個資及資安日常防護需知

宜蘭區網中心
ILAN REGIONAL CENTER

宜蘭區域網路中心
講師：吳文達

2 個資保護暨資訊安全淺談

資安事件可能造成的影響

- **個人**：身分遭盜用、遭到勒索、重要資料遺失、金錢上損失等問題。
- **系統**：系統無法正常運作、資料庫毀損、服務無法正常運行等等。
- **學校**：校方、學生或教職員機敏資料外洩、校譽受損等。
- **公司**：業務停擺、或商業機密被竊(萬一這家公司關鍵的基礎設施、或是護國神山、或者是AI供應鏈、國家隱形冠軍隊)
- **國家**：國家機密、例如外交計畫、軍事設施、兵力佈署圖、戶政資料等

資安即國安

資訊安全與個資防護息息相關

個人資料保護法

資通安全管理法

3 法規法令

附註：特定非公務機關，其中後者依據『資通安全管理法』第三條定義共分為三類，包括關鍵基礎設施提供者(如台電)、公營事業(如台糖)，以及政府捐助的財團法人(如工研院)。

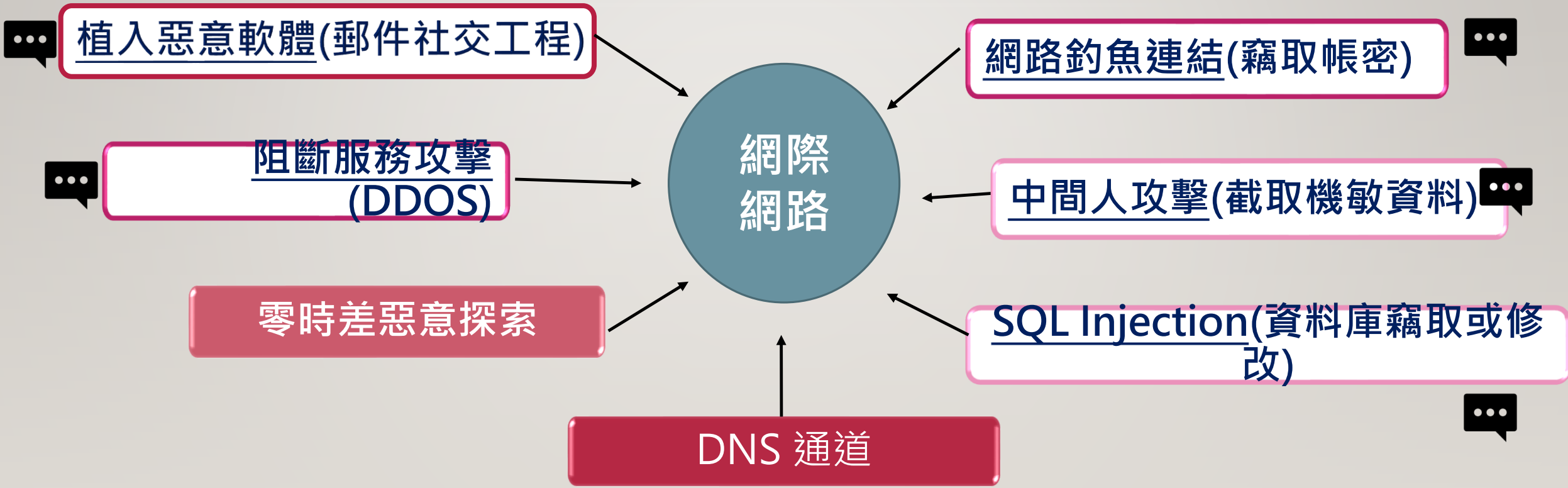
▲資安法修正草案納管機關若遭遇重大資安事故須配合調查，若不配合最高可罰百萬

行政院院會於2024 / 7/ 4 號通過「資通安全管理法修正草案」，根據草案，資安署得稽核所有納管的**公務機關或特定非公務機關，當發生重大資安事件時，若規避、妨礙或拒絕調查，可開罰10萬以上、100萬元以下罰鍰。**

▲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。**

4 最常見的網路攻擊有哪些？



資料來源：Cisco (https://reurl.cc/VjYQd5)

5 社交工程

藉由人際關係的互動來進行犯罪的行為，利用人性的弱點進行**詐騙**，(資安最脆弱的一環)屬於非全面技術性的資訊安全攻擊方式。

社交攻擊

缺乏警覺心、人有好奇心...

騙取個人資料、
騙取系統帳號密碼

6 社交工程-手法


偽裝委外廠商
帳號及密碼
網路釣魚
利用郵件誘騙開啟圖檔
植入惡意程式
暗中收集機密資料
利用工具誘騙下載(如P2P)
植入惡意程式
暗中收集機密資料
利用電話
佯裝資訊人員
騙取帳密
利用即時通訊軟體
誘騙點選連結後中毒

7 常見社交工程攻擊方式

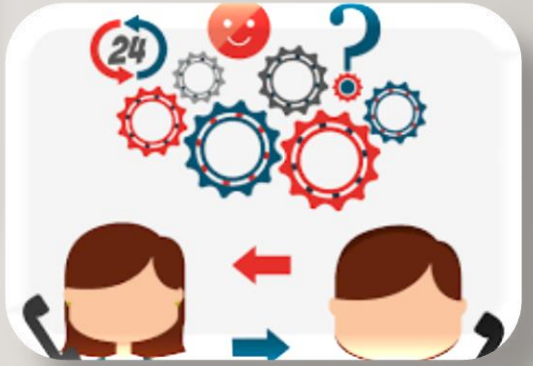
惡意電子郵件

恭喜您中獎

圖片夾帶惡意程式

社群或社交網站散布連結

領取端午節紅包



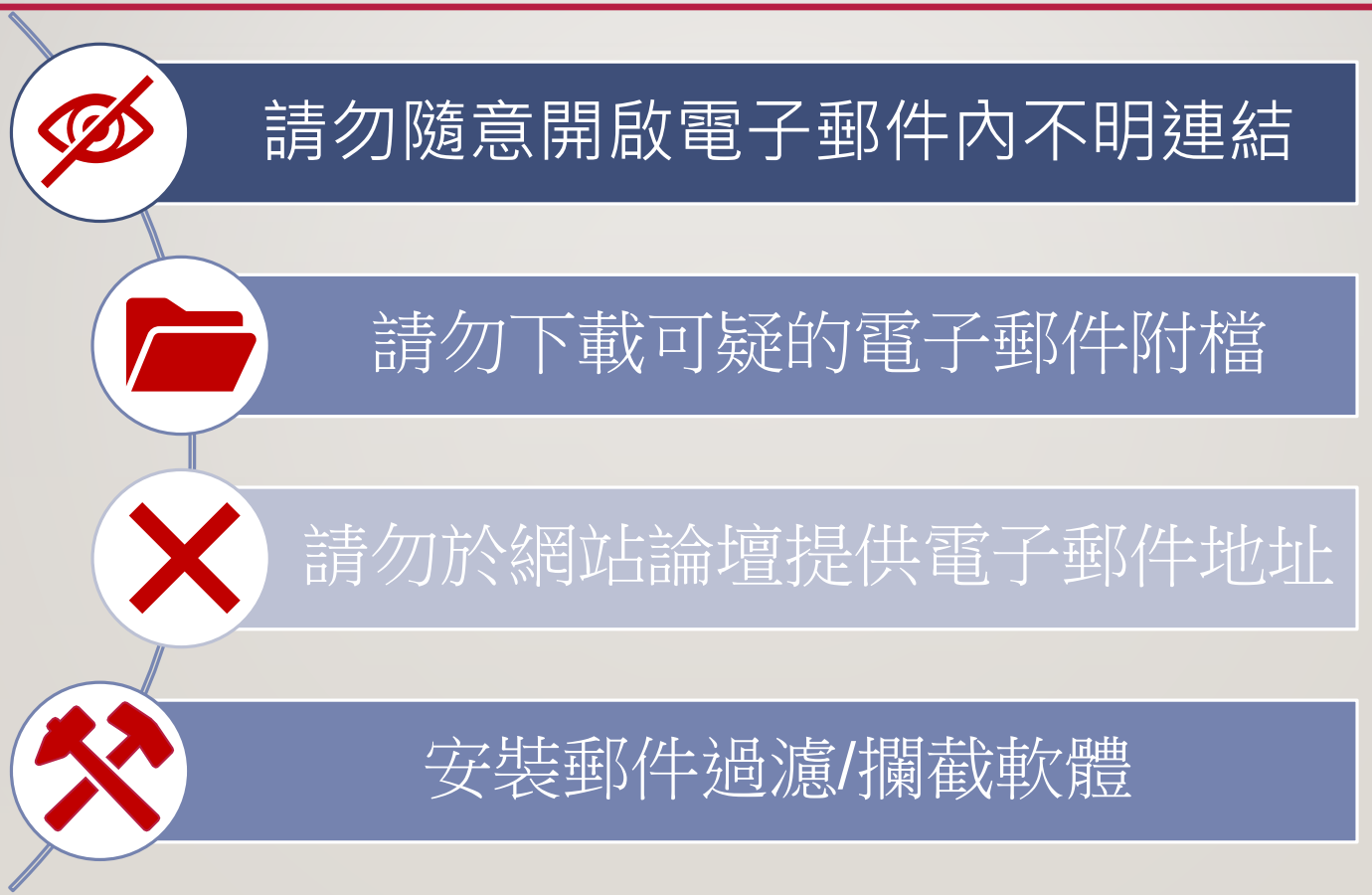
電話詐騙

假裝學生重設密碼
假裝好友急需轉帳

8 AI 社交工程攻擊(真假難辨)

- 透過AI技術生成聲音或影像，偽冒其當事人，以達到索取資料或金錢之目的。
- AI聲音(盜取您的聲音)
- AI影像(盜取您的肖像)

