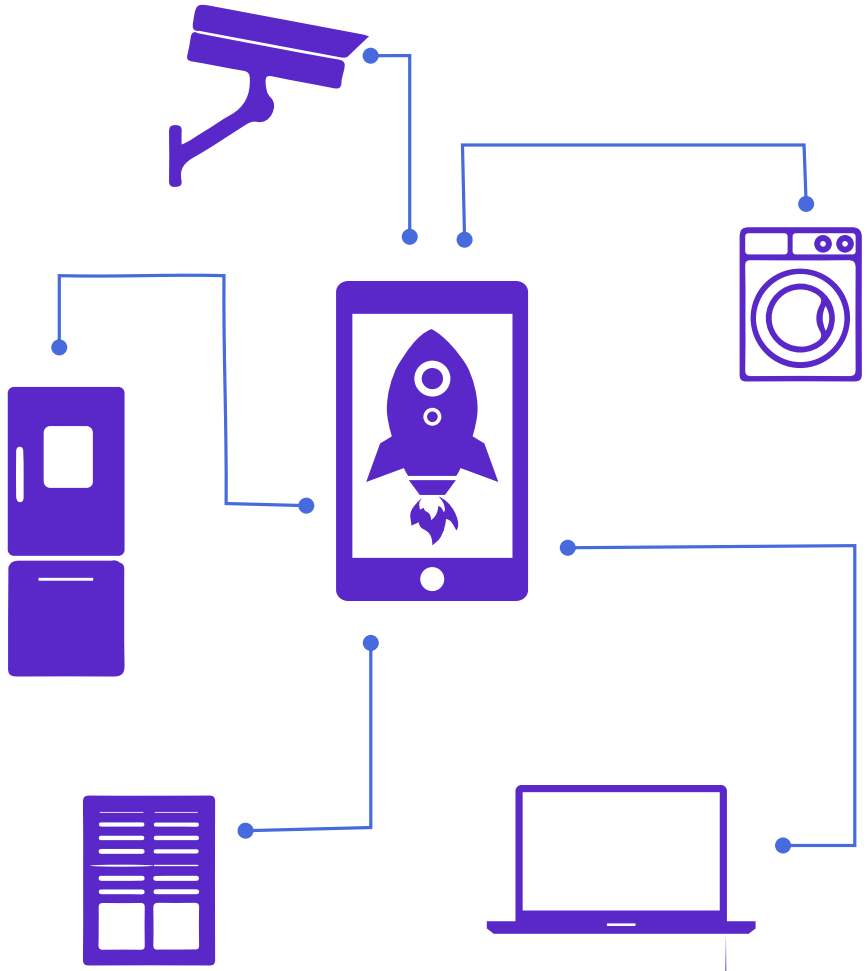
國立高雄師範大學

資訊超載與焦慮

源源不絕的訊息，超過自身可處理的量，將會引起負面效果。期待不斷得到某種資訊，將會引起焦慮。如股市、疫情。

暗網威脅

暗網(Dark Web)，是一種無法被搜尋引擎發現的網站，屬於深網的一種。一般人無法拜訪，需有特殊權限甚至專用軟體。如「絲路(Silk Road)」



網路謠言與假訊息

設刺揶揄、深度偽造、標題殺人、機器帳號、網軍、斷章取義、預期管理(帶風向)等。

網路犯罪

詐騙、援交、色情、恐嚇、毀謗、辱罵、侵權、言語霸凌、賭博、入侵他人網站、散佈病毒、散佈假訊息等。

國立高雄師範大學

資訊素養與倫理

Information Literacy & Ethics

