# 資安與個資保護之道

## 從日常生活到法規遵循


114年08月27日
國立宜蘭大學 蔡雅芳 技術員

宜蘭區網中心
ILAN REGIONAL CENTER

# 資訊安全

# 個人資料

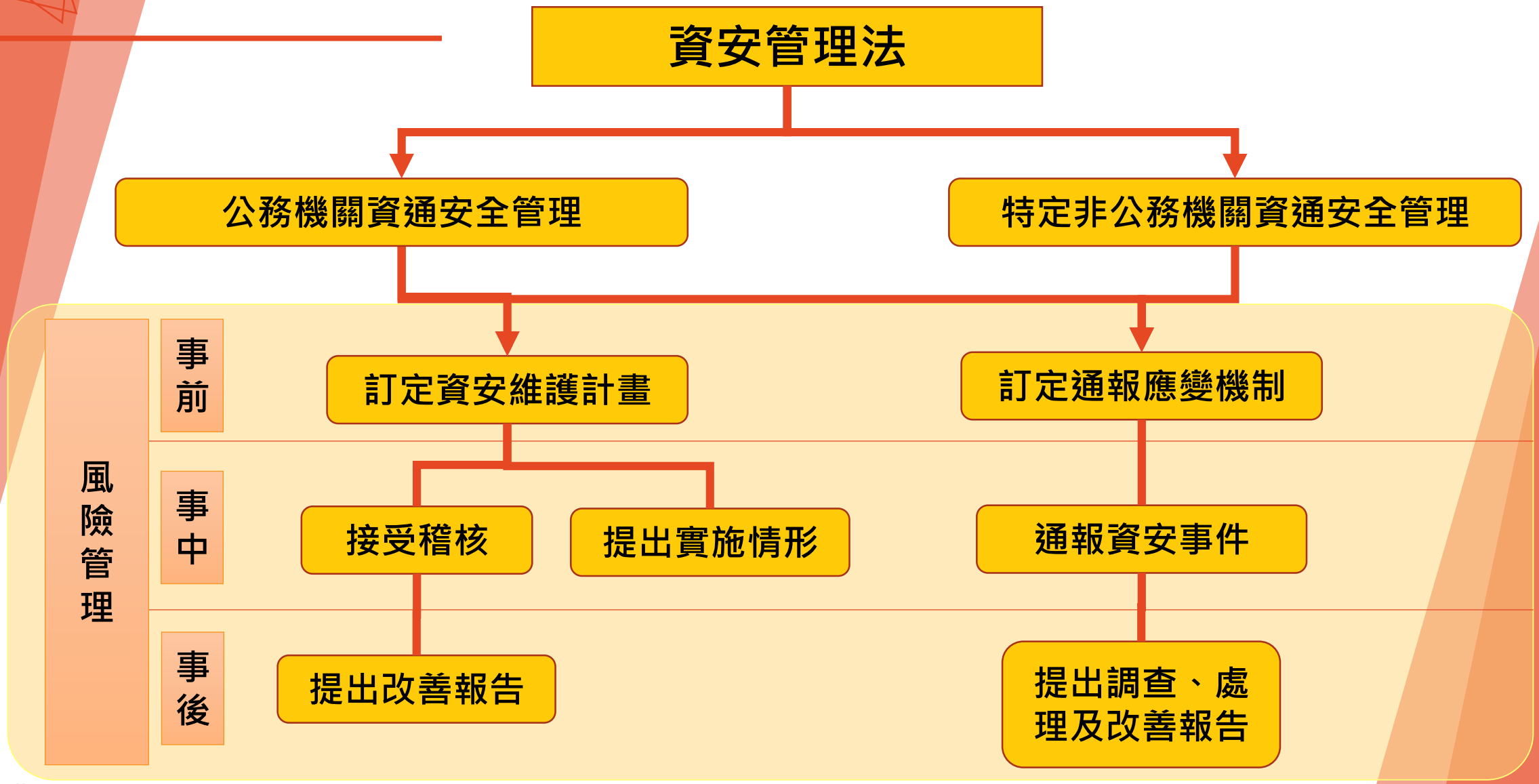

宜蘭區網中心
ILAN REGIONAL CENTER

# 資通安全管理法

實施日：108.01.01


宜蘭區網中心
ILAN REGIONAL CENTER

# 資安法架構


資安管理法
公務機關資通安全管理
特定非公務機關資通安全管理
風險管理
事前
事中
事後
訂定資安維護計畫
訂定通報應變機制
接受稽核
提出實施情形
通報資安事件
提出改善報告
提出調查、處理及改善報告