9 防禦惡意郵件(提高警覺-收到EMAIL停看聽)



10 不要任意開啟附加檔案(提高警覺-收到EMAIL停看聽)

根據刑事警察局科技犯罪防制中心的說明，該惡意郵件夾帶一釣魚網站連結，並要使用者下載一個ZIP壓縮檔conference-2020.docx.zip，而網站檔案其實夾藏惡意程式（ZIP檔解壓縮後為conference-2020.docx.exe），如點擊下載開啟該檔案，電腦恐遭安裝木馬程式。

https://www.ithome.com.tw/news/137789

11 您的密碼安全嗎?

- 懶人密碼
- 員工編號
- 車牌
- 生日
- 身分證

Findings

Taiwan

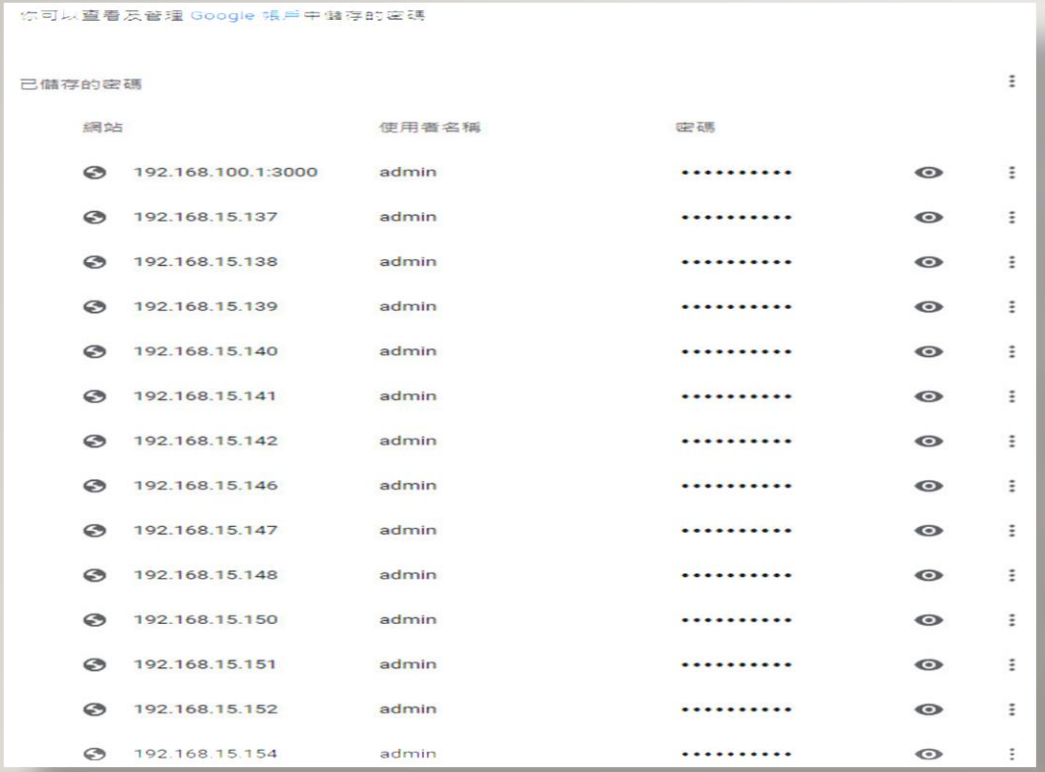
Get the 2019-2022 password list

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	admin	< 1 Second	8,430
2	123456	< 1 Second	8,035
3	a123456	< 1 Second	6,843
4	12345678	< 1 Second	3,730
5	1qaz2wsx	< 1 Second	3,542
6	123456a	< 1 Second	3,378
7	janejane123	2 Minutes	2,768
8	password	< 1 Second	2,092
9	a123456789	< 1 Second	2,057
10	abc123	< 1 Second	1,857

資料來源：https://nordpass.com/most-common-passwords-list/

密碼不秘密?

12 習慣自動登入記憶密碼?



一、不要讓任何人有機會偷用你電腦

二、開啟兩步驟認證(確認是本人)

三、使用密碼管理軟體(幫您產生複雜的密碼)

四、當個原始人

五、清除瀏覽器記憶的密碼

資料來源：
https://www.storm.mg/lifestyle/434683?page=2

13 什麼是魚叉式網路釣魚 (SPEAR PHISHING)？

魚叉式網路釣魚是專門針對特定對象的網路釣魚（Phishing），其對象通常是某個機構，其最終目標是取得機密資訊。(高針對性，例如公司高層、財務部門等)

其技巧則包括：
假冒他人名義、使用迷人的誘餌、
避開安全機制 (如電子郵件過濾及防毒) 等等
誘騙目標對象開啟郵件中的附件檔案或
點選郵件中的連結

資料來源：https://blog.trendmicro.com.tw/?p=15888

14 案例分享 -網路釣魚

疫情過後 肺炎 這個關鍵字 就深植在
大家心中...

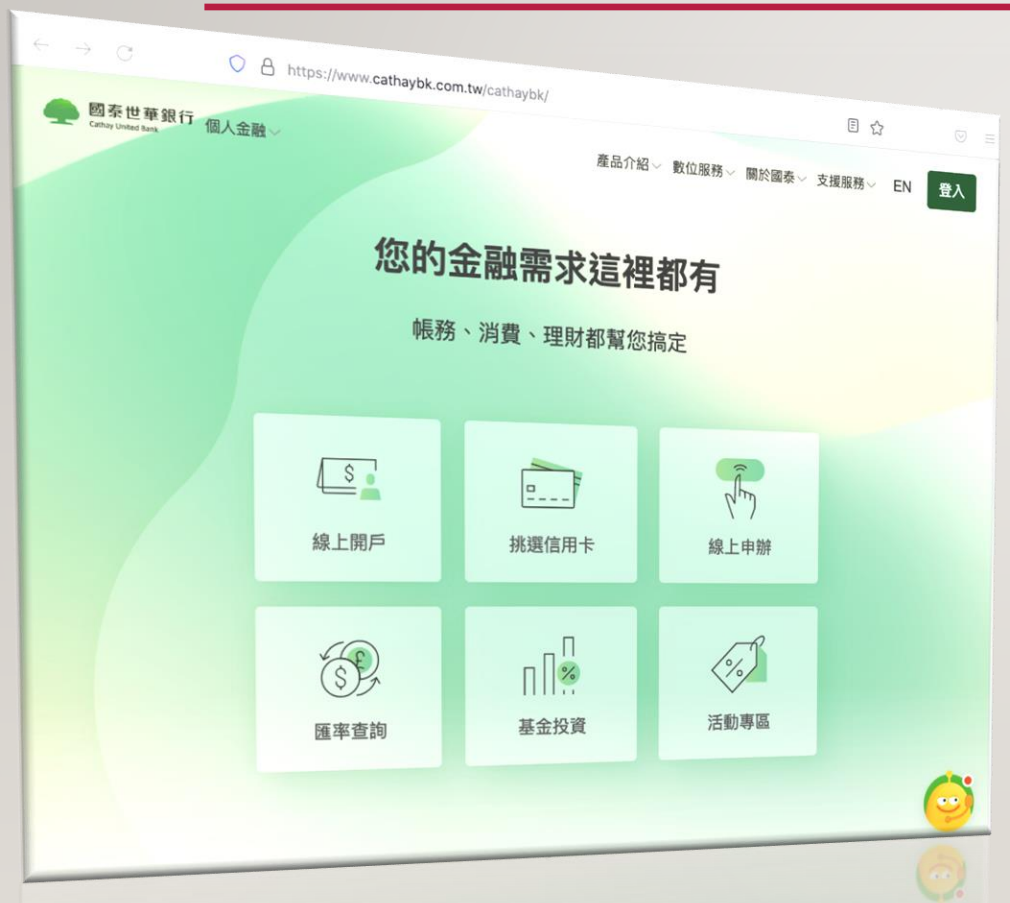
黑客就是藉由時事或生活周遭事物
來引誘你上當!!!