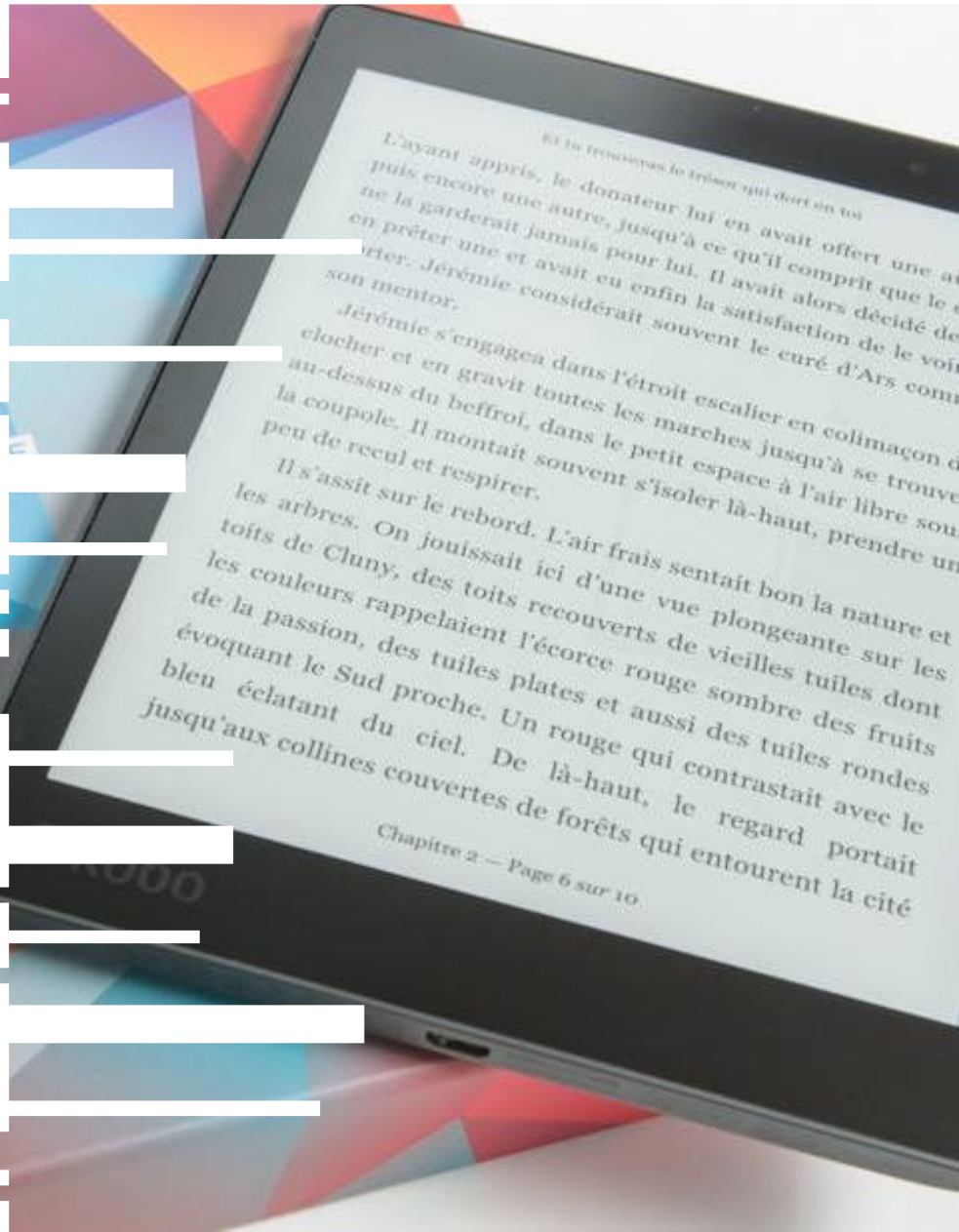
資訊素養與倫理

Information Literacy & Ethics

國立高雄師範大學

資訊素養，由美國圖書館學會(American Library Association, ALA)的主席於1974年首次提出，指的是個人能掌握並有效利用各種資源以利學習的能力。在1989年時美國圖書館學會的「資訊素養委員會」將其列入美國國民日常生活的必備技能。

確認 to identify	理解問題所需要的資訊，並籌劃如何尋獲。
尋獲 to locate	如何利用圖書館內的分類目錄和網路上的檢索尋找知識。
評估 to evaluate	對資訊版權的認知及理解。
使用 to use	辨別資訊的來源與真偽。