# 資安跟我們生活有什麼關係？

## 詐騙

你收到一封假的「銀行簡訊」，點進去輸入資料，結果帳戶被盜。

## 資料外洩

你存在雲端的照片被駭客偷走，甚至拿去賣。

## 勒索

電腦被病毒鎖住，壞人要求你付錢才能解鎖。

# 為什麼資安很重要？

資安不只是技術人員的事，而是關係到
我們每個人的學習、教學與生活。
資訊安全做得好，才能確保：

1 **確保校務無中斷**

維護關鍵系統的穩定運作，避免資安事故造成校務中斷。

2 **保護教學資料**

確保教學資料的完整性和安全性，讓教學活動不受影響。

3 **保護個人隱私**

防止學生和教職員的個人資訊外洩，維護自身的隱私權。

4 **避免財務損失**

降低資安事故造成的財務損失和聲譽受損，保護學校利益。

# 生活中怎麼保護資安?

1.**設好密碼**：別用「123456」或生日當密碼，換成複雜一點的，像「IlovePizza2025!」。

2.**小心釣魚**：收到奇怪的簡訊或email（像是「您的包裹有問題，點此領取」），別亂點，可能是詐騙。

3.**更新軟體**：手機或電腦跳出「更新」通知，別偷懶，更新能修補安全漏洞。

4.**備份資料**：重要照片、文件記得多存一份到隨身碟或雲端，以防萬一。

5.**用雙重認證**：像Gmail或銀行帳戶可以設「簡訊驗證」，多一層保護。

# 資訊安全的三大重點


## 不讓別人偷看（機密性）

就像你不希望鄰居隨便翻你的日記，資安確保你的資料（例如LINE聊天、信用卡號）只有你和授權的人能看。

生活例子：你設了手機密碼或指紋鎖，這樣別人拿你手機也看不到你的資料。

## 不讓別人亂改（完整性）

想像你寫了一封重要的email，結果被壞人偷偷改成亂七八糟的內容。資安就是要保證你的資料不會被竄改，保持原樣。

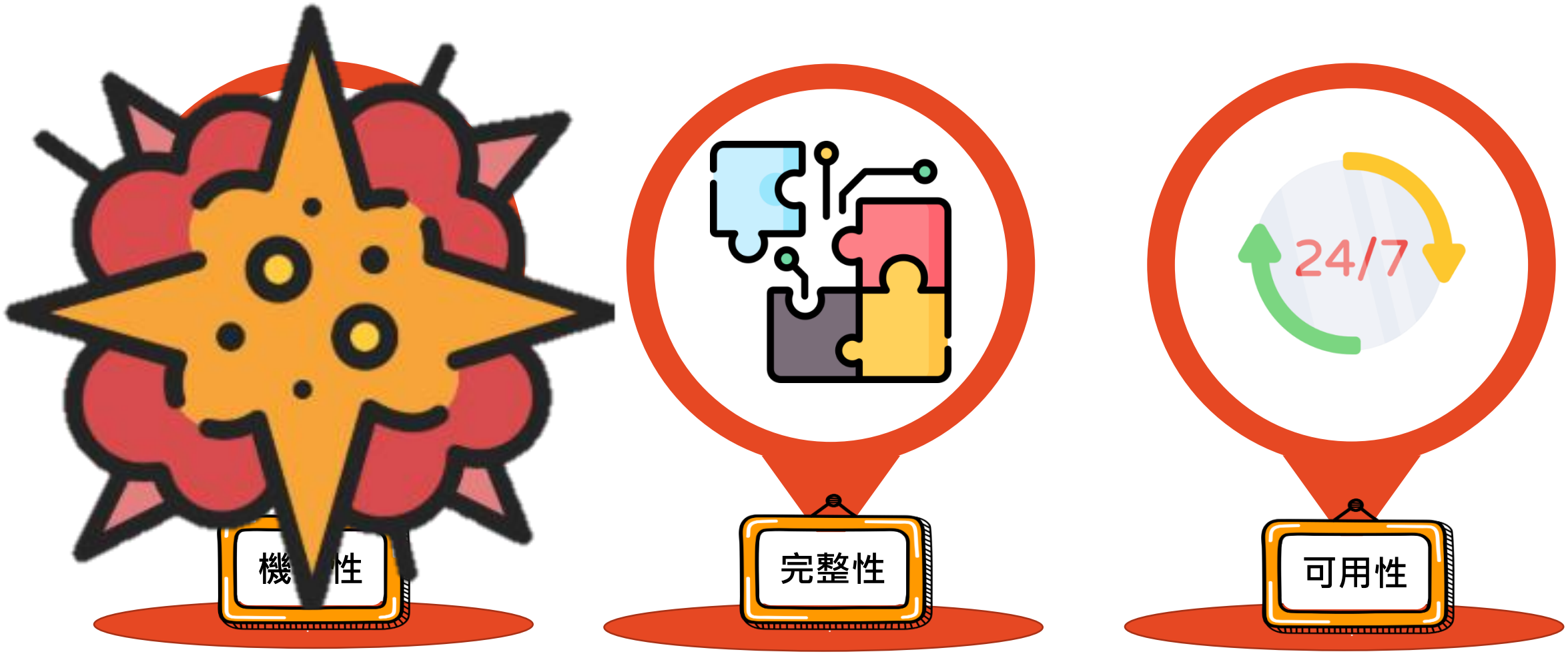
生活例子：你傳照片給朋友，資安確保照片不會被惡意改成別的圖。

## 隨時都能用（可用性）

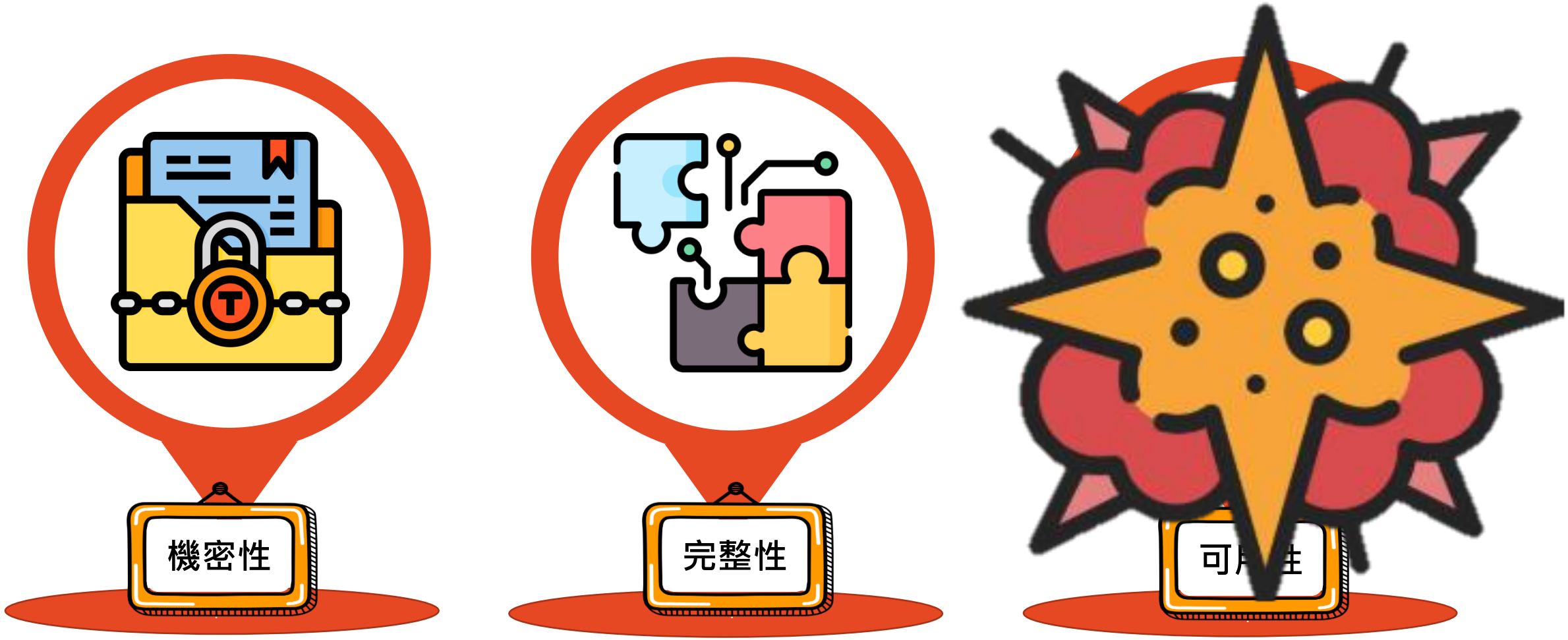
你想用網路銀行轉帳，結果網站掛了，半天登不進去，這就是可用性出了問題。資安要確保你的系統或服務隨時能正常用。

生活例子：像LINE或Google突然當機，你就知道有多麻煩，資安就是要避免這種情況。

# 機關同仁誤點釣魚郵件，造成通訊錄外洩



# 系所網站因為DDoS攻擊導致網頁無法顯示



# 資訊安全-常見案例分享1

## 案例1：網路釣魚簡訊騙取銀行資料

**情境：**小明收到一則簡訊：「**您的銀行帳戶有異常，請點此連結更新資料！**」他點進去，輸入帳號、密碼，還填了身分證號。結果，這是詐騙網站，帳戶被盜，存款被轉走。


**資安問題：**網路釣魚（Phishing）攻擊，騙取個人敏感資料，違反 **機密性**。

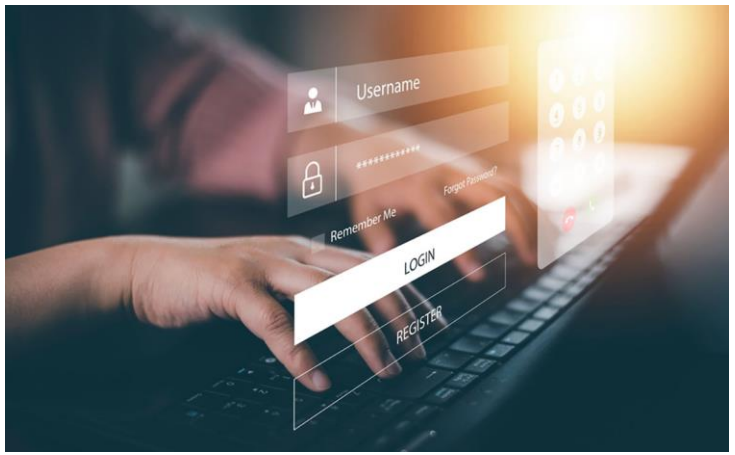
**影響：**財務損失、個人資料外洩，甚至可能影響信用。


**防範方法：**

- 不要隨意點擊簡訊或email中的不明連結。
- 檢查網址是否正確（例如，銀行官方網址通常是「www.bankname.com.tw」，不會有怪怪的字尾）。
- 開啟銀行帳戶的雙重認證（例如簡訊OTP），增加安全層。

# 資訊安全-常見案例分享2

## 案例2：用生日當Wi-Fi密碼被鄰居破解


**情境：**小花把家裡Wi-Fi密碼設成她的生日「19950315」，鄰居猜到密碼，連上她的Wi-Fi，不只偷用網路，還入侵她連網的智能家電，偷看攝影機畫面。

**資安問題：**弱密碼與未加密的Wi-Fi，導致未授權存取，違反**機密性**與**完整性**。

**影響：**隱私曝光、網路被濫用，甚至可能被用來進行其他攻擊。

**防範方法：**

- Wi-Fi密碼設成複雜組合（例「MyCat2025!WiFi」）。
- 使用WPA3或至少WPA2加密協定。
- 定期檢查連線設備，關閉不必要的遠端存取功能。

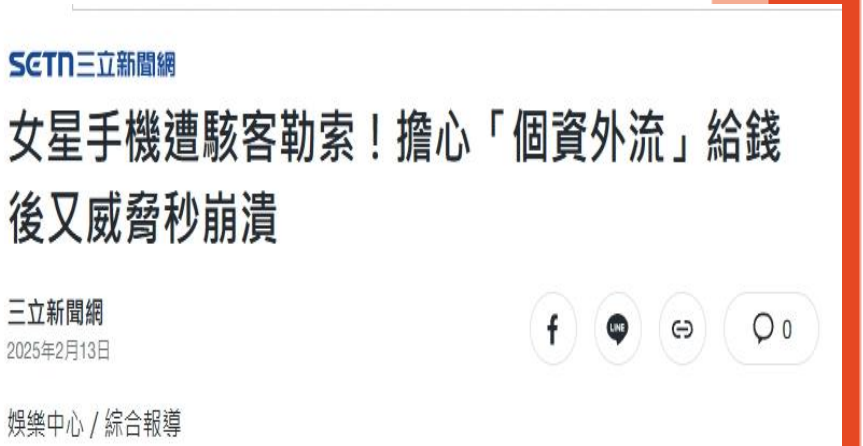
# 資訊安全-常見案例分享3

## 案例3：手機沒更新被勒索軟體鎖住

**情境：**阿偉的手機好幾個月沒更新系統，某天點了一個來路不明的免費遊戲APP，結果手機被勒索軟體鎖住，螢幕顯示「付1000美元解鎖」。導致他無法使用手機，照片和文件也打不開。


**資安問題：**惡意軟體（Malware）與未修補的系統漏洞，影響可用性與完整性。

**影響：**資料損失、設備無法使用，支付贖金疑慮或重置手機。


SETN三立新聞網

女星手機遭駭客勒索！擔心「個資外流」給錢後又威脅秒崩潰

三立新聞網
2025年2月13日

娛樂中心 / 綜合報導

**防範方法：**

- 定期更新手機作業系統和APP，修補安全漏洞。
- 只從官方商店（如Google Play、App Store）下載應用程式。
- 重要資料定期備份到雲端或外接硬碟。

# 資訊安全-常見案例分享4

## 案例4：咖啡廳用公共Wi-Fi被竊聽


**情境：**小芳在咖啡廳用公共Wi-Fi查詢銀行餘額，沒注意網站沒加密（網址是「http://」而非「https://」）。駭客在同一個Wi-Fi網路攔截她的帳號密碼，後來盜用她的帳戶。

**資安問題：**未加密的通訊與不安全的公共Wi-Fi，違反機密性。

**影響：**帳戶被盜、個人資料外洩。

**防範方法：**

- 使用公共Wi-Fi時，開啟VPN（虛擬私人網路）加密連線。
- 確認網站使用「https://」並有鎖頭圖示。
- 定期檢查連線設備，關閉不必要的遠端存取功能。