該案例信件標題為「世界衛生組織 **COVID-19** 疫情報告」（**WHO COVID-19 SITUATION REPORT**），用以取信被害人
在這封魚叉釣魚郵件中夾帶的惡意 Excel 檔，名稱為「covid_usa_nyt_8702.xls」，屬於Excel 4.0 格式；打開後會看到一個安全提問訊息；如果用戶同意的話，就會自網路上下載一個巨集程式，同時執行內含的 RAT 遠端遙控工具

資料來源：https://www.twcert.org.tw/tw/cp-104-3634-245b1-1.html

15 案例分享

國泰世華銀行
https://www.cathaybk.com.tw/cathaybk/



hxxp://www.cathay-bk.com

hxxp://www.cathaydc.com

hxxp://www.cathaydf.com

16 案例分享-QR碼也會掉入黑洞

掃實聯制QR碼竟跳出「冰冰姐泡湯」氣炸怒轟店員

資料來源：https://reurl.cc/8W6m74QR code 條碼產生器：http://qr.calm9.com/tw/
存款恐遭竊！亂掃QR Code「密碼被看光」

17 何謂勒索病毒?(先植入木馬，下載惡意程式、檔案加密、利用網路共用在內部傳播)

勒索病毒是一種惡意程式，
專門將本機與網路儲存上
的重要檔案加密
之後要求支付贖金才能解開檔案。

駭客開發這類**惡意程式**的目的是為了
經由**數位勒索**來牟利。

資料來源：https://www.twcert.org.tw/tw/cp-104-5359-9c0ac-1.html

18 中勒索病毒的前兆是什麼？

發現不明的對外連線。

檔案出現奇怪的檔名，例如.crypt、.locky、.AAA、.XXX等。

出現支付贖金的說明檔案，多為.txt或.html文字檔。

電腦防毒軟體持續偵測到病毒，不斷跳出提醒視窗。

資料來源：https://www.sysage.com.tw/news/technology/211

感染勒索病毒後處理方式

- 切斷網路連線，以免勒索病毒對網路磁碟機、共用資料夾內的檔案進行加密。
- 立即強制關機，避免勒索病毒持續加密檔案。
- 聯絡專業資訊人員，詳細說明中毒情況，並耐心等候處理。