資訊素養的內涵及概念

國立高雄師範大學

保護自己的數位便捷生活

現今最重要的網路素養

國立高雄師範大學

有效的使用網路資源，並安全、合宜、合禮、合法地使用網路。
注重網路禮節，遵守網站的規章，勿亂轉發信件或訊息。

BBS
電子佈告欄

全球資訊網

留言板
聊天室

社群網站

元宇宙

Web 1.0

Web 2.0

Web 3.0

資訊倫理與PAPA

國立高雄師範大學

資訊隱私權
Privacy

資訊正確權
Accuracy

資訊倫理
Information Ethics

資訊財產權
Property

資訊存取權
Access

著作權的觀念

國立高雄師範大學

一般資料

姓名、生日、身分證字號、指紋、特徵、家庭、財務情況、社會活動等

特種資料

醫療、基因、性生活、健康檢查、犯罪前科。

行為定義

蒐集、處理、利用。

其他資料

得以直接或間接方式識別該個人之資料。

個人資料保護法

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。

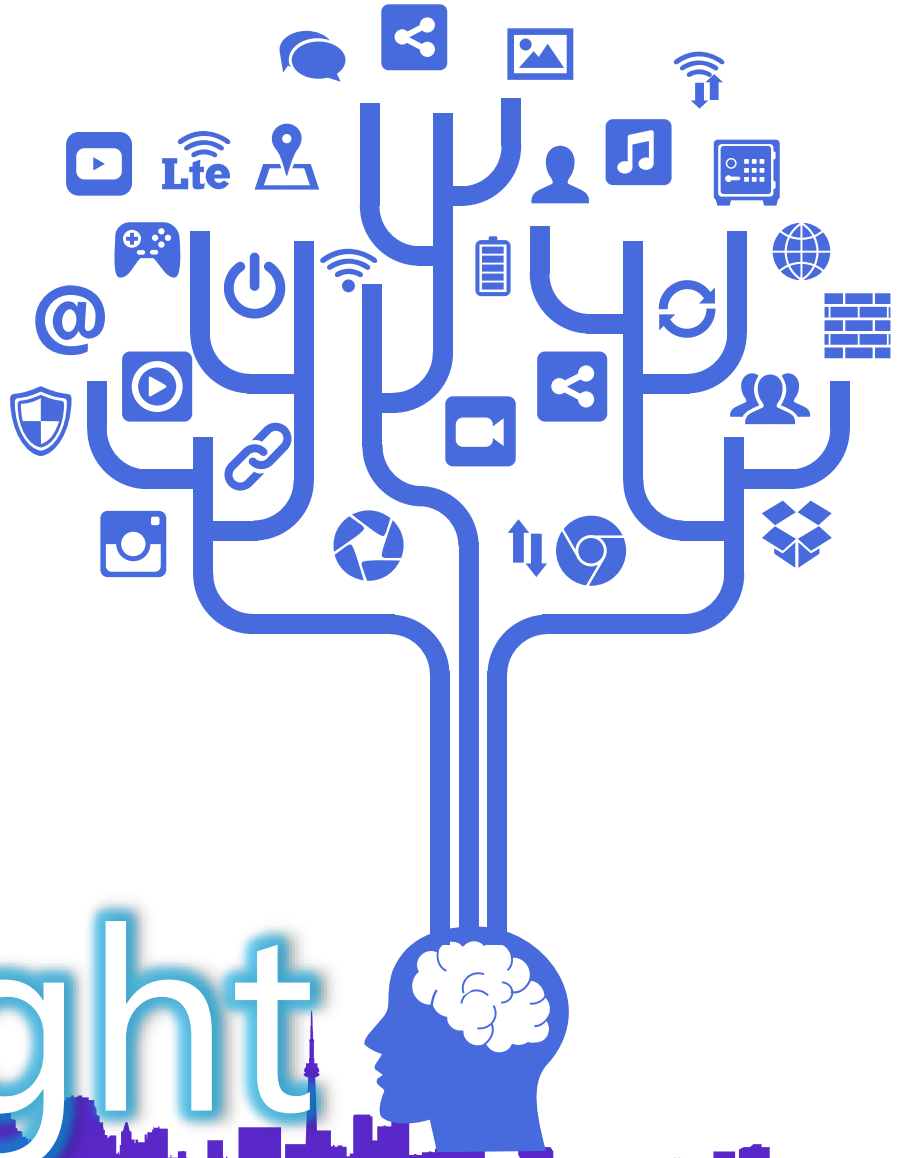
規範對象

公務機、非公務機關、法人、自然人。

前身為民國84年所公布施行之《電腦處理個人資料保護法》

為因應社會現況，擴大適用範圍，於民國101年10月1日上路。

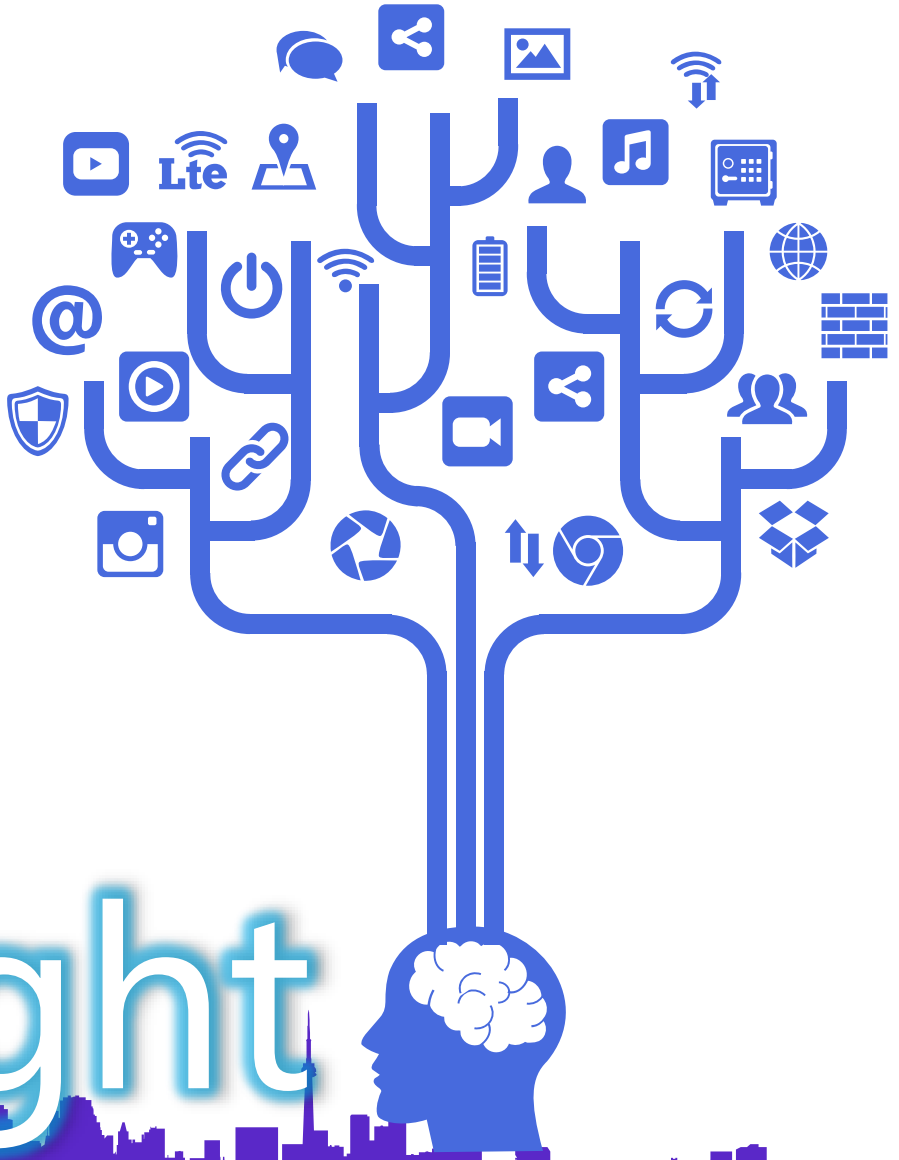
著作權的觀念



- 由**國家制定法律保障著作創作者的權益**，法律所規定的這些權利稱為著作權。
- 著作**完成時**創作者立即享有著作權。
- 效期為著作人**終生+50年**。
- 著作權包括了**人格權**與**財產權**兩部分。
- 著作權法的**落實**是邁向已開發國家的象徵。