TVBS 新聞網

**郵輪WiFi藏危機！女花8千買網路 24萬「瞬間被清空」**

簡雅婷 林亞男

2025年7月16日

14

宜蘭區網中心 ILAN REGIONAL CENTER

# 資訊安全-常見案例分享5

## 案例5：社群媒體帳號被盜用發詐騙訊息

**情境：**小強的Instagram帳號用簡單密碼「password123」，被駭客破解。駭客用他的帳號向朋友發訊息：「我急需用錢，幫我轉5000元！」結果朋友被騙，損失金錢。


**資安問題：**弱密碼與缺乏雙重認證，導致未授權存取，違反機密性。

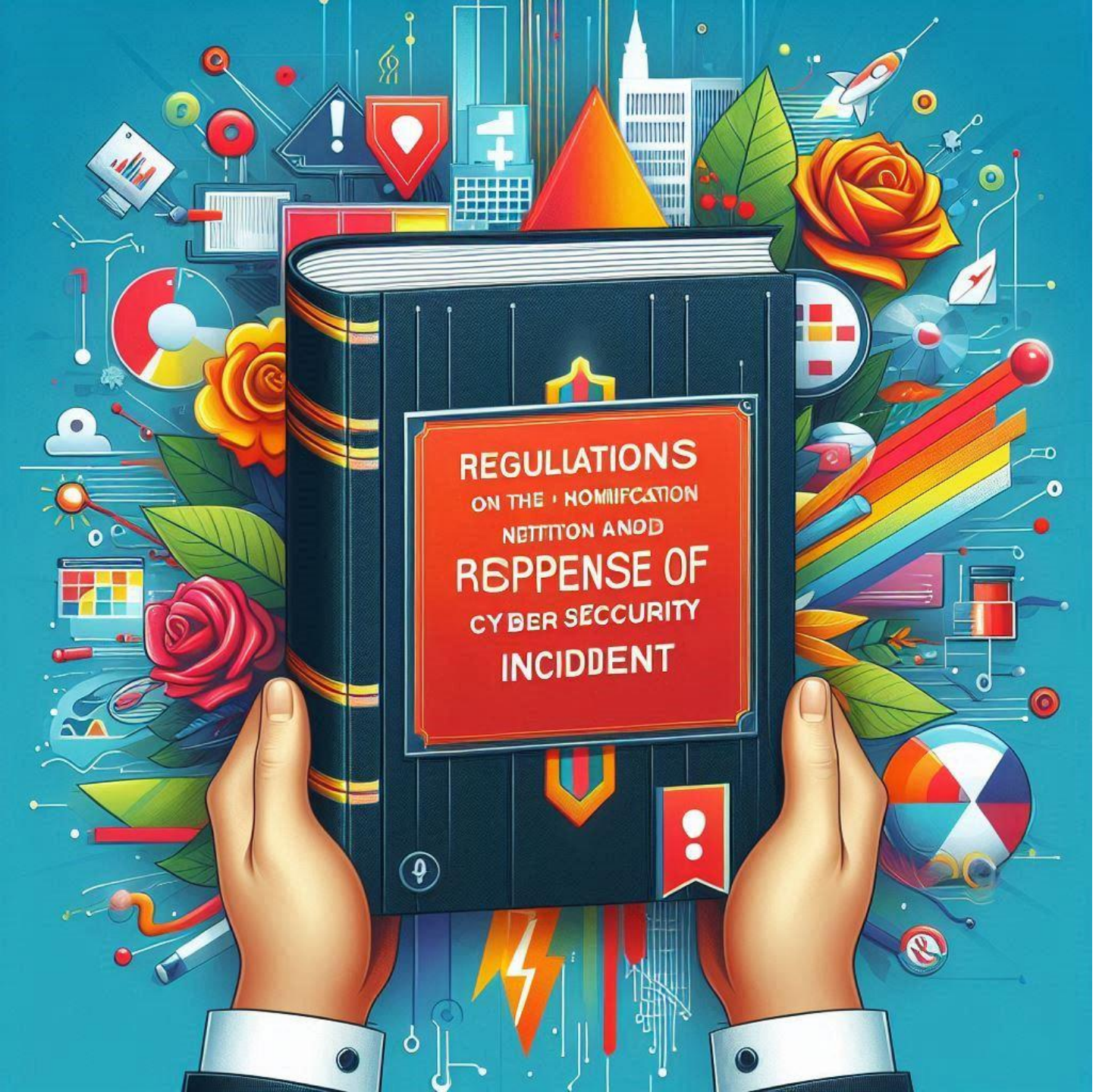
**影響：**　　個人帳號被盜、朋友受騙、聲譽受損。

**防範方法：**

- 使用強密碼（結合大小寫、數字、符號，例如「Sunny2025!Ig」）。
- 開啟雙重認證（2FA），例如收到簡訊驗證碼或使用認證APP。
- 定期檢查帳號是否有異常登入紀錄。

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU

宜蘭區網中心 ILAN REGIONAL CENTER



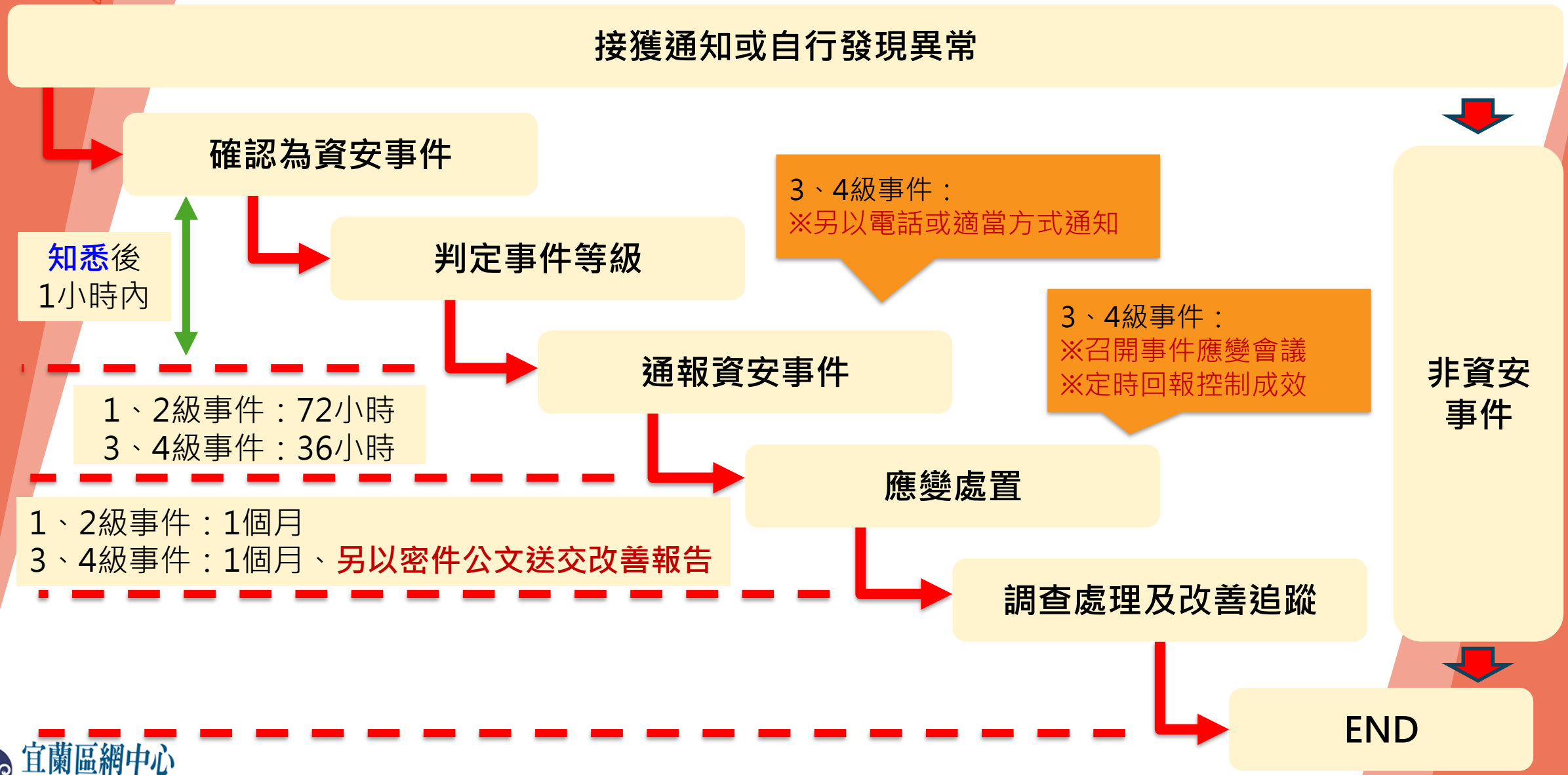

# 資通安全事件通報及應變辦法

# 資安事件分為4個等級

| | 機密性(C) | | 完整性(I) | | 可用性(A) | |
|---|---|---|---|---|---|---|
| | 輕微洩漏 | 嚴重洩漏 | 輕微竄改 | 嚴重竄改 | <可容忍時間 | >可容忍時間 |
| 非核心業務/系統 | 1級 | 2級 | 1級 | 2級 | 1級 | 2級 |
| 核心業務/系統(未涉及CI) | 2級 | 3級 | 2級 | 3級 | 2級 | 3級 |
| 核心業務/系統(涉及CI) | 3級 | 4級 | 3級 | 4級 | 3級 | 4級 |
| 一般公務機密、敏感資訊 | 3級 | 4級 | 3級 | 4級 | | |
| 國家機密 | 4級 | 4級 | 4級 | 4級 | | |