資料來源：https://www.sysage.com.tw/news/technology/211

勒索病毒的防範

1.不輕易點擊 Email 內的超連結，建議直接在瀏覽器中輸入你所要去的網站網址。

2.不開啟Email的附件，除非你知道寄件者並且確定附件內容。

3.不要瀏覽名聲不佳的網站，特別是情色影片網站或是盜版電影網站，很可能只要瀏覽這些網站就會受到電腦病毒感染。

4.不軟體任意下載，確保是在官方網站下載，安全度較高。

5.定期備份你的檔案或資料在另外一個獨立裝置（如行動硬碟），或者使用雲端硬碟來備份，萬一出事，還可以找回重要資料。

6.電腦防毒務必安裝，且不要輕易關閉。

資料來源：https://isafe.moe.edu.tw/article/1992?user_type=4&topic=9

案例分享-已加密勒索病毒檔

資料來源：https://ofeyhong.pixnet.net/blog/post/226059662

案例分享-勒索病毒

解密警長

2019年勒索病毒襲衛福部 波及18間醫院。

以擴散型態大量感染，包含病歷資料、員工名冊帳冊、醫療數位影像；如果不付贖金，資料會被全數銷毀，重建要花幾10億台幣、影響病患權益。

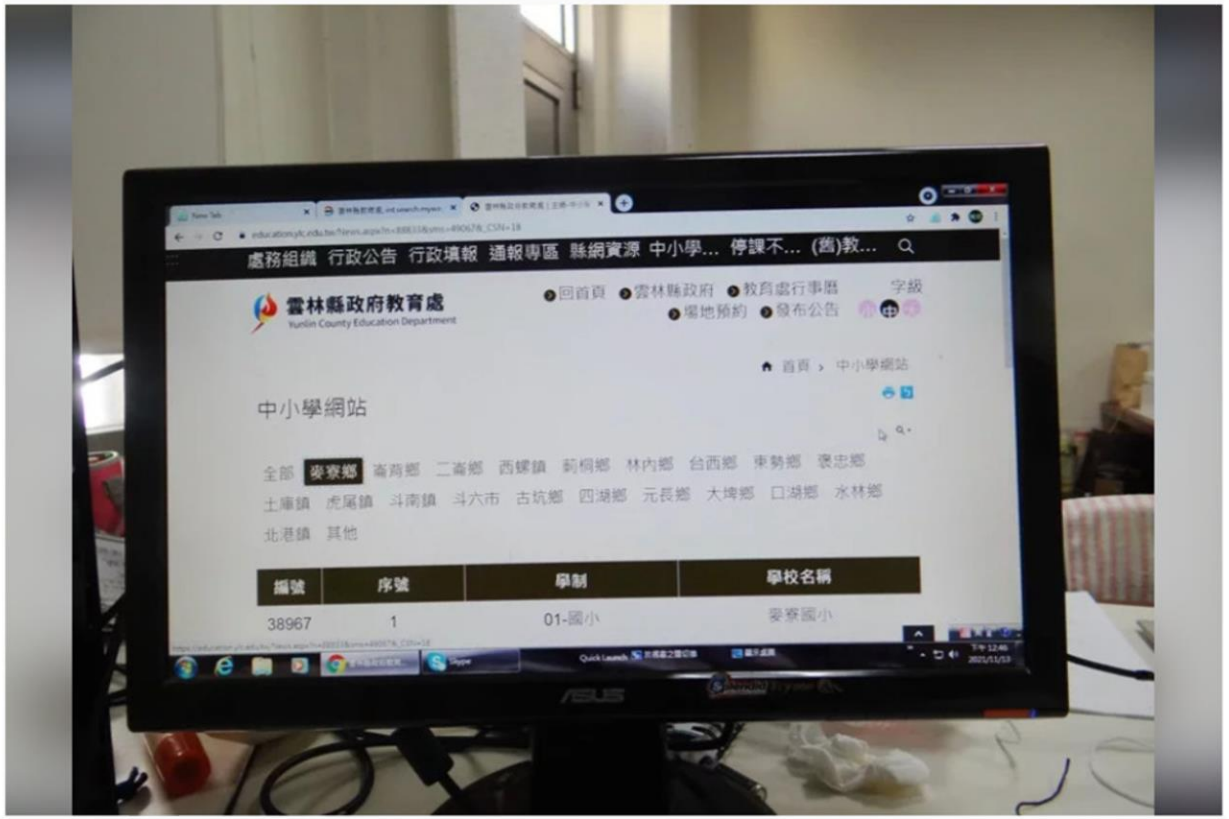
資料來源：https://reurl.cc/ReX3AG

23 案例分享

雲林教育處網路遭駭客勒索 全縣百餘所學校網路全掛點

2021-11-13 14:54 聯合報 / 記者蔡維斌／雲林即時報導

+ 駭客

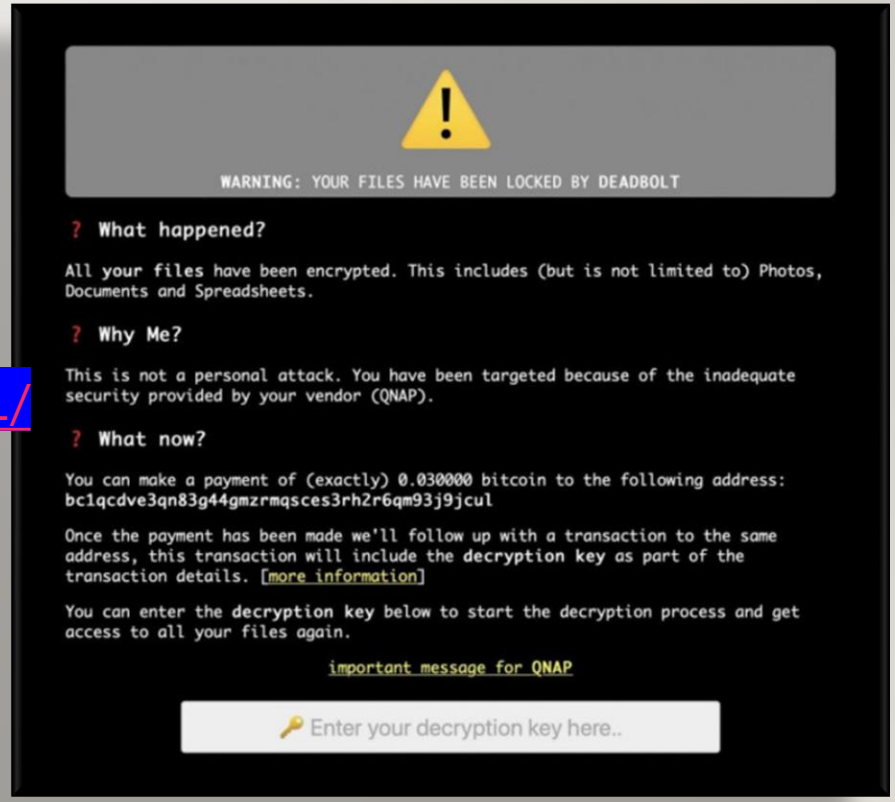


資料來源：https://udn.com/news/story/6885/5888400

24 案例分享-NAS (大量儲存空間)

NAS文件突然灰飛煙滅
威聯通緊急提醒：斷開外網抵禦勒索軟體

QNAP威聯通出來面對-
Qlocker勒索病毒自救會
https://www.facebook.com/groups/771468783554131/



資料來源：https://www.twcert.org.tw/tw/cp-104-5359-9c0ac-1.html

25 案例分享-手機病毒

TWCERT/CC

上千萬Android用戶遭151支
惡意App攻擊，擅自訂閱高價服務

資料來源：https://www.twcert.org.tw/tw/cp-104-5249-3f048-1.html

26 案例分享-手機病毒

資料來源：https://www.twcert.org.tw/tw/cp-104-5359-9c0ac-1.html

27 案例分享-手機病毒

NoReboot 病毒偽裝 iPhone 關機，
以劫持用戶的麥克風與鏡頭

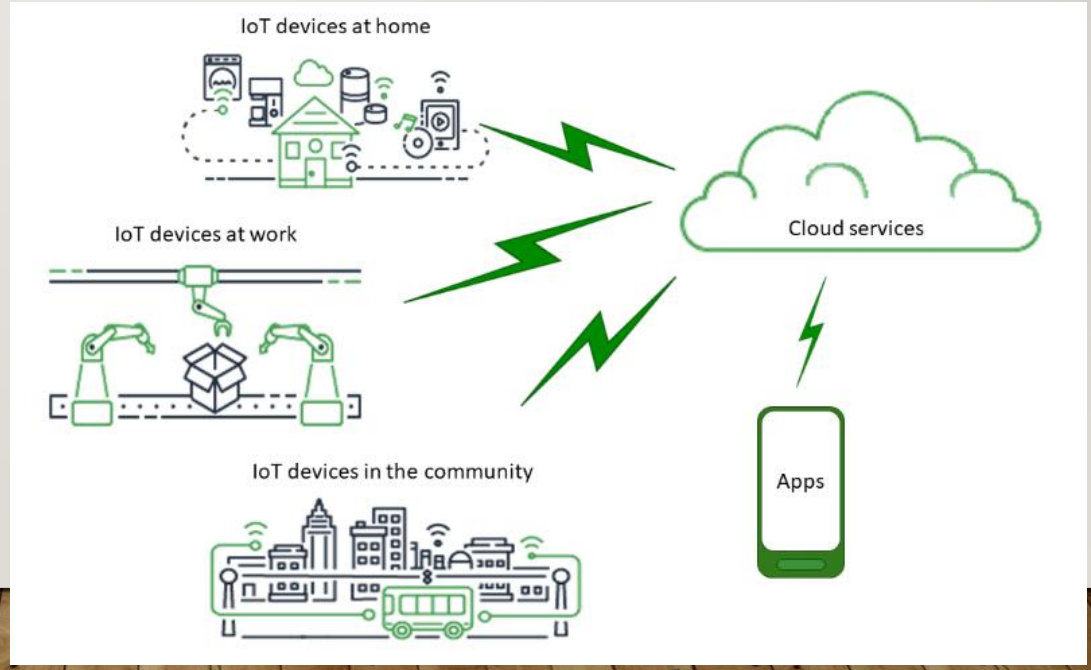
資料來源：https://www.kocpc.com.tw/archives/422099
iPhone中毒訊息是真的嗎？
手機被駭客入侵該怎麼辦？

28 案例分享

資料來源：https://www.twcert.org.tw/tw/cp-104-5359-9c0ac-1.html

物聯網 - IOT

- 物聯網 (IoT) 是指連接著各種裝置的集體網路和幫助裝置與雲端和裝置之間互相通訊的技術。現今世界上有數十億個裝置與網路連結。這代表每天各種裝置如牙刷、吸塵器、汽車和各種機器可以使用感測器收集資料並能智慧化地回應使用者的需求。



資料來源：https://aws.amazon.com/tw/what-is/iot/

30 物聯網 – IOT –常見應用

- 智慧家電 : 空氣清淨機、冷氣等
- 隨身裝置 : 平板、手機等
- 家用網路設備 : 無線分享器、NAS等

圖片來源：https://nordvpn.com/zh-tw/blog/wulianwang/

31 物聯網- 安全性威脅

預設密碼

物聯網裝置常使用預設或簡單的密碼，容易遭駭客入侵。

軟體漏洞

物聯網裝置缺乏及時更新，使其容易遭到利用。

私隱洩露

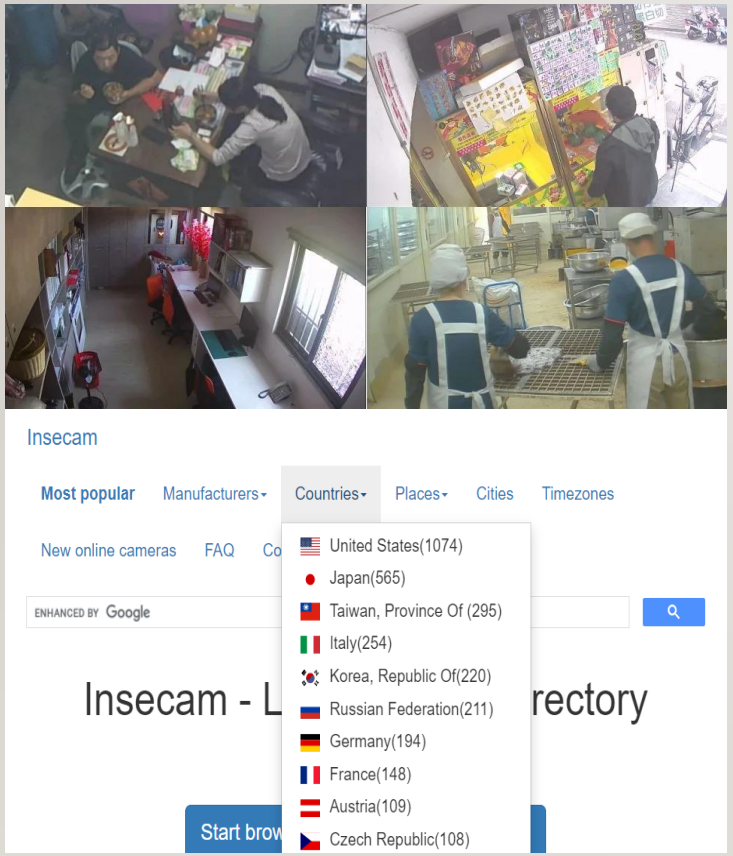
駭客可能竊取物聯網裝置的私人資訊或監控使用者。

網路攻擊

受感染的物聯網裝置可能遭利用發動分散式阻斷服務攻擊。

32 你家監視器安全嗎？

國外網站《Insecam》
（網址：http://www.insecam.org/）



該網站多年前曾被媒體揭露，但許多民眾及機構仍對監視器密碼設置不設防，目前該網站仍持續運作，包括民眾室內吃飯、睡覺畫面都直接被直播。另據業者表示，這些監視器大多是使用中國「Hi3516」海思半導體的晶片。

資安專家也說，目前刑法規定，駭客入侵系統後，公布其他人未公開活動畫面有刑事責任，若以此營利，還涉營利妨害祕密，最重可判刑5年，但這網站架在國外，執法或求償有難度，民眾只能自保或避免使用中國製晶片監視器。