Copyright

著作權的觀念



- **著作人格權**：來保護著作人的名譽、聲望及人格利益。著作人的人格無法分離，因此不可以讓與或繼承。(包括公開發表權、姓名表示權及禁止不當修改權)

- **著作財產權**：賦予著作人財產上的權利，使其獲得實質上經濟利益，促使著作人繼續從事創作活動，精進創作質與量。(重製權、公開口述權、公開播送權、公開上映權、公開演出權、公開傳輸權、公開展示權、改作權、編輯權、出租權及散布權，共11種)

- **使用他人著作時，不可侵害到人格權，且應得到著作財產權人的同意或授權。**

Copyright

著作權的觀念

國立高雄師範大學

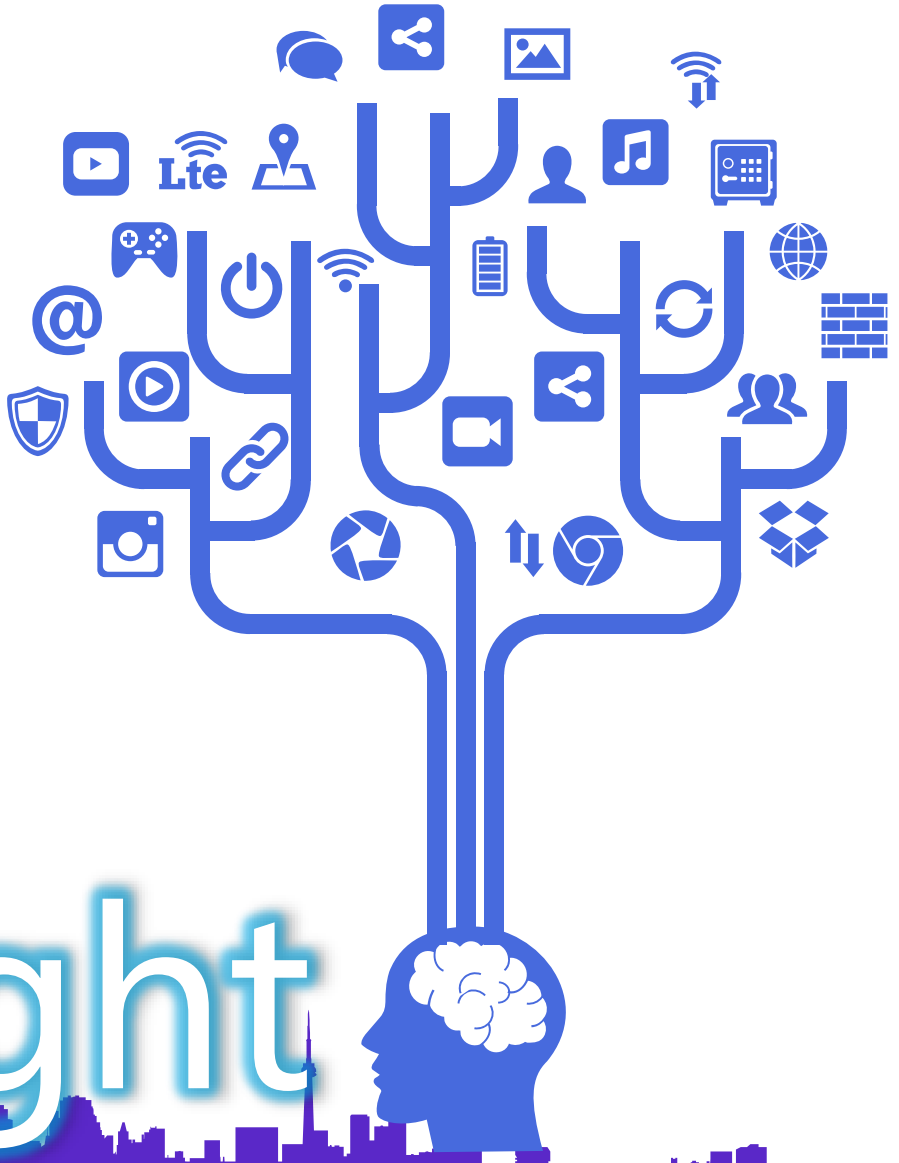
著作權法第11條第1項至第3項：

受雇人於**職務上完成之著作**，以該**受雇人為著作人**。**但契約約定以雇用人為著作人者，從其約定**。

依前項規定，以受雇人為著作人者，其**著作財產權歸雇用人享有**。但契約約定其**著作財產權歸受雇人**享有者，從其約定。

前二項所稱受雇人，包括公務員。

公司與員工間關於「職務上完成的著作」，可透過契約約定著作權的歸屬是屬於公司或員工，但如果**沒有契約特別規定**的時候，原則上**應以受雇人為著作人**，而享有**著作人格權**，但著作**財產權則歸屬於公司享有**。



Copyright

著作權的合理使用原則

國立高雄師範大學

1. 利用之目的及性質，包括係為商業目的或非營利。
2. 著作本身的性質。
3. 所利用之質量及其在整個著作所佔之比例。
4. 利用結果對著作潛在市場與現在價值之影響。