個人資料

# 資通安全事件通報流程


接獲通知或自行發現異常
確認為資安事件
知悉後
1小時內
判定事件等級
3、4級事件：
※另以電話或適當方式通知
通報資安事件
1、2級事件：72小時
3、4級事件：36小時
3、4級事件：
※召開事件應變會議
※定時回報控制成效
應變處置
1、2級事件：1個月
3、4級事件：1個月、另以密件公文送交改善報告
調查處理及改善追蹤
非資安事件
END

# 資訊安全-日常危機嚴謹看待

## 提升防範意識　增加風險概念

案例顯示資安問題無處不在，像是釣魚簡訊、弱密碼、公共Wi-Fi或惡意軟體，都可能讓你的資料、錢財或隱私暴露在風險中。

簡單的防範習慣（強密碼、更新系統、謹慎點擊）就能大大降低風險。

就像出門會鎖門，數位世界也要隨手「鎖好」你的資料！

# 有資安疑慮或異常時怎麼辦？

**選我正解：**

**當然是聯絡資安窗口**

**「註冊組電話:03-9509788分機112」**

## 1 個資外洩的風險

個資外洩的風險一：成為詐騙與廣告目標、帳號被盜用、銀行資金被竊取、身份被冒用、企業商業機密、商譽受損

## 2 個資保護法-個資處理原則、罰則

個資法並非一味的限制個人資料的運用，而是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

## 3 個資外洩案例

常見個資外洩原因有誤寄Email、附件未加密、誤設定資料公開、實體文件遺失、設備遺失、惡意攻擊、ChatGPT聊天小心洩漏個資

## 4 個資保護的落實方法

要做好個人資料的保護，基本上有賴於科技、管理與法律三大要素的結合與有效運作。

# 什麼是個人資料呢?

**個人資料保護法第二條第一項明訂**


## 一般個資:

姓名
出生年月日
身分證號碼
護照號碼
特徵
指紋
婚姻
家庭
教育
職業
聯絡方式
財務情況
社會活動

## 特種個資

病歷
醫療
基因
性生活
健康檢查
犯罪前科

## 其他

得以直接或間接方式識別該個人之資料

例如：婚姻史
家庭成員的細節
學校紀錄
學習過程
受僱情形

# 什麼是個資保護法? 人格權保護

## 個資法

訂定了個人資料的定義、合法收集和使用的條件，及個人的權利。


## 未經授權(沒有取得同意)

如果未經授權擅自蒐集或利用個資，將面臨高額罰款和其他懲罰。而個人也能向主管機關申訴，維護自己的隱私權。

## 一言以蔽之

個資法並非一味的限制個人資料的運用，而是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

# 為什麼教職員要重視個資保護?

## 個資外洩頻傳

近年個資外洩事件頻傳，教育單位尤須重視

## 校譽受損

學生、家長、同仁的資料安全是責任

一旦外洩可能涉及法律責任與名譽損失

## 法律責任

個資法有明文規範

民事責任

刑事責任

# 個資定義-個人資料無處不在

EMAIL、帳戶資料、帳單地址


宅配地址、信用卡資料、使用者註冊資料、周年慶抽獎卷

病歷資料、健檢報告、診斷書


保單資料、帳戶資料、貸款徵信資料、會員資料

身分證、結婚登記、報稅資料、駕照申請換發

學籍資料、人事資料、註冊報名資料、畢業校友聯絡資料

# 個資敏感系統有哪些?


教職員、學生填寫紙本資料


辦公室電腦教職員、學生資料檔案

# 個人資料值多少?

## 暗網價格表(2023年)

| 類別 | 產品 | 暗網平均價格（美元） |
|---|---|---|
| **信用卡數據** | 信用卡詳細信息，帳戶餘額最高可達5000 | 110美元 |
| | Card.com 帳號被駭 | 75美元 |
| | 信用卡詳細信息，帳戶餘額最高可達1000 | 70美元 |
| | 網路銀行登入資料被盜，帳戶餘額至少 2,000 美元 | 60美元 |
| | 帶有 CVV 碼的阿聯酋信用卡 | 35美元 |
| | 網路銀行登入資料被盜，帳戶至少有 100 個 | 40美元 |
| | TDBank帳戶被盜 | 30美元 |
| | 加拿大駭客竊取信用卡CVV資訊 | 30美元 |
| | 澳洲駭客竊取信用卡CVV訊息 | 23美元 |
| | 以色列竊取信用卡CVV資訊 | 20美元 |
| **社群媒體** | 被駭客入侵的 Gmail 帳戶 | 60美元 |
| | 駭客入侵 Facebook 帳戶 | 25美元 |
| | Instagram 帳號被駭 | 25美元 |
| | 推特帳號被駭 | 20美元 |
| | Twitter 轉寄 x 1000 | 10美元 |
| | LinkedIn 公司頁面追蹤者 x 1000 | 5美元 |
| | Instagram 粉絲 x 1000 | 2美元 |
| | Pinterest 粉絲 x 1000 | 2美元 |
| | Twitch 粉絲 x 1000 | 2美元 |
| | Instagram 讚 x 1000 | 2美元 |

https://www.privacyaffairs.com/dark-web-price-index-2023/

# 個資管理-處理利用原則

## 正確性

保持個人資料正確性

## 告知當事人

告知當事人蒐集資料的特定目的、安全處理與使用方式及範圍

## 保管、刪除、銷毀

做好個人資料確實的保管、刪除與銷毀工作

## 別過度反應

別因為擔心會違反個資法，卻導致過度的避免或迴避相關必要資料的蒐集與利用。

宜蘭區網中心
ILAN REGIONAL CENTER

# 個資管理-生命週期

1.蒐集

◎依法進行**告知**義務
◎取得書面同意

2.處理

採取適當保護措施，避免個資被竊取、竄改或毀損

紙本處理方式
例:個資影印本如何保護?

3.利用

◎應於蒐集之特 定目的內使用

◎特定目的外之使用應另外取得書面同意

學生資料轉移

4.儲存

採取適當保護措施，避免個資被竊取、竄改或毀損

5.銷毀

保存越久風險越高

銷毀紀錄要留存

◎特定目的消失
◎期限屆滿
◎當事人要求

# 罰則-違反個人資料保護法，有哪些法律責任

## 民事責任

- 原告是否因個人資料之相關權益受損，得向被告請求損害賠償。
- 由當事人進行訴訟
- 由法院判決被告進行金錢賠償或回復名譽

## 刑事責任

- 被告是否有違反個人資料保護法而應受刑事制裁
- 由國家進行訴訟
- 處以有期徒刑、拘役或罰金

# 個資管理-個資蒐集、處理與利用的合法原則

合法、特定、明確之目的

目的拘束原則： 個人資料之蒐集、處理或利用，應尊重當事人權益，依誠實及信用方法為之

特定目的限制： 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

取得當事人同意的重要性與範圍

告知義務：蒐集個資前應明確告知蒐集目的、個資類別、利用期間及方式等

書面同意：特定目的外利用個資，應獨立作成書面同意，確保當事人充分了解

最低必要原則與保存期限

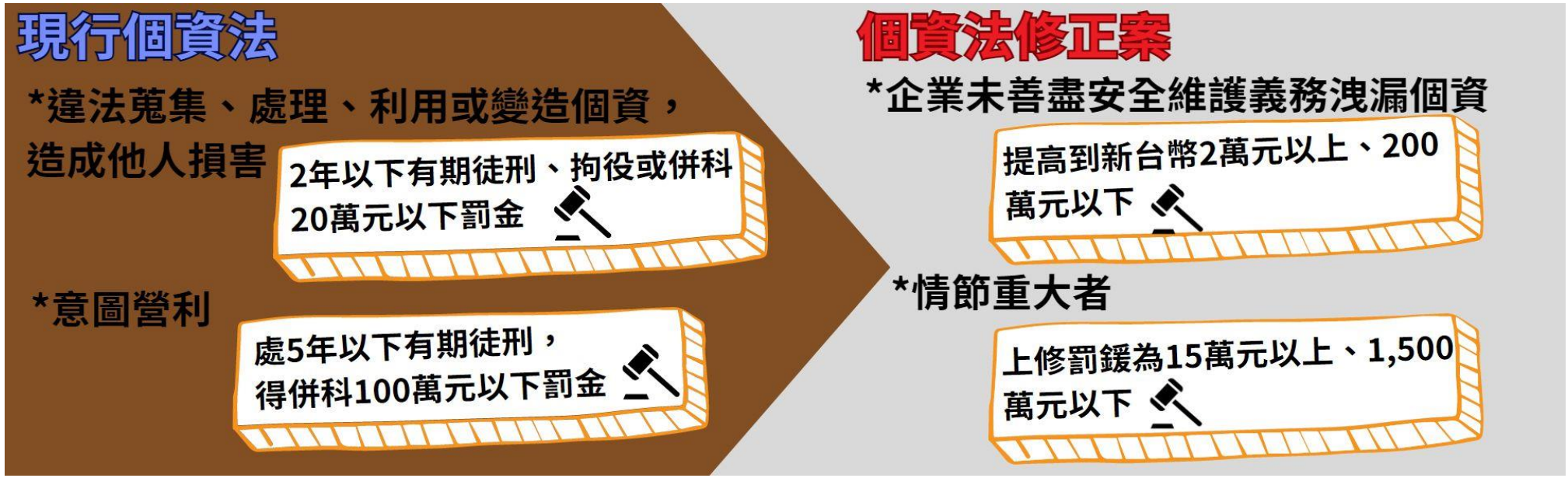
最小化原則：僅蒐集為達成目的所必要之最少資料，避免過度蒐集

保存期限：應依特定目的之存續期間或法令規定之保存期限保存，期限屆滿應主動刪除

# 罰則-個資外洩罰多少?

**▲立院三讀通過個資法修法，企業外洩個資可直接開罰要求改善，最重可罰1,500萬元**

個資外洩案件頻傳，立法院會於2023/ 5/ 16日三讀通過「個人資料保護法修正案」，**針對非公務機關（即企業）未善盡安全維護義務洩漏個資，將罰鍰提高到新台幣2萬元以上、200萬元以下，屆期未改正將按次處罰；對情節重大者，上修罰鍰為15萬元以上、1,500萬元以下。**



