資訊安全與個資保護管理實務

鍾沛原

講師簡介

- 鍾沛原
- 經歷：

  教育機構資安驗證中心資安暨個資主導稽核員

  成大資通安全研究與教學中心 專案經理

  行政院資通安全稽核委員

  教育部所屬公務機關及所管特定非公務機關資通安全稽核委員

  教育體系資通安全職能訓練課程講師

  國教署校園資通安全業務管理輔導團資安輔導委員

  經濟部能源及水資源領域關鍵基礎設施資通安全稽核委員

  衛生福利部資通安全稽核委員

  交通部公路局所屬機關資通安全稽核委員
- 證照： ISO27001:2022 LAC、 ISO27701:2019 LAC、ISO29100:2011 LAC、BS 10012:2017 LAC、CEH、CCNA、經濟部iPAS 資訊安全工程師中級能力鑑定...
- 計畫執行：經濟部「關鍵基礎設施資安聯防服務專案」科技部「資安監控與管理技術開發」、經濟部能源局「強化民營能源關鍵資訊基礎設施資安防護計畫」、經濟部水利署「水資源關鍵設施升級及安全管理確保旗艦計畫」、行政院「我國電腦機房異地備援機制委託研究計畫」、教育部「教育單位網站弱點檢測與防洩漏個資資安服務計畫」.....等。