著作權的合理使用原則

國立高雄師範大學

「重製」依據目前的規定涵蓋了以物理和非物理方式重復製作該著作的行為皆包含在內。在一般情形下，除本法另有規定外，著作人享有重製其著作之權利。

合理使用規範：

- 教育文化目的
- 一般家庭或個人的非營利目的
- 身心障礙族群的合理使用

著作權的合理使用原則

國立高雄師範大學

「公開播送」係指以公眾直接收聽或收視為目的，以有線電、無線電或其他器材之廣播系統傳送訊息之方法。

合理使用規範：

- 為教育目的需求
- 非營利目的使用

我國著作著法目前對於「公開傳輸」的合理使用規範，限定較為嚴格，較少有合理使用的解釋空間，應特別注意觸法可能。

實例介紹

國立高雄師範大學

成大

MP3

事件

奧運

主題

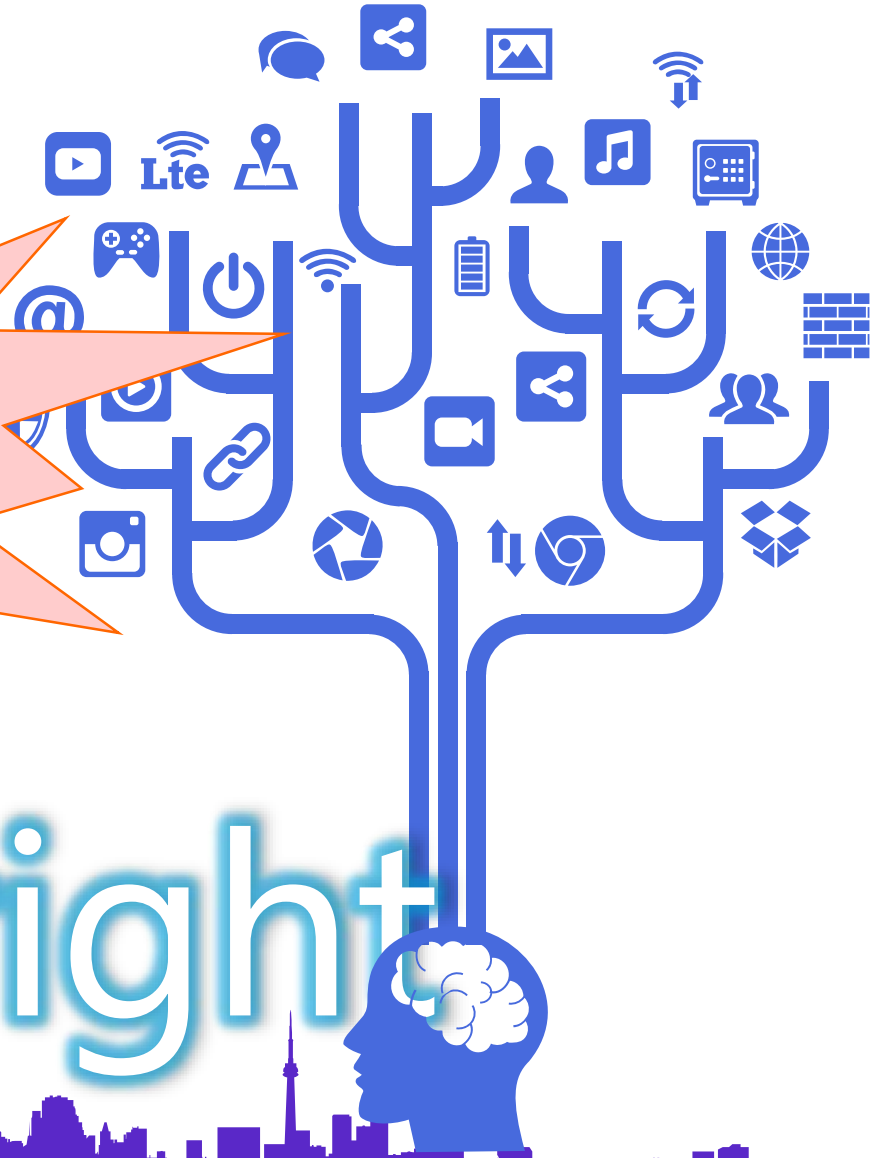
曲

地震

速報

APP

注意!!
授權並非權利的移轉，必須注意授權內容及範圍



Copyright

近期實例介紹

國立高雄師範大學

健行科技大學
CHIEN HSIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

國立屏東大學
National Pingtung University

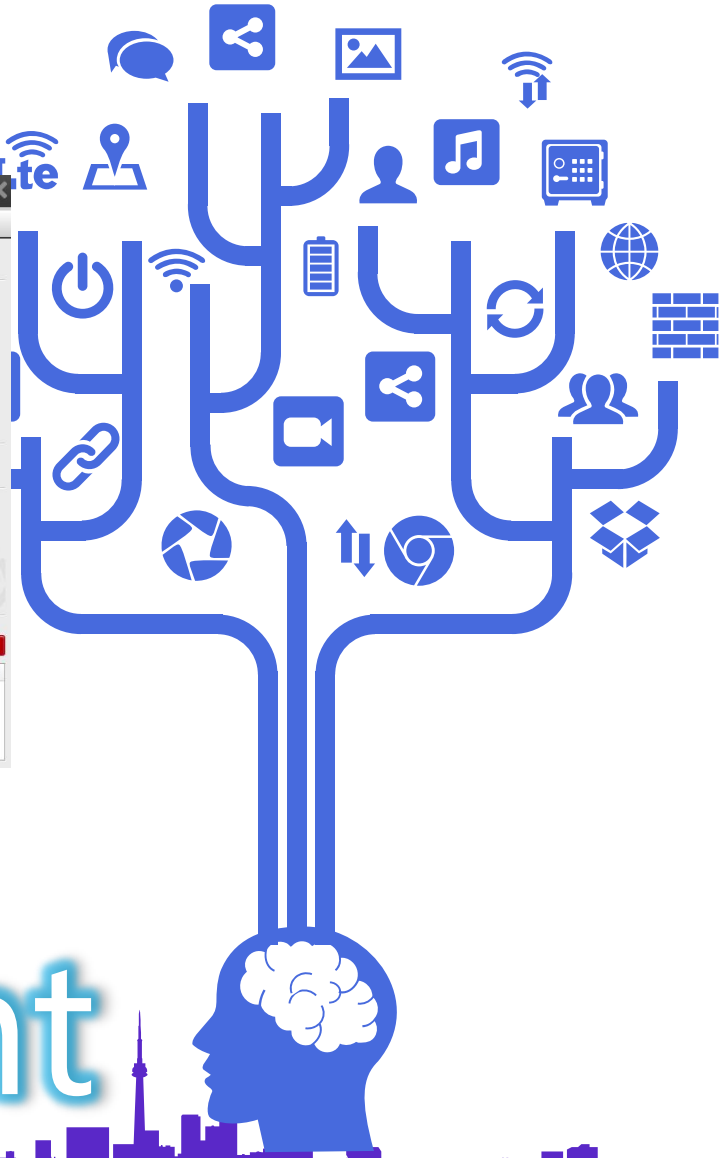
最終屏大以100萬元與楊姓 設計師達成和解並取得授權。

近期實例介紹

國立高雄師範大學