# 釣魚簡訊(Smishing)

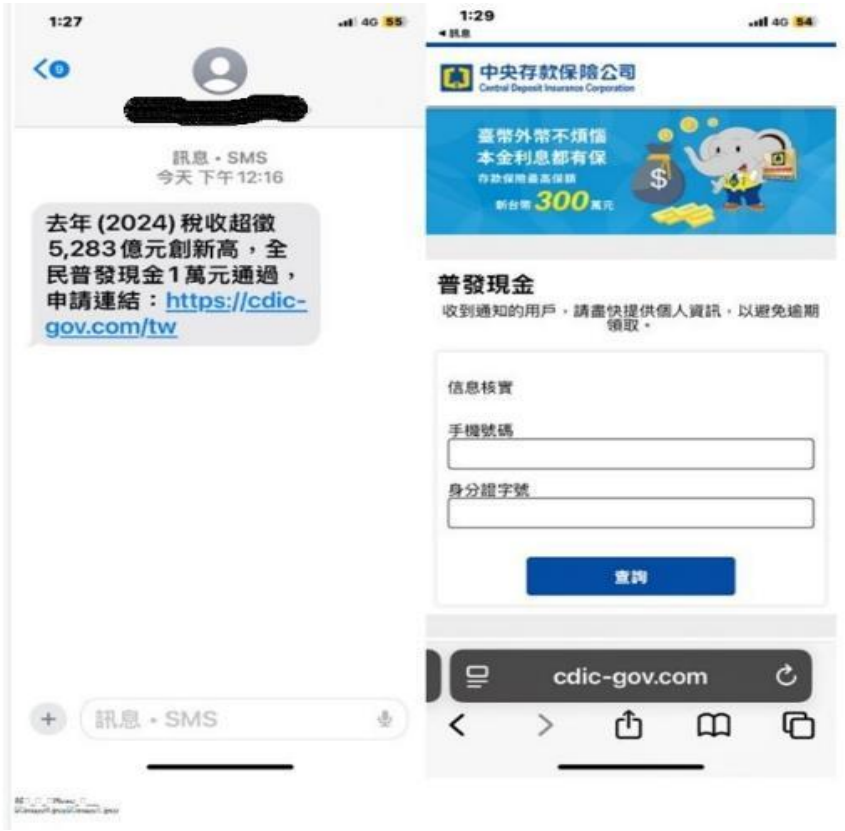
## 常見釣魚簡訊類型

### 假冒機構
假冒銀行、電信、政府單位：要求點擊連結更新資料。

### 獎品誘惑
獎品、優惠誘惑：點擊領取獎品，實則竊取個資。

### 虛假通知
包裹、罰單通知：假冒物流或政府單位，引導至惡意網站。

立法院7月11日三讀通過「因應國際情勢強化經濟社會及民生國安韌性特別條例」，匡列新台幣5450億元，並明定每人普發現金1萬元，

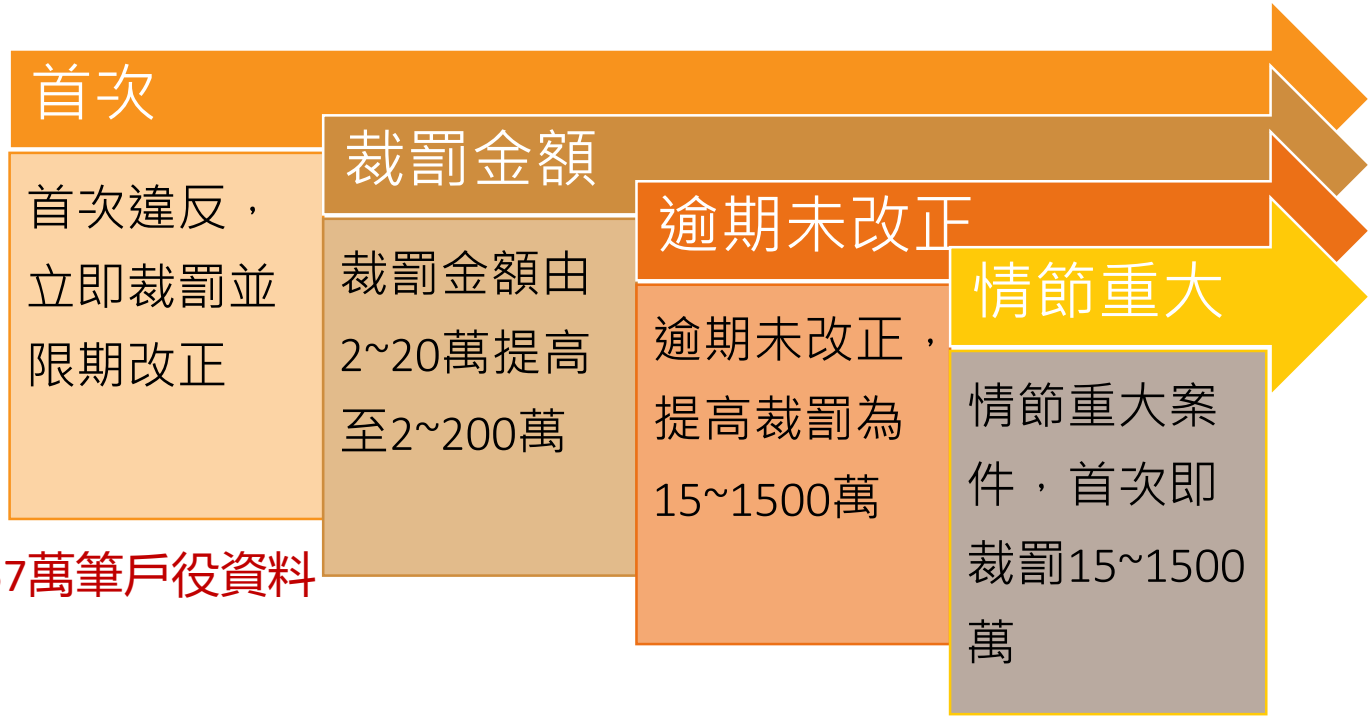


# 釣魚簡訊(Smishing)


From:自由時報




# 近年重大資安、個資外洩事件




## 公部門、關鍵設施

2021　內政部戶政資料 駭客在暗網兜售2357萬筆戶役資料

2023　華航 駭客勒贖、會員個資外洩

2023.3 故宮 行政院證實數千件國寶約十萬張圖檔遭竊賤賣

2023　雄獅旅遊 遭網路駭客攻擊案，遭核處罰鍰200萬元

2023年蝦皮跟誠品生活個資保護程序沒做好，委外廠商未落實監督管理等，已違反個資法第27條第1項規定，開罰蝦皮新台幣20萬元、誠品生活10萬元



https://topic.udn.com/event/newmedia_hacker_taiwan

# 近年重大資安、個資外洩事件

## 消費娛樂

2017.5 雄獅旅行社 36萬筆個資外洩，導致客戶被詐騙

2023.1 iRent 40萬筆個資外洩

2023.1 博客來、誠品等5家電商 遭刑事警察局點名詐騙高風險賣場

2023.2 微風 90萬筆個資外洩

https://topic.udn.com/event/newmedia_hacker_taiwan

# 應辦事項-教育部重申學校使用資通系統或服務蒐集及使用個人資料注意事項

一、依教育部113年2月21日臺教資通字第1130015530A號函辦理。

二、因近期國教署所轄學校於網站公告時，未進行個資識別化動作即進行資料公告，造成個資外洩事件。

請轉知學校人員在處理個資相關業務時，務必遵守個人資料保護法相關規定，並參酌教育部「學校使用資通系統或服務蒐集及使用個人資料注意事項」、Google表單蒐集個人資料使用原則（https://sites.google.com/email.nchu.edu.tw/gform）及建立檢查機制，請學校落實檢討網頁公告上架流程及審查機制，務必確保無個資外洩疑慮。

三、另依「資通安全事件通報及應變辦法」，知悉資通安全事件後，學校應於一小時內進行資通安全事件之通報；另資通安全事件有一般公務機密、敏感資訊（個人資料等）遭輕微洩漏或竄改，為第三級資通安全事件；檢附國教署資安事件通報流程說明圖、「國立高級中等以下學校資安情傳遞及應變處理作業流程」。