科技來自於人性(資安最脆弱的一環)

最大的資安漏洞，是人的疏忽

最好的防駭工具，是人的警覺

今天來這裡→目的就是要強化大家的使用網路的警覺心

34 何謂個人資料

1.姓名　2.出生年月日　3.身分證統一編號　4.護照號碼　5.特徵　6.指紋

7.婚姻　8.家庭　9.教育　10.職業　11.病歷

特種個人資料

12.醫療　13.基因　14.性生活　15.健康檢查　16.犯罪前科

17.聯絡方式　18.財務情況　19.社會活動　20.其他可以直接或間接識別該個人的資料

資料來源：全國法規資料庫

35 個人資料無處不在

EMAIL、帳戶資料
帳單地址

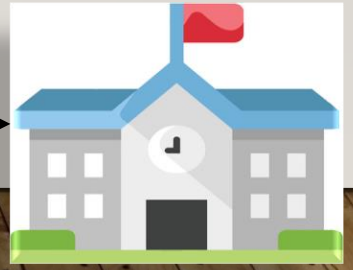
保單資料、帳戶資料、
貸款徵信資料、會員
資料

宅配地址、信用卡資
料、使用者註冊資料、
周年慶抽獎卷

身分證、結婚登記、
報稅資料、駕照申請
換發

病歷資料、健檢報告、
診斷書

學籍資料、人事資料、
註冊報名資料、畢業
校友聯絡資料



個人資料保護的重點

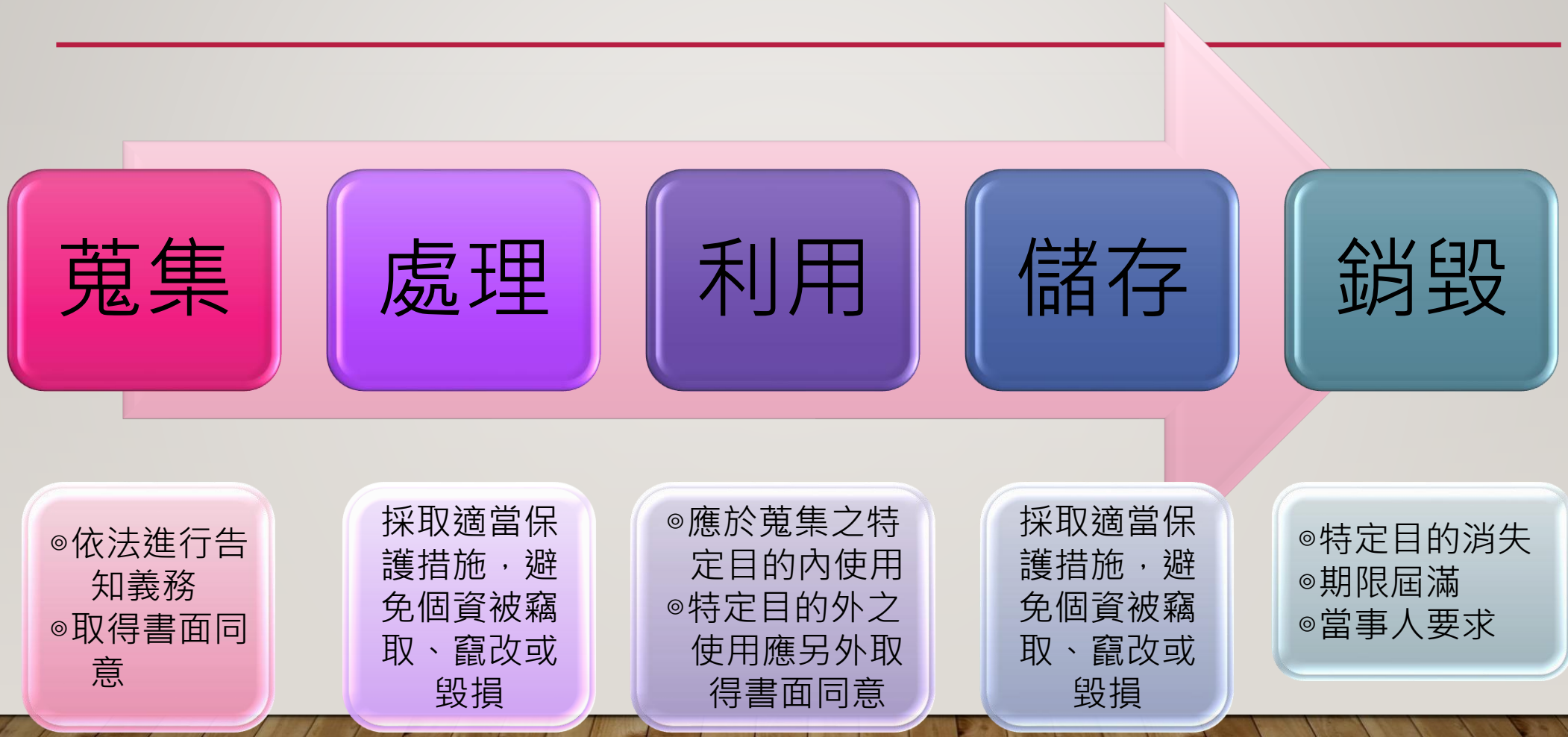
保持個人資料正確性

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

做好個人資料確實的保管、刪除與銷毀工作

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。

37 個資管理生命週期


蒐集
處理
利用
儲存
銷毀
◎依法進行告知義務
◎取得書面同意
採取適當保護措施，避免個資被竊取、竄改或毀損
◎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
採取適當保護措施，避免個資被竊取、竄改或毀損
◎特定目的消失
◎期限屆滿
◎當事人要求

如何降低個資之風險?