地震速報APP

地牛 Wake up !



國立高雄師範大學

個人資料的保護

Personal Data Protected

保護自己的數位便捷生活

個人資料的保護

國立高雄師範大學

一般資料

姓名、生日、身分證字號、指紋、特徵、家庭、財務情況、社會活動等

特種資料

醫療、基因、性生活、健康檢查、犯罪前科。

行為定義

蒐集、處理、利用。

其他資料

得以直接或間接方式識別該個人之資料。

規範對象

公務機、非公務機關、法人、自然人。

個人資料保護法

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。

前身為民國84年所公布施行之《電腦處理個人資料保護法》

為因應社會現況，擴大適用範圍，於民國101年10月1日上路。

現實狀況的情境探討

國立高雄師範大學

變造影片

肉搜

醫療資料

攝影

學校公佈欄

求職求才資料

促銷通知訊息

歐盟的個案

一名西班牙男子於2011年到法院，要求當地報章刪除一篇有關他16年前因陷入財政危機，無力交稅而被迫拍賣事業的報導。
該男子雖早已還清債務，但事隔多年仍能在網路上搜尋到相關內容，男子認為影響其名譽因而控告Google。
歐盟法院最終於2014年5月裁定Google敗訴，確立歐洲公民享有「被遺忘權」。

歐盟使用「一般資料保護規範(General Data Protection Regulation, GDPR)」做為資料保護規範。