# 近年重大資安、個資外洩事件

## 金融

2016.7　第一銀行 東歐駭客入侵盜領8327萬元

2017.2　13家證券公司 首起集體遭駭客勒索

2017.10　遠東銀行 被盜轉6010萬美元

2021.11　7家證券、期貨商 駭客撞庫攻擊、客戶被異常下單

https://topic.udn.com/event/newmedia_hacker_taiwan

# 近年重大資安、個資外洩事件

## 科技

2018.8 台積電 生產線停擺、營收損失達52億

2019.3 廣達 東歐駭客冒名詐取貸款

2019.3 華碩 軟體更新檔被入侵影響上萬台電腦

2020.11 鴻海、仁寶、研華 駭客資料勒贖

2021 宏碁、日月光、廣達、技嘉、東元 勒索軟體攻擊

2022 竹科7家半導體廠商 陸駭客展開持續性滲透威脅（APT）行動

https://topic.udn.com/event/newmedia_hacker_taiwan

# 個資外洩的原因-案例分享

## 某國立大學個資千筆個資外洩

**EMAIL寄發機敏個資：**

向校內220位學生寄出講座通知信，當中竟夾帶104至108學年度全數新生共計8495筆個人資料。校方則召開校務會議，說明事件始末，並提出加強教育訓練、成立個資保護及處理小組等補救方案

**影響範圍：**

學生姓名、身分證字號、電子郵件、行動電話等項目

**應變措施：**

個資事故通報、承辦老師發送EMAIL請學生將信件刪除、課堂中再次請學生將信件刪除、加強教育訓練、增加人員資安意識、落實個資保護措施。

# 駭客入侵7高中校務系統 教育部清查26校學習歷程

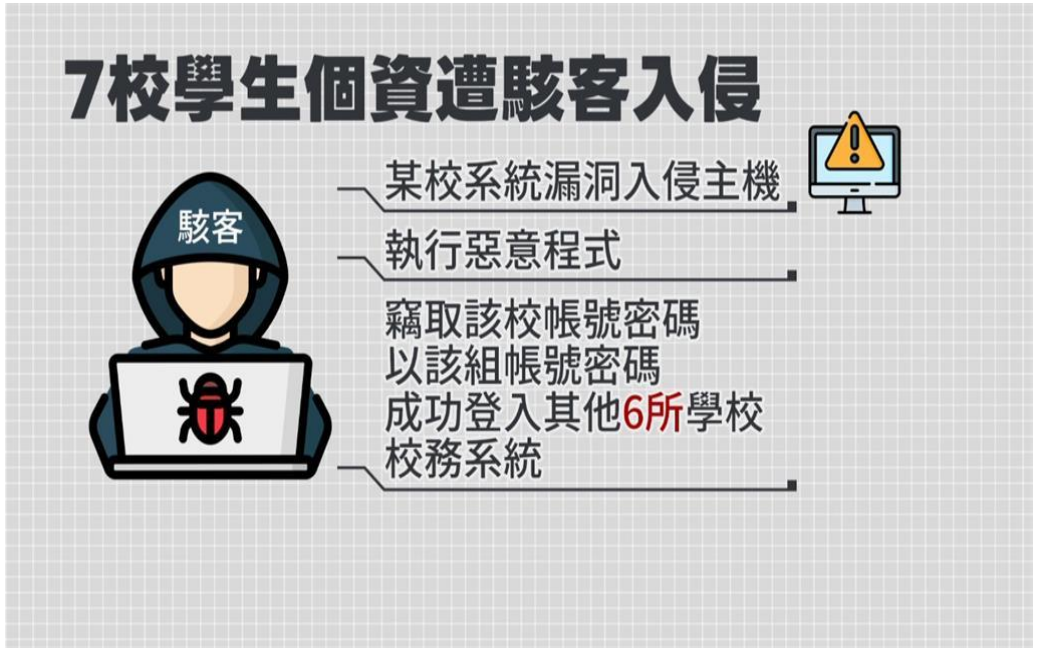
被駭客盯上！7高中校務系統遭駭、個資外洩 教育部公布學校名單

2024-03-30 17:29 聯合報／記者許維寧／台北即時報導

+ 資安

**手法探討:**

駭客是透過1所學校的系統漏洞入侵主機，成功執行惡意程式，進而竊取學校的帳號密碼，並以該組帳號密碼，成功登入其他6所使用亞x公司的高中校務行政系統（共7所被入侵）。

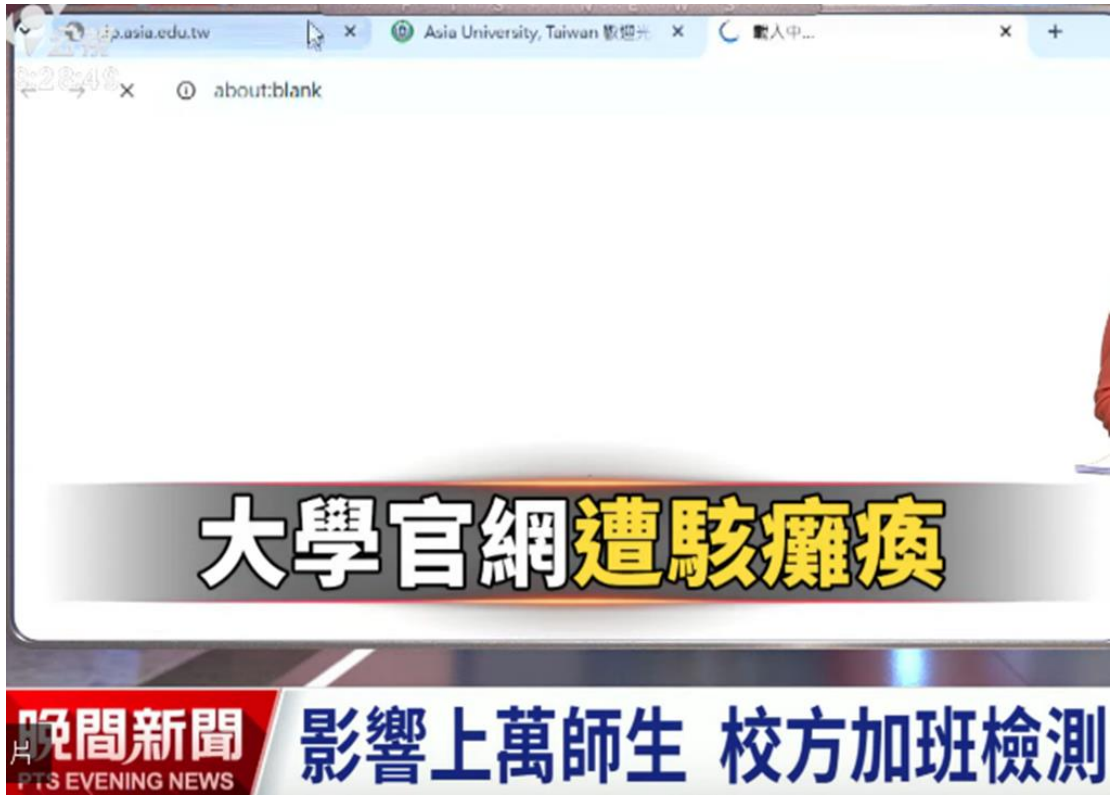



**影響範圍:**

被入侵的7校，還有19校使用亞x公司單機版校務行政系統（共26校）。

# 新聞案例-某大學網站於春節死當

- **除夕起：學生無法進入學校官網，學貸申請、繳費單列印等作業全面受阻**
  - 校內繳費機同步癱瘓，張貼「故障」公告
  - 官網身分驗證主機異常，懷疑遭外部攻擊
- **受影響範圍：**
  - 學貸申請、對保
  - 線上繳費
  - 轉學申請
  - 選課、查詢成績




**學生反應：必須改為親自到校辦理，抱怨「很不方便」、「延誤時間」**

https://www.cyberresilience.com/threatintel/apt-group-kimsuky-targets-university-researchers/

# 醫療機構受駭個資外洩事件增加

醫療機構受駭事件增加，「特種資料」洩露如馬偕、彰基等醫院遭 CrazyHunter 等組織入侵，病歷、個資甚至在暗網兜售。

2025 年重大事件：
馬偕醫院（2025 年 2 月）：遭 CrazyHunter 勒索軟體攻擊，600 台以上電腦系統癱瘓，部分病歷與文件被加密封鎖。院方未支付贖金，但費時耗資修復並購置端點防護軟體。

彰化基督教醫院（2025 年 3 月）：同樣遭 CrazyHunter 入侵，雖未發生資料外洩，但多系統短暫癱瘓。

長慎醫院（桃園中壢，2025 年 4 ~ 5 月）：系統疑似遭 NightSpire 駭侵，網路掛號、處方等服務受阻，據稱竊得 800 GB 醫療系統資料。

https://www.twreporter.org/a/hospitals-sensitive-data-breach

# 醫療機構受駭個資外洩事件增加

來自中國的駭客CrazyHunter從今年（2025）2月起，陸續針對台灣醫學中心發動「系統性攻擊」。攻擊首先鎖定馬偕醫院，導致核心醫令系統與掛號系統停擺，隨後擴大至彰化基督教醫院及其他企業等。駭客不僅加密檔案勒索，更竊取了大量病患病歷、醫護人員個資及手術紀錄，並將之公布於網路上，導致台灣首宗「特種資料」外洩風暴的產生。