進行個人資料盤點

設置組織負責規劃
個資保護相關事宜

進行資訊安全與個
資教育訓練

確實且明瞭自己的個資運用

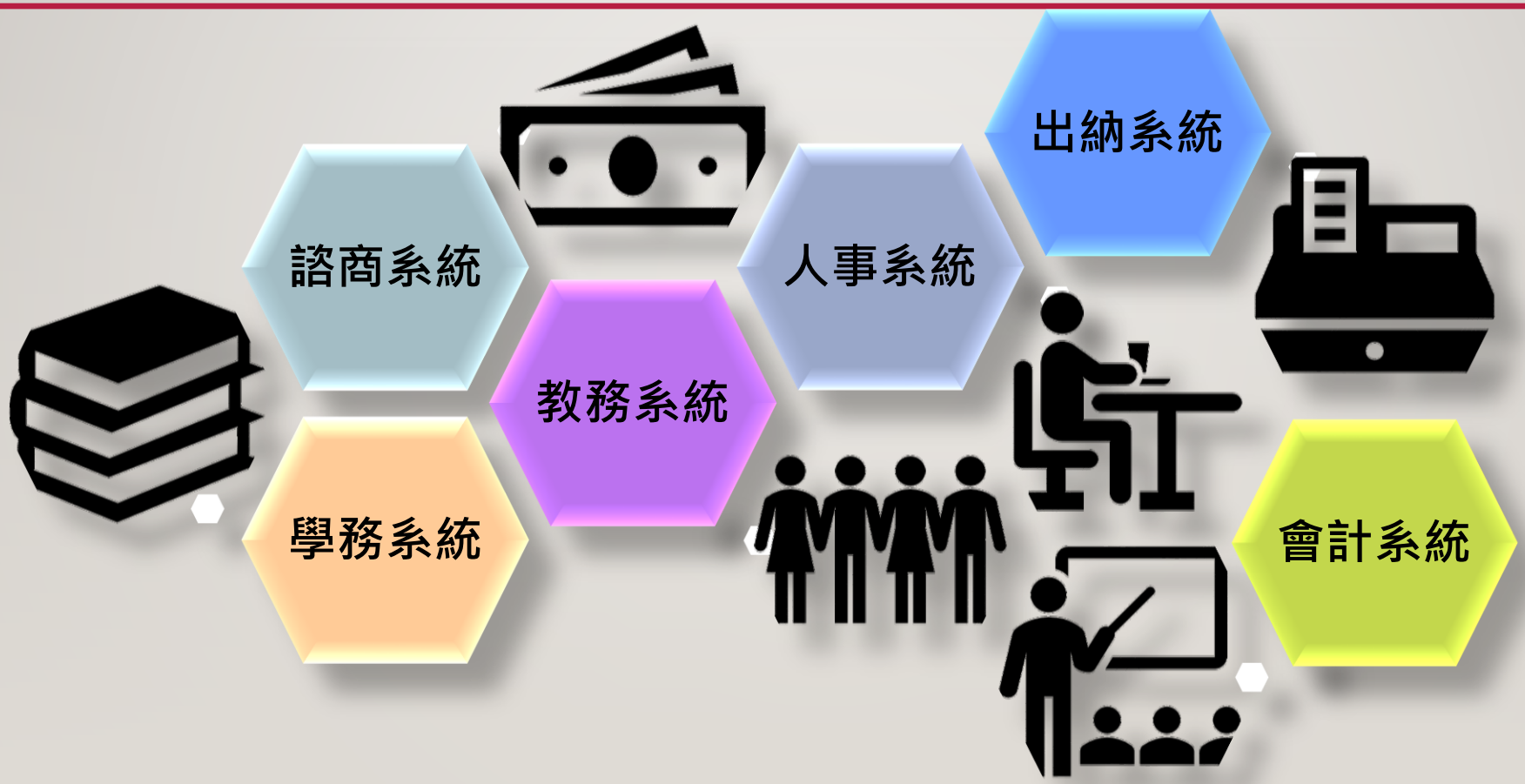
執行現有的規範增加防護效果

建立正確良好的觀念與認知

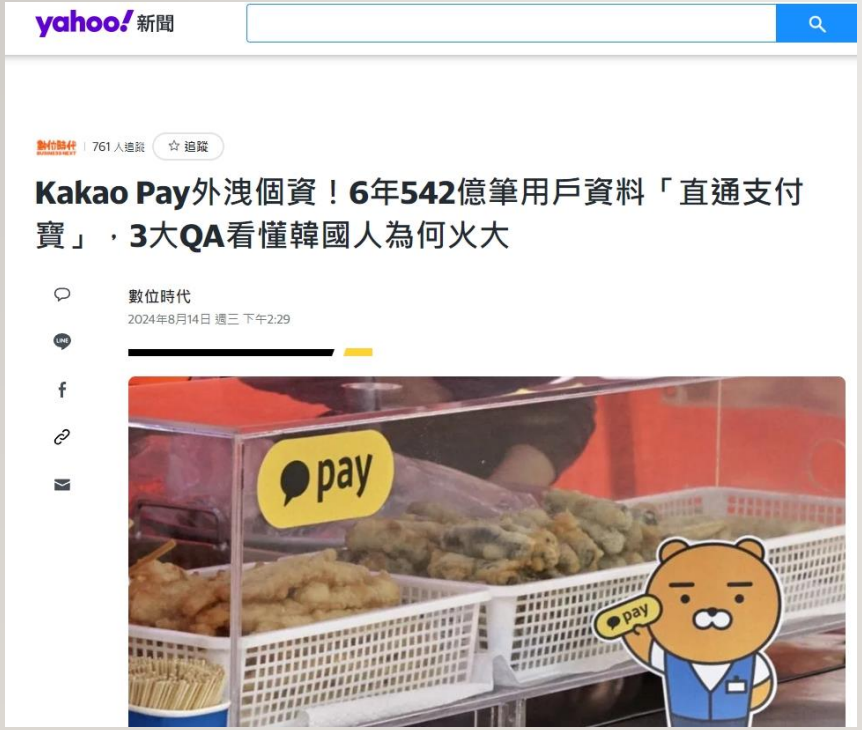
39 降低個資外洩風險

- 含有個資的機敏文件勿隨意擺放。
- 網路表單需進行權限控管。
- 傳送含有個資之電子文件應加密處理。
- 認知宣導及教育訓練。

40 個資敏感系統



41 個資外洩案例分享2024.8.14 (只要提供個資，就必須經過用戶同意)



Q1:Kakao Pay從2018年4月起，每天向支付寶提供一次使用者個資，累計達542億筆，包括Kakao帳號、手機號碼、電子郵件、訂單交易內容、帳戶餘額與加值紀錄等。

Q2:支付寶是全球規模最大的第三方支付平台一，**Kakao Pay透過委託合作，就能在與支付寶簽約的TEMU、Google、Apple等46國8100萬家商店提供支付服務，擴大全球市場影響力。**

Q3:Kakao Pay強調，提供支付寶的用戶資料都經過加密處理，無法作為其他用途使用。
****但金融監督院認為，加密處理的個資也能被輕易復原，安全性不足，只要提供個資，就必須經過用戶同意。**。**

資料來源：https://reurl.cc/93OVdd

個資案例分享

某國立女中疑似個資外洩

網路調查表單：疑似個資洩漏約613筆

影響範圍：新生基本資料(包含班級、姓名、性別、身分證字號、生日、地址、電話、個人及家庭概況等資料。)

應變措施：資安通報、移除表單及連結、檢討表單發布程序、加強教育訓練、增加人員資安意識、落實個資保護措施。

資料來源：https://reurl.cc/7e4qQk

43 使用雲端服務蒐集個資注意事項

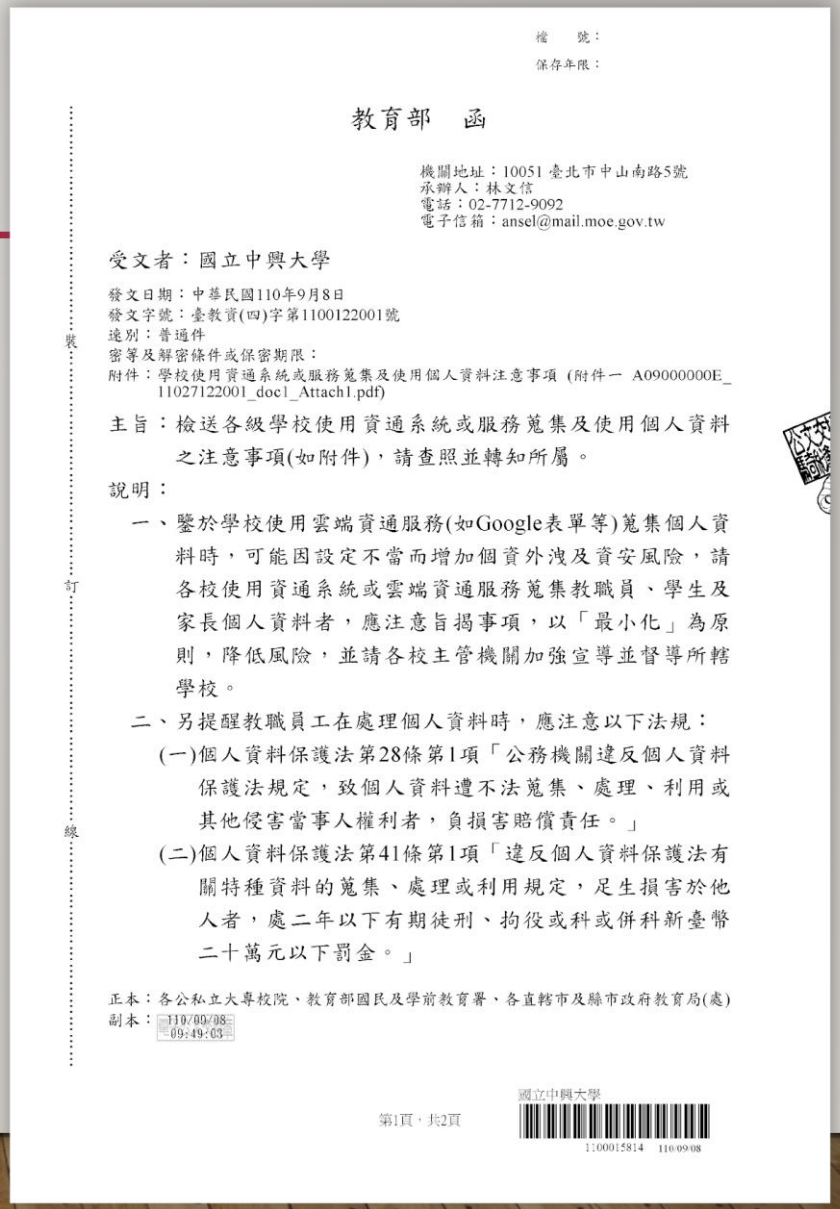
依據教育部110年9月8日函告各級學校使用資通系統或服務蒐集及使用個人資料之注意事項中，鑒於學校使用雲端資通服務(如Google表單等)蒐集個人資料時，可能因設定不當而增加個資外洩及資安風險。

44 使用雲端服務蒐集個資注意事項

- 依據 教育部 函
- 發文日期：中華民國110年9月8日
- 發文字號：臺教資(四)字第1100122001號
- 學校為行政目的使用資通系統或雲端資通服務(如Google表單、Microsoft Forms等問卷調查服務)蒐集個人資料時應注意事項，其中有三項尤其要特別小心謹慎處理：