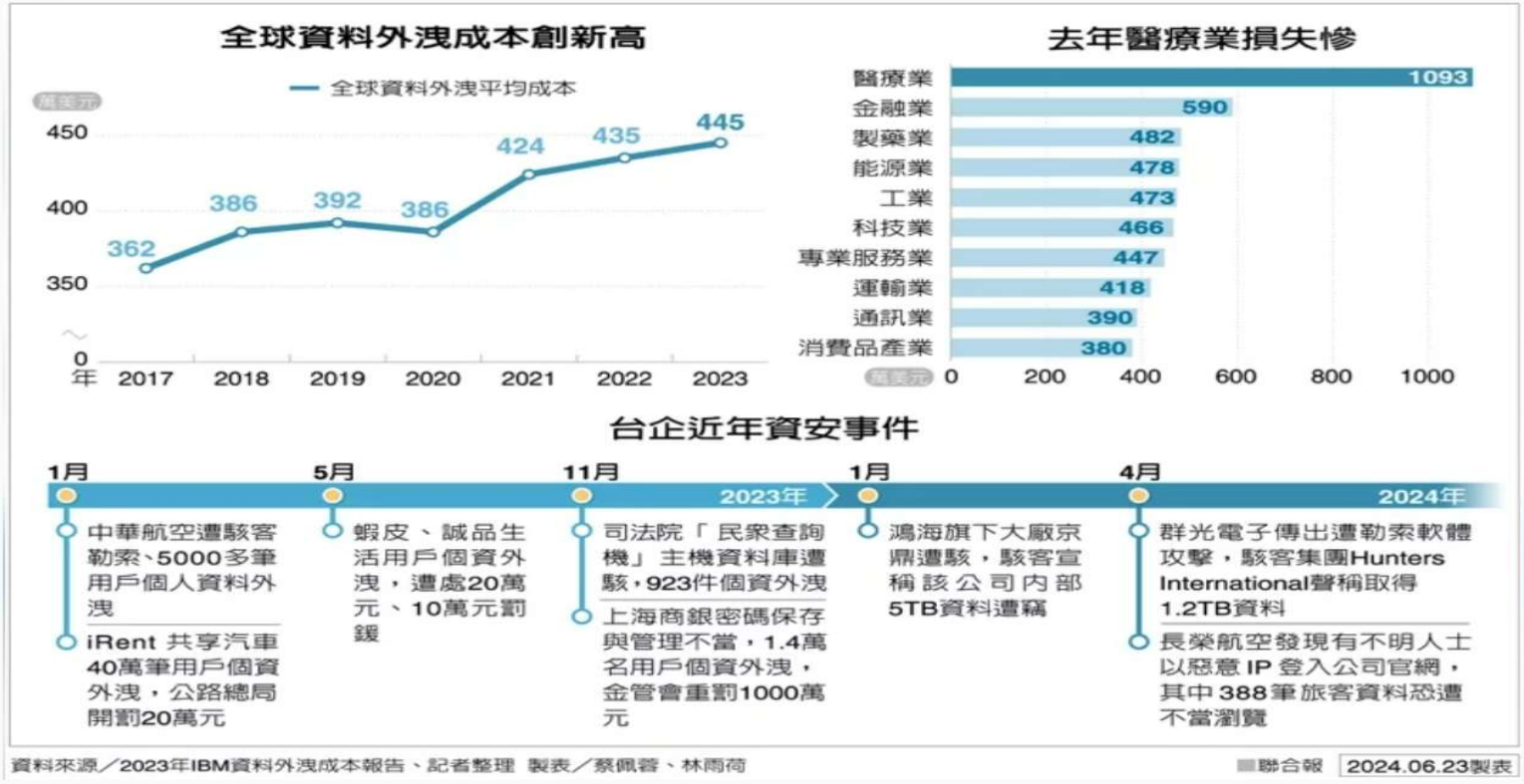
大綱

- 網路威脅趨勢
- 近期校園資通安全事件案例
- 常見校園個資事件
- 結論

看不見的戰爭持續發生

不見血戰爭／去年遭攻擊近4千億次 台企淪駭客眼中肥羊

2024-06-24 00:57 聯合報／ 記者馬瑞璿／專題報導



全球資料外洩成本創新高 製表／蔡佩蓉、林雨荷 圖／聯合報提供

https://udn.com/news/story/124068/8049888

勒索軟體攻擊並未消失

電腦王 讚 9 LINE

首頁 > 雲端/資訊安全

勒索軟體獲利再創新高，受害者支付贖金的意願卻降低

netizen 發表於 2024年8月22日 13:00 收藏此文 讚 9

這家區塊鏈情報公司在今年早些時候發布的報告中透露，2023年全球勒索軟體支付總額首次超過10億美元，其於週四發布的年中報告顯示，2024 年也有可能達到甚至超過去年的數字。

雖然2023年上半年和2024年上半年全球勒索軟體的總收入僅增加了2%，從4.491億美元增加到4.598億美元，但個別支付的成本顯示出更顯著的趨勢變化。

舉例來說，在支付金額超過 100 萬美元的嚴重勒索軟體集團中，勒索軟體付款的中位數從 2023 年初的不到 20 萬美元，到 2024 年 6 月中旬增加了近八倍，達到約 150 萬美元。

歷史上最高的勒索軟體付款金額是 2024 年初一家未具名的財富 500 強公司向 Dark Angels 勒索軟體集團支付的 7500 萬美元，這也比 2023 年最高的 3780 萬美元付款金額增加了近 100%。

Chainalysis 表示，這些數據表明，主要的勒索軟體集團「正在優先考慮針對大型企業和關鍵基礎設施供應商，這些企業由於財力雄厚和系統重要性，可能更願意支付高額贖金」。

同時，儘管今年到目前為止被勒索軟體組織洩漏網站曝光的受害者數量增加了10%，但總的勒索軟體支付事件卻減少了超過27%，這表明在勒索軟體攻擊後，成功被勒索的受害者比例較小。

根據Chainalysis在上週發布的2024年加密犯罪年中更新報告，儘管支付勒索軟體的受害者減少，2024 年的勒索軟體付款總額仍有可能再創新高。

https://www.techbang.com/posts/117696-ransomware-software-victims

勒索病毒=資料竊取+資料加密

駭客盜走「1.2TB資料」揚言勒索 台灣群光發重訊回應

陳奕廷

2024年4月22日

（記者陳奕廷／綜合報導）電子零組件大廠群光電子傳出16日遭勒索軟體攻擊，駭客組織聲稱取得共1.2TB逾414萬個檔案，並將所有檔案加密。群光電子終於在昨（21）日於公開資訊觀測站發布重大訊息。

群光電子在第一時間未主動發布遭駭客入侵，是否已違反證交所規定？群光電子表示，在檢視證交所的資安事件規定後，認為攻擊程度並未達到需要發布重訊的標準，且對公司營運沒有影響。

證交所在2024年1月發布新版「上市公司重大訊息發布應注意事項」，明定資安事件的重訊標準，其中包括公司的核心資通系統、官方網站或機密文件檔案資料等，遭駭客攻擊、破壞等。

至於駭客聲稱將部分檔案加密，外傳群光找了國內解密公司協助後才脫困，並沒支付贖金。群光說明，公司持續有與外部顧問公司合作，檔案非機密檔案，也不存在無法開啟檔案的問題。

不過，經過數日後，群光電子終於發布重訊，證實公司資安單位於查知遭受網路攻擊時，已啟動相關防禦機制與復原作業，且經檢視證交所資安事件重訊規定，並未有公司核心資通系統、官方網站遭駭客攻擊或入侵，致無法營運或正常提供服務，亦未有個資、機密文件檔案資料外洩之情事，因此未造成公司重大損害或影響。

https://tw.news.yahoo.com/%E9%A7%AD%E5%AE%A2%E7%9B%9C%E8%B5%B0-1-2tb%E8%B3%87%E6%96%99-%E6%8F%9A%E8%A8%80%E5%8B%92%E7%B4%A2-%E5%8F%B0%E7%81%A3%E7%BE%A4%E5%85%89%E7%99%BC%E9%87%8D%E8%A8%8A%E5%9B%9E%E6%87%89-094553661.html