正當大眾還沉浸在新年節慶的餘韻時，名為CrazyHunter的駭客悄悄摸進了馬偕醫院的系統裡，他小心地偵查、刺探龐大的醫院內部網路，並在一天後鎖定漏洞，鑽進擁有眾多權限管理權的AD主機內。隨著這樣的關鍵資安核心遭到攻陷，駭客還將自己使用的軟體偽裝成印表機驅動程式來躲避防毒軟體偵測，成功滲透進馬偕醫院台北院區和淡水院區的600多台電腦內，並開始大量散布如crazyhunter.exe的惡意程式，將接觸到的大量檔案統統加密上鎖。

https://www.twreporter.org/a/hospitals-sensitive-data-breach

# 新聞案例-醫院千萬筆個資外流傳詐團買下

- 醫院日前遭遇駭客入侵，現在更被發現駭客在暗網公開販售，聲稱握有馬偕醫院1660萬筆病患個資，包含姓名、手機號碼、病歷紀錄等資料，開價大約328萬元台幣

受影響範圍：

- 病歷資料
- 個人資料

# 個資外洩的原因-案例分享

## 把ChatGPT 當心理師？OpenAI執行長示警：對話記錄恐變法律證據

OpenAI執行長奧特曼（Sam Altman）近日坦言

用戶與ChatGPT掏心掏肺的對話記錄不受法律上的隱私保障，法院有權調閱並當成訴訟證據。

https://stock.ltn.com.tw/article/md7db9wjrrum

Open AI 執行長奧特曼（Sam Altman）

# 驚！ ChatGPT 11萬筆私密對話外流Google全看光 官方急滅火

在使用Google搜尋時，意外發現超過500筆ChatGPT使用者與AI的對話內容，若使用網路存檔工具「時光機」更能找到超過11萬筆過去的對話，引發外界對AI資安與隱私保護的高度關注。


這些聊天內容涉及內線交易計畫、詐騙自白、針對哈瑪斯網路攻擊的構想，甚至包含醫病與法律諮詢等私密資訊

事件曝光後，ChatGPT開發公司OpenAI已於114年7月31日關閉「分享至搜尋引擎」功能。

https://tw.news.yahoo.com/%E9%A9%9A-chatgpt-11%E8%90%AC%E7%AD%86%E7%A7%81%E5%AF%86%E5%B0%8D%E8%A9%B1%E5%A4%96%E6%B5%81google%E5%85%A8%E7%9C%8B%E5%85%89-%E5%AE%98%E6%96%B9%E6%80%A5%E6%BB%85%E7%81%AB-071000436.html

# ChatGPT設定防止被收集資料，避免個資外洩

為了提升ChatGPT透明度與保護個人資料，OpenAI 也在 2023 年 11 月 14 日更新了隱私政策，明確揭示收集哪些資訊，又如何運用

**方法 1. 啟用臨時聊天模式：**詢問比較私密問題，像是算命、星座命盤解析等，過程會需要輸入個資

**方法 2. 關閉個人化參考儲存的記憶：**避免AI會持續收集用戶性格和資料來回答問題

**方法 3. 刪除個人化聊天記憶：**點擊「管理記憶」，從裡面點擊「全部刪除」就能一次清空

**方法 4. 停用聊天記錄改善AI模型：**要是不想ChatGPT聊天記錄被用來訓練AI模型，也可以自己關閉拒絕提供

**方法 5. 謹慎輸入避免上傳敏感資訊：**要是不打算關閉 ChatGPT 記憶功能，那就聊天時請勿輸入機敏個資

https://mrmad.com.tw/how-avoid-chatgpt-personal-information-privacy

# 如何安全使用ChatGPT？保護你的隱私與對話內容

**1.避免輸入個人隱私或敏感資訊**：包括身份證號碼、家庭狀況、健康資料、財務資訊等，這些都不應輸入於AI對話中。

**2.不要將AI當作情感諮詢對象**：ChatGPT無法提供心理治療，也無法理解複雜的人際情感。遇到情緒問題，應尋求真人協助。

**3.審慎對待每一次輸入**：所有輸入內容都有可能被記錄或被調用，請先思考「如果這段對話被公開，我是否能接受？」。即使關閉聊天紀錄功能，也不代表資料完全隔離不被存取。

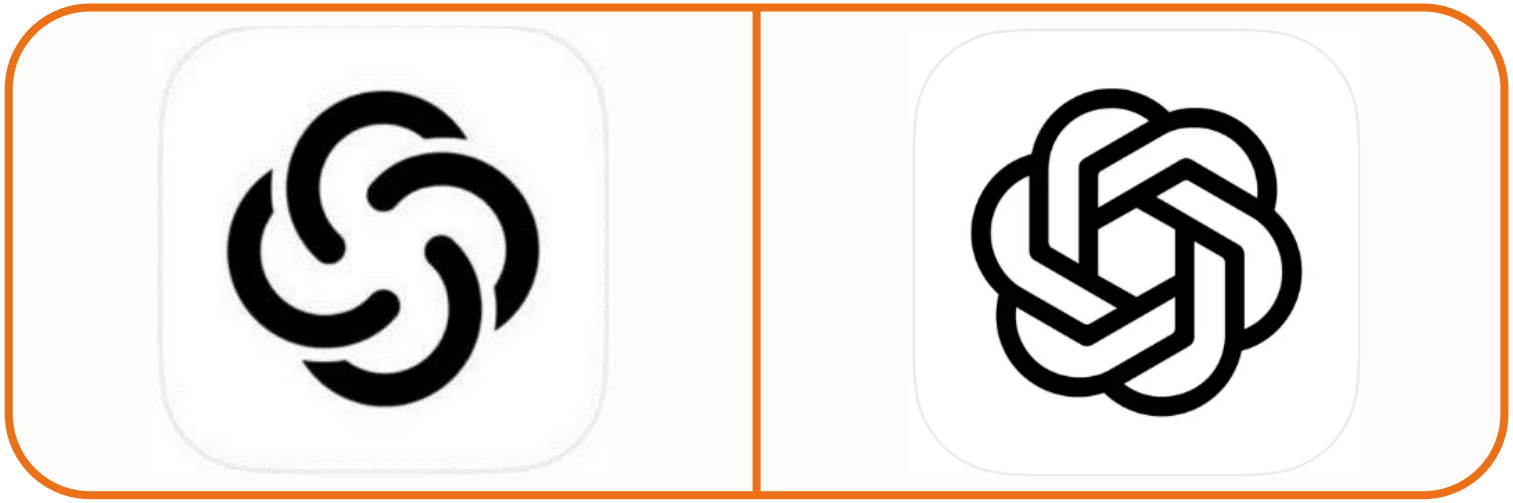
**4.高風險問題交給專業**：AI不適合解決法律、醫療或財務問題，這些應交由具備資格的人員處理。

**5.定期檢視使用習慣**：若你越來越常對AI傾訴心事，甚至仰賴AI做出決定，這可能是該停下來、重新思考的警訊。

**6.小心被AI的語氣誤導**：ChatGPT有時會「自信地錯誤」，用非常肯定的語氣說出其實不正確的資訊。使用者應保持質疑態度，重要內容應進一步查證，不應完全照單全收。

https://dailyview.tw/popular/detail/29817

# 偽冒程式案例：假冒知名App



**ChatGTP：中文AI智慧聊天** 4+

AI智慧聊天與答覆

ChatAI Tech

專為 iPhone 設計

在「工具程式」類中排名第 84

免費・提供 App 內購買

**ChatGPT** 12+

OpenAI 的官方應用程式

OpenAI

在「生產力工具」類中排名第 1

★★★★★ 4.9 • 33.5万 則評分

免費・提供 App 內購買

## 混淆名稱與標誌

「ChatGTP」僅將字母「P」與「T」互換位置，使名稱與正版極為相似。同時，圖示設計也模仿官方應用，使消費者難以辨別真偽。

## 不明開發者背景

ChatGTP 應用由開發者「ChatAI Tech」推出，但其背景資料模糊，且無其他應用程式開發紀錄，缺乏可靠性。

## 誘導付費模式

ChatGTP 提供極少量免費試用問題後，即要求用戶支付費用或訂閱服務，最高收費達新台幣3340元，遠高於OpenAI官方ChatGPT Plus每月660元的收費。

# 你的穿戴裝置安全嗎?智慧連網真的沒問題?

ESP32是一款整合了傳統藍牙、BLE和Wi-Fi網路的平價MCU晶片。
可廣泛製作於各種物聯網應用，是打造居家自動化系統不可或缺的核心模組。

智慧燈控系統：搭配繼電器模組，用手機 App 遠端開關燈。
門窗狀態感知：使用磁簧開關與即時通知，保障居家安全。
語音控制助手：連接麥克風模組與雲端語音 API，打造自己的語音助理。
空氣品質監測：整合溫溼度與 PM2.5 感測器，自動開啟排風系統。

穿戴式裝置
**電子手錶**

# 中國製品，搭載後門指令? ESP32

中國製作的單晶片微控制器 ESP32 被發現藏有後門指令，該晶片因其超低價格（約2歐元）被全球許多大眾市場的物聯網設備所使用。

ESP32 是總部位於上海的中國公司樂鑫所開發，根據 2023 年樂鑫公司自己的聲明報告，迄今這個晶片已經販售超過十億個，也就是目前有超過十億個設備可能已經使用這樣的晶片。

塔羅吉安全研究人員用該公司開發的安全稽核工具USB藍牙驅動程式（BluetoothUSB），對不同類型的藍牙設備進行安全測試時，
意外發現ESP32具有29個樂鑫科技未公布的隱藏指令，
這些指令屬於主機控制器介面命令（HCI）。