- **1.資料蒐集最小化**
- 僅蒐集適當、相關且限於處理目的所必要之個人資料，處理及利用時，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。
- **2.存取控制**
- 應注意檔案存取權限設定，應採最小權限原則，僅允許使用者依目的，指派任務所需之最小授權存取。
- **3.避免個資外洩**

使用雲端資通服務者，應詳閱設定內容，不宜使用者共同編輯個人資料檔案清冊，並應注意避免設定允許顯示其他使用者作答內容（如Google表單不應勾選「顯示摘要圖表和其他作答內容」），避免使用者能瀏覽其他使用者資料，造成個人資料外洩。公佈前應確實做好相關設定檢查，並實際操作測試，確認無誤後再行發布。



檔　　號：
保存年限：

教育部　函

機關地址：10051 臺北市中山南路5號
承辦人：林文信
電話：02-7712-9092
電子信箱：ansel@mail.moe.gov.tw

受文者：國立中興大學

發文日期：中華民國110年9月8日
發文字號：臺教資(四)字第1100122001號
速別：普通件
密等及解密條件或保密期限：
附件：學校使用資通系統或服務蒐集及使用個人資料注意事項（附件一 A09000000E_11027122001_doc1_Attach1.pdf）

主旨：檢送各級學校使用資通系統或服務蒐集及使用個人資料之注意事項(如附件)，請查照並轉知所屬。

說明：

一、鑒於學校使用雲端資通服務(如Google表單等)蒐集個人資料時，可能因設定不當而增加個資外洩及資安風險，請各校使用資通系統或雲端資通服務蒐集教職員、學生及家長個人資料者，應注意旨揭事項，以「最小化」為原則，降低風險，並請各校主管機關加強宣導並督導所轄學校。

二、另提醒教職員工在處理個人資料時，應注意以下法規：

(一)個人資料保護法第28條第1項「公務機關違反個人資料保護法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。」

(二)個人資料保護法第41條第1項「違反個人資料保護法有關特種資料的蒐集、處理或利用規定，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。」

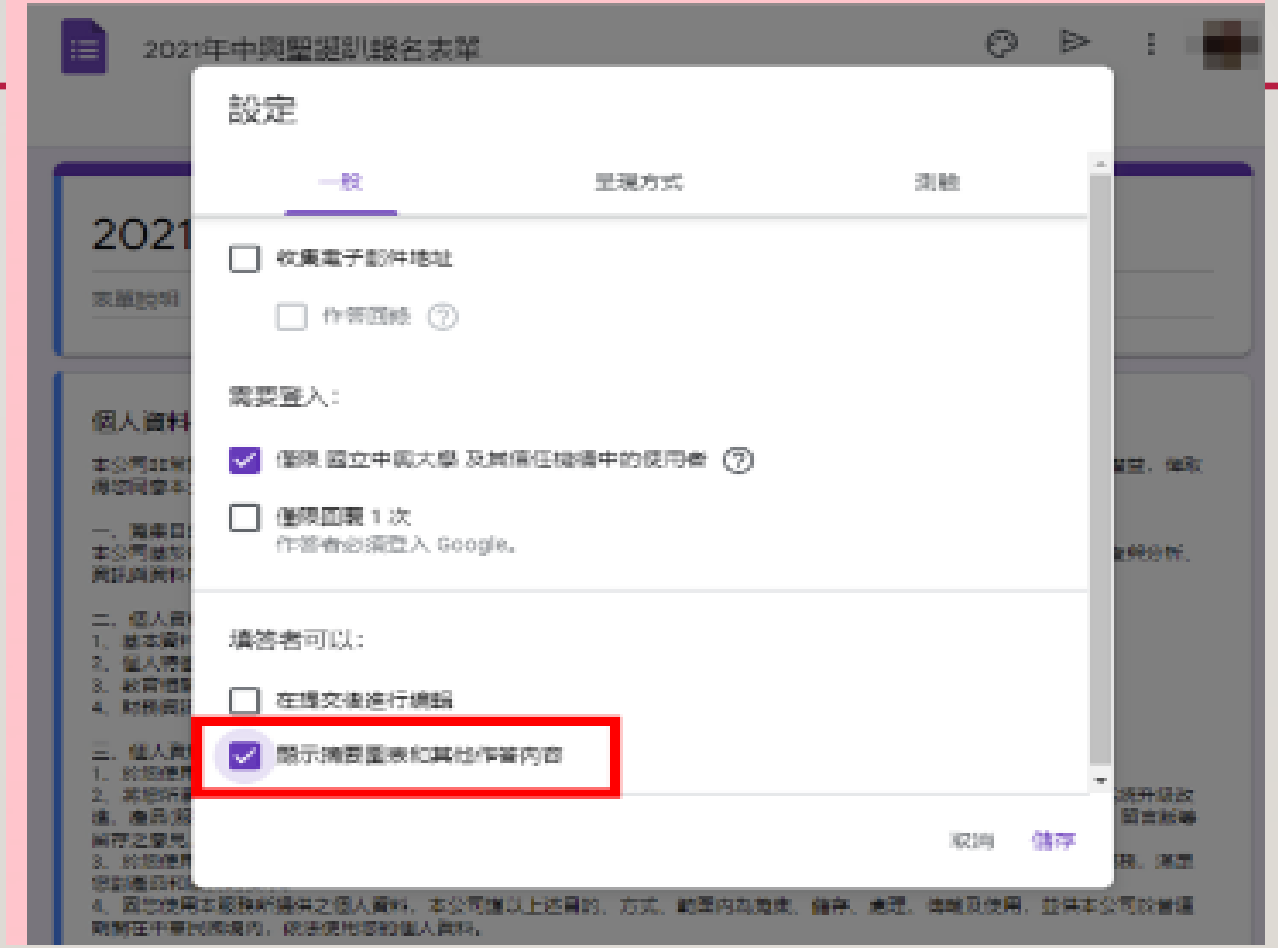
正本：各公私立大專校院、教育部國民及學前教育署、各直轄市及縣市政府教育局(處)
副本：110/09/08 09:49:03

第1頁，共2頁

國立中興大學
1100015814　110/09/08

45 GOOGLE表單錯誤範例

1. 假如Google表單右上角的齒輪(設定)選項「顯示摘要圖表和其他作答內容」被勾選了。



影片：Google表單蒐集個人資料使用原則

46 GOOGLE表單錯誤範例1

2.當「顯示摘要圖表和其他作答內容」勾選起來後讓其他人填寫表單並送出後會有「查看先前的回應」可以點選。

影片： Google表單蒐集個人資料使用原則

47 GOOGLE表單錯誤範例2

3.點選「查看先前的回應」可以看到所有人填寫的回覆。

影片：Google表單蒐集個人資料使用原則

案例分享

某國立大學個資外洩

EMAIL：個資洩漏約450筆

影響範圍：姓名、身分證字號、學號、科系及報名類別等資料。

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。

49 案例分享

補教師找駭客 竊750萬個資販售

2021-11-18 00:36 聯合報 / 記者邵心杰、趙宥寧／連線報導

+ 教育部

讚 25 分享 分享

調查官清查時，赫然發現自己名字，向檢方提報指揮偵辦，不少檢察官小孩正念國中小及高中學生，也發現自己名字名列其中。記者邵心杰／翻攝

台南地檢調查，蔡男是補教業最大個資販售商，柴男曾任學校網路管理員，熟稔機關及學校網頁設計架構，擅長撰寫程式攻擊網頁漏洞，自機關及學校竊取學生資料；張男國小起自研駭客程式，曾於大學時期駭入他人網站遭起訴，擅長破壞網頁防火系統侵入後台。

資料來源：https://udn.com/news/story/7321/5898667
https://reurl.cc/8W6A3X

50 案例分享

北市員警涉勾結徵信業並洩漏民眾個資

臺北市警察局在11月17日發布公告，指出台北市警局去年偵辦刑事案件時，在搜索徵信業電腦時，發現與北市員警的往來資訊，有員警涉嫌利用警政知識聯網查詢民眾個資，再洩露給徵信業者，因此昨日已與警政署政風室進行搜索，並以刑法洩密罪，以及違反個人資料保護法偵辦。警方同時強調，此事由內部發現主動查辦防弊，並表示將加強落實內部資安管理，以及資訊稽核作為。