被遺忘權：數據主體有權要求數據控制者永久刪除有關數據主體的個人數據，有權被網際網路所遺忘，除非數據的保留有合法理由。

國立高雄師範大學

校園資訊安全教育

Information Security Education in Campus

保護自己的數位便捷生活

校園資訊安全教育

國立高雄師範大學

家長與教師

1. 指導、建議和監督的角色，確保孩子在資訊世界活動中的安全。
2. 家長和教師更應該了解網路世界的風險，並教導孩子如何適當地應對這些風險，保護個人隱私和安全。
3. 建立與孩子之間開放和溝通的關係，鼓勵他們分享使用資訊工具及活動中的經歷。
4. 校園應該推動資訊安全教育活動，例如講座、工作坊或資訊安全相關課程。例如今天的演講。

培養資安素養

資安素養能夠幫助個人適應快速變化環境，幫助學生彈性應對未來可能的威脅和挑戰。
學校可以舉辦相關競賽、實踐活動等，使學生自然而然讓資訊素養融入生活當中。

學生的責任與自我保護

1. 學生需學會辨別和應對網路中的各種風險和威脅，建立自我保護意識。
2. 透過對資安的正確認識程責任感的建立，提高自主判斷能力，提升自信心，進而應對高風險情況。
3. 學生應接受定期資訊安全教育，學習如何保護個人隱私、如何建立強大密碼、如何辨識網路詐騙等。
4. 學生應遵守校園的資訊安全政策和規定，不輕易洩漏個人資料，不參與非法的網路活動。

國立高雄師範大學

謝謝您的聆聽

Thanks for your attention

廖仁宏