▲隱藏指令允許黑客執行記憶體操作（讀/寫RAM與閃存）、MAC地址欺騙（設備冒充）、LMP/LLCP數據包注入等攻擊，甚至植入惡意程式，進而控制手機、電腦、智能鎖或醫療設備。

此一漏洞由西班牙資安公司 Tarlogic Security 的研究人員所發現，並於 114/3/6 在馬德里舉行的 RootedCON 安全會議上公諸於世。

Tarlogic detects a backdoor in the mass-market ESP32 chip that could infect millions of IoT devices

06 - Mar - 2025 - Tarlogic Security


https://kuma-academy.org/article/100

# 角色與責任：自我習慣養成


- **離開座位時鎖定電腦（Windows+L）**

  養成習慣，無論離開多久，都要鎖定電腦，防止他人未經授權存取系統或查看敏感資料。


- **定期更換強密碼**

  每6個月更換一次密碼，使用至少12位元的複雜密碼（含大小寫字母、數字、符號），避免使用生日等個人資訊。

- **謹慎使用電子郵件**

  避免在電子郵件中傳送未加密的個資，必要時使用加密附件並另外傳送密碼。

# 角色與責任：自我習慣養成

## 加密敏感檔案與隨身碟

使用加密軟體保護含有學生個資的檔案，特別是需要攜出校園的資料，確保即使設備遺失也不會外洩資料。

## 妥善處理紙本文件

含個資的紙本文件使用後立即歸檔上鎖，不再需要時使用碎紙機銷毀，切勿直接丟入垃圾桶。

## 定期參與個資保護培訓

主動參與學校或教育部舉辦的個資保護相關培訓，持續更新個資保護知識與技能。

# 角色與責任：我們每一位都是資料保護的守門人

## 教師的責任

**課業資料保護：** 妥善保管學生成績、作業及評量資料，避免未經授權的存取

**學生隱私維護：** 尊重並保護學生的個人隱私，不隨意公開或分享學生個資

## 行政人員的責任

**文件處理：** 確保個資文件的安全處理、儲存與銷毀

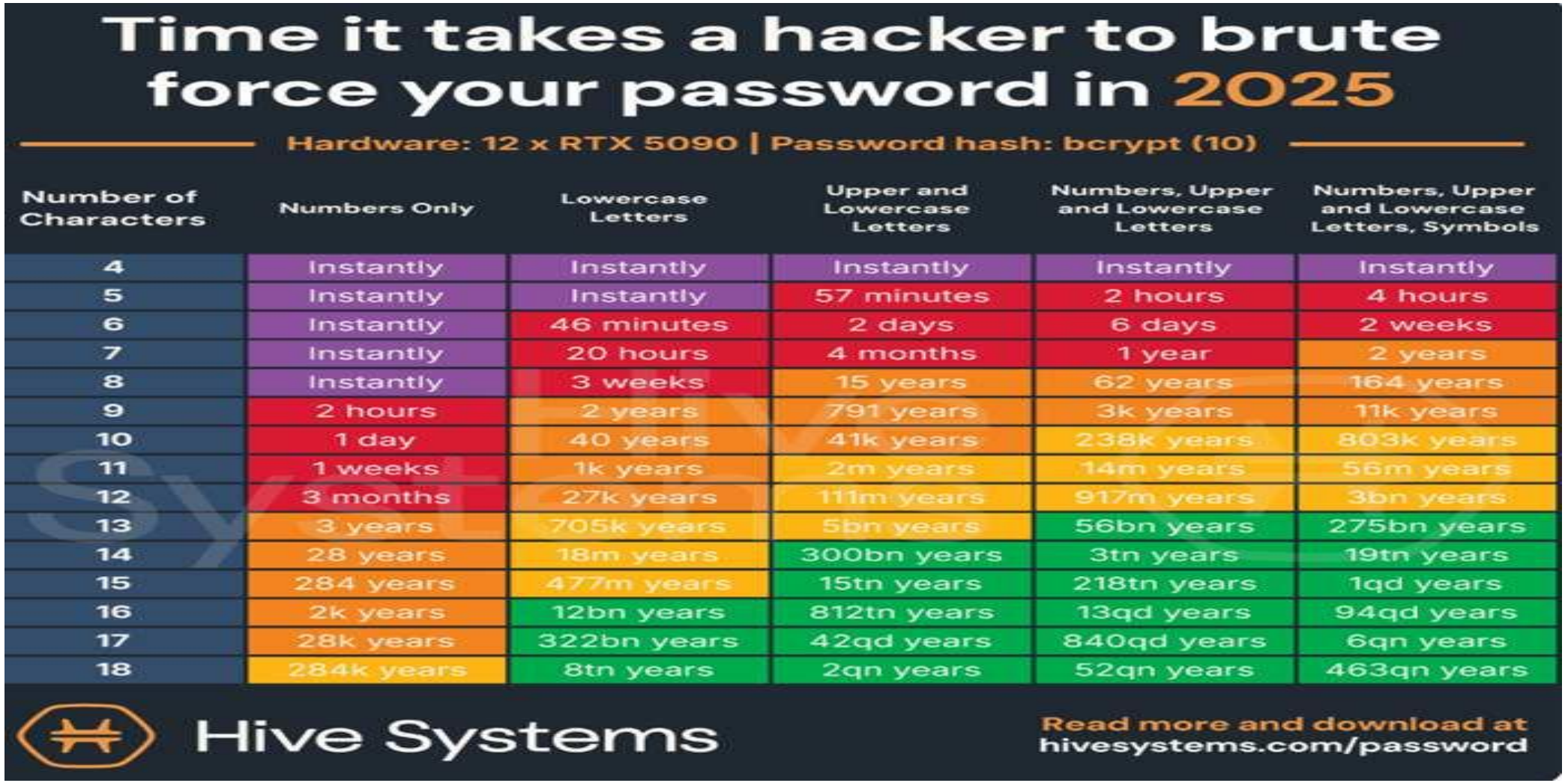
**保密義務：** 嚴守工作中接觸到的教職員生個資，遵守保密規範

## 學生的責任

**網路行為：** 在網路上保護自己與他人的個人資料，避免過度分享

**自我保護：** 提升個資保護意識，了解個資外洩的風險與防範方法

# 密碼破解時間


Time it takes a hacker to brute force your password in 2025
Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)
Number of Characters
Numbers Only
Lowercase Letters
Upper and Lowercase Letters
Numbers, Upper and Lowercase Letters
Numbers, Upper and Lowercase Letters, Symbols
4 Instantly Instantly Instantly Instantly Instantly
5 Instantly Instantly 57 minutes 2 hours 4 hours
6 Instantly 46 minutes 2 days 6 days 2 weeks
7 Instantly 20 hours 4 months 1 year 2 years
8 Instantly 3 weeks 15 years 62 years 164 years
9 2 hours 2 years 791 years 3k years 11k years
10 1 day 40 years 41k years 238k years 803k years
11 1 weeks 1k years 2m years 14m years 56m years
12 3 months 27k years 111m years 917m years 3bn years
13 3 years 705k years 5bn years 56bn years 275bn years
14 28 years 18m years 300bn years 3tn years 19tn years
15 284 years 477m years 15tn years 218tn years 1qd years
16 2k years 12bn years 812tn years 13qd years 94qd years
17 28k years 322bn years 42qd years 840qd years 6qn years
18 284k years 8tn years 2qn years 52qn years 463qn years
Hive Systems
Read more and download at hivesystems.com/password

# 密碼強度差異影響巨大，簡單密碼的安全性極為脆弱

8 位純數字密碼：單張 RTX 5090：3 小時

8 位全小寫字母密碼：單張 RTX 5090：8 個月

8 位混合大小寫 + 數字密碼：12 張 RTX 5090：需時約 62 年

| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols | Hardware |
|---|---|---|---|---|---|---|
| 8 | 4 hours | 10 months | 219 years | 896 years | 2k years | RTX 4090 |
| 8 | 3 hours | 8 months | 172 years | 703 years | 1k years | RTX 5090x1 |
| 8 | 22 mins | 1 month | 23 years | 93 years | 246 years | RTX 5090x8 |
| 8 | 15 mins | 3 weeks | 15 years | 62 years | 164 years | RTX 5090x12 |
| 8 | 51 mins | 2 months | 52 years | 212 years | 559 years | A100 x8 |
| 8 | 34 mins | 2 months | 35 years | 141 years | 373 years | A100 x12 |
| 8 | Instantly | 1 hour | 2 weeks | 2 months | 5 months | A100 x10,000 (ChatGPT 3) |
| 8 | Instantly | 43 mins | 1 weeks | 1 month | 3 months | A100 x20,000 (ChatGPT 4) |

https://www.techbang.com/posts/123120-rtx-5090-password-cracking-speed

# 十要!

1. 要使用高強度密碼
2. 要定期修改密碼
3. 電腦系統要更新
4. 電腦防毒要更新
5. 社交工程要小心
6. 要使用合法軟體
7. 電子郵件要過濾
8. 重要資料要備份
9. 機敏資料要保護
10. 電腦不用要登出

# 十不要!

- 網站不要亂上
- 連結不要亂點
- 信件不要亂開
- 簡訊不要亂點
- 密碼不要簡單
- 密碼不要相同
- 密碼不要寫在紙上
- 不要亂裝軟體
- 不要亂插隨身碟
- 不要隨便連WIFI

# 問題與討論

# 問題與討論

# 簡報結束

## 謝謝您

宜蘭區網中心