不付贖金，我幫你通報

iThome 新聞 產品&技術 專題 AI Cloud 醫療IT 資安 研討會 社群 IT EXPLAIN

全新系列【數位轉型攻略 V：戰略新 IT】 2024臺灣資安大會徵稿啟動 2024 臺灣雲端大會徵稿「

新聞

上市公司遭網路攻擊未披露，勒索軟體集團向SEC告狀

攻擊上市公司MeridianLink的勒索軟體集團AlphV，宣稱向美國證券交易委員會（SEC）指控MeridianL依法對外揭露資安事故細節，違反SEC的規定

文/ 陳曉莉 | 2023-11-17 發表

https://www.ithome.com.tw/news/159886

勒索軟體集團威脅受害者支付贖金的招數愈來愈多，從早期加密受害者系統上的資料、竊取受害者資料，一直到最近，勒索軟體集團AlphV竟然直接向美國證券交易委員會（SEC）告狀，指控於美國紐約股市公開發行股票的MeridianLink並未如實對外揭露其遭到網路攻擊的意外事件。但迄今不管是SEC或MeridianLink都拒絕回應此事。

過去勒索軟體集團加密受害者系統資料時，以解密作為要脅，等到大多數企業都知道要備份系統時，勒索軟體集團開始竊取系統資料，並以外洩資料作為要脅，目的都是為了逼迫受害者支付贖金，而隨著SEC祭出新規定，要求上市公司要在4天內披露重大資安事件，也成為駭客的要脅手段。

MeridianLink專門提供各種解決方案予金融組織，包括端對端平臺、貸款發放系統、抵押貸款、開立存款帳戶、資料與報告等，客戶則涵蓋了銀行、信用合作社及抵押貸款機構。

而根據《DataBreaches》引用一名參與該攻擊的消息來源報導，AlphV是在11月

誠實為上策/被偷一次可能後患無窮

9.2k 人追蹤 ☆ 追蹤

證實遭匿名勒贖 華航

華視
2023年1月8日

本資料由 (上市公司) 2610 華航 公司提供

序號	2	發言日期	113/03/26	發言時間	22:31:30
發言人	魯淑慧	發言人職稱	處長	發言人電話	(03)399-8600
主旨	針對駭客於暗網放出會員資料提出說明				
符合條款	第 26 款	事實發生日	113/03/26		
說明	1.事實發生日:113/03/26 2.發生緣由:本公司發現駭客於暗網販售公司會員資料事件。 3.處理過程:經查本次駭客揭露內容與本公司現有會員資料庫不符，並非113年1月更新之資料，應為之前同起個資情事。本公司已依程序報警，並依法通報主管機關。 4.預計可能損失或影響:目前評估對公司營運尚無重大影響。 5.可能獲得保險理賠之金額:不適用。 6.改善情形及未來因應措施: 本公司已通知提醒所有會員，自113年4月2日起，所有會員於線上登入須透過手機或電子信箱接受一次性密碼(OTP)。 7.其他應敘明事項:無。				

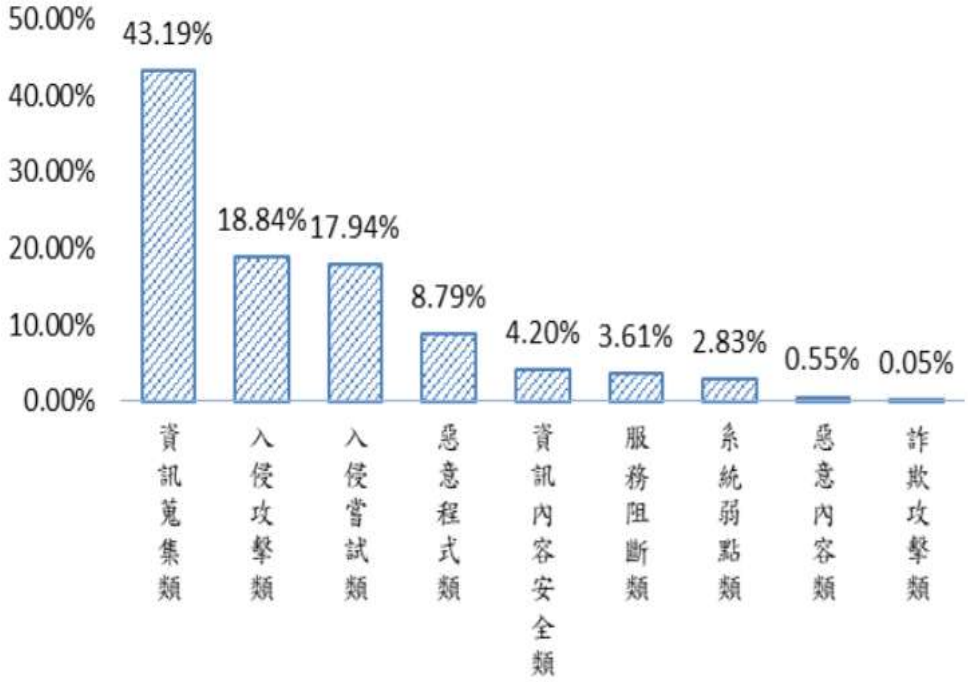
的網路勒索信件，第一時間啟
通報主管機關，強調並沒有影
示，雖然華航沒有指出，是哪
刨勒索病毒的層級，但仍提醒
號密碼區隔。