資料來源：https://www.ithome.com.tw/news/147931
https://reurl.cc/g0ebQ4

51 案例分享

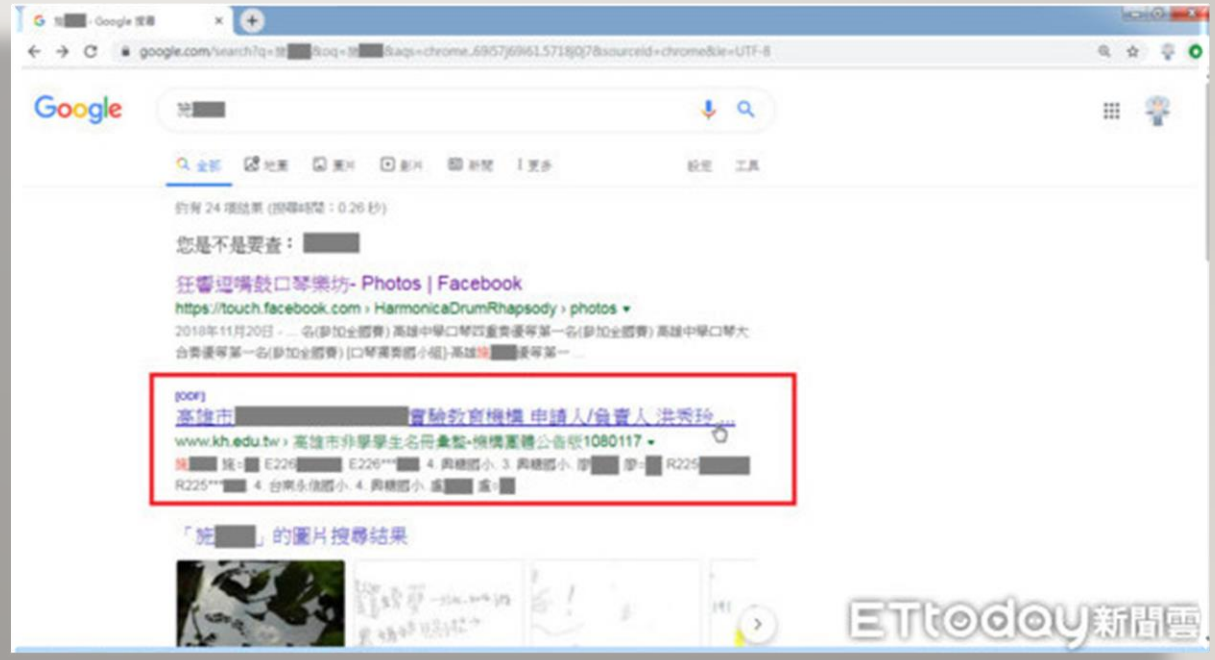
資料來源：https://news.tvbs.com.tw/life/1577012

52 案例分享

資料來源：https://technews.tw/2021/12/07/line-pay-github/

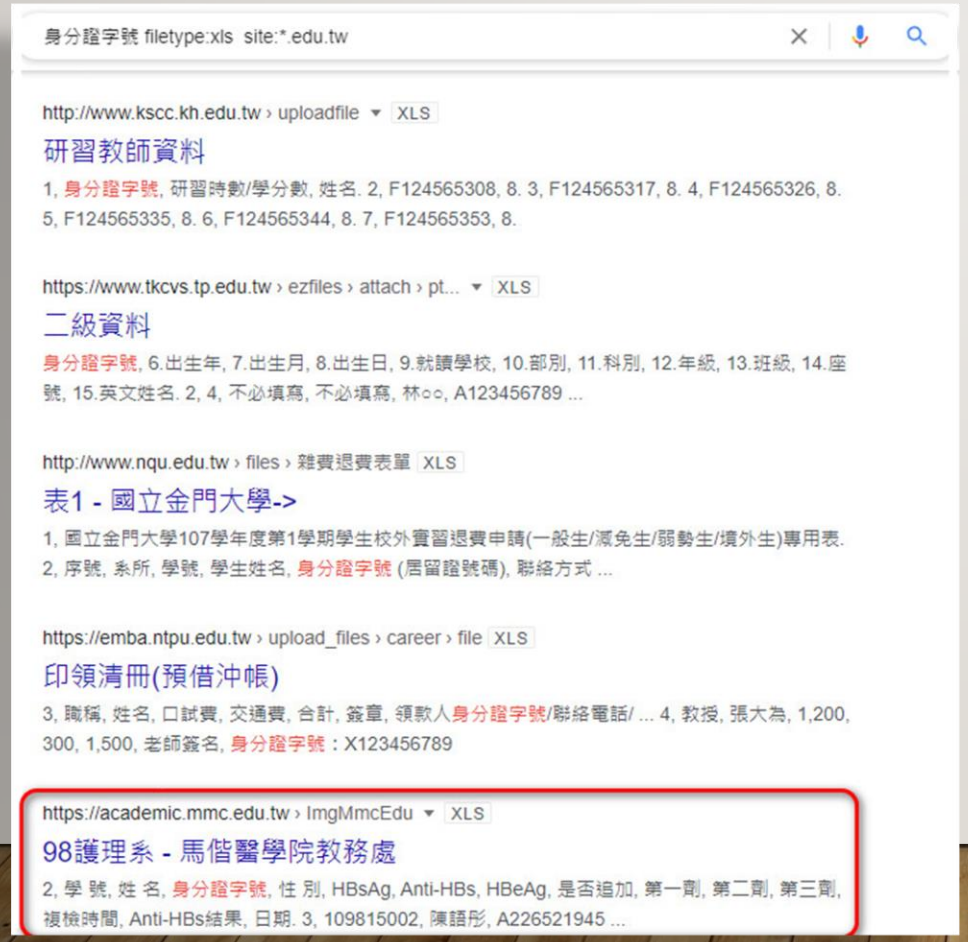
案例分享

高雄市府又挨罵了！
280名學生個資外洩...
家長怒轟教育局：還怪我破解檔案



資料來源：https://www.ettoday.net/news/20200116/1626999.htm?from=pctaglist

案例分享-實際演練



馬偕醫學院　醫學系B型肝炎疫苗追蹤注射名冊98學年度

姓　名	身分證字號	性　別	複檢時間	Anti-HBs結果
林　萱	A2[redacted]0	女	99.12.31	POSITIVE
陳　奇	H1[redacted]9	男	99.03.01	POSITIVE
朱　樺	A1[redacted]9	男	98.09.11	BORDERLINE NEGATIVE
章　綱	F1[redacted]0	男	99.5.13	POSITIVE
張　宇	F1[redacted]3	男	98.9.11	NEGATIVE
林　婷	A2[redacted]0	女	98.09.10	BORDERLINE NEGATIVE
謝　敏	A2[redacted]7	女	98.09.11	NEGATIVE
李　顗	A1[redacted]4	男	98.09.11	NEGATIVE
徐　蓁	F1[redacted]4	男	99.05.13	POSITIVE
宋　佑	F1[redacted]5	男	98.09.11	NEGATIVE
郭　志	F1[redacted]9	男	98.09.11	NEGATIVE
呂　謙	F1[redacted]2	男	98.09.11	NEGATIVE
許　涵	F1[redacted]7	男	98.09.11	NEGATIVE
李　煒	F1[redacted]8	男	98.09.11	NEGATIVE
許　顥	H1[redacted]8	男	98.09.11	NEGATIVE
林　慧	N2[redacted]7	女	98.09.11	NEGATIVE
李　宇	K1[redacted]8	男	98.09.11	BORDERLINE NEGATIVE
林　杰	P2[redacted]3	女	98.09.11	NEGATIVE
邱　叡	E1[redacted]4	男	98.09.11	NEGATIVE
林　逸	E1[redacted]3	男	99.05.06	POSITIVE
陸　偉	G1[redacted]7	男	98.09.11	NEGATIVE
高　碩	B1[redacted]5	男	98.09.11	NEGATIVE
王　琪	A2[redacted]5	女	98.09.11	NEGATIVE

案例分享

MOMO購物網成「高風險賣場」
192人受害，半年被詐走2824萬

資料來源：https://www.ettoday.net/news/20200627/1747439.htm?from=pctaglist

案例分享

秀泰影城遭駭取個資90人挨詐
他接「客服電話」8小時被騙114萬

網路訂票系統疑似遭到駭客入侵
盜取個資

電話詐騙>會員系統設定錯誤>
誤訂20張電影票，將從綁定的信用卡扣款

請協助設定取消扣款>網銀、ATM操作...

資料來源：https://www.ettoday.net/news/20211108/2119077.htm?from=pctaglist

十要!


要使用高強度密碼
要定期修改密碼
電腦系統要更新
電腦防毒要更新
社交工程要小心
要使用合法軟體
電子郵件要過濾
重要資料要備份
機敏資料要保護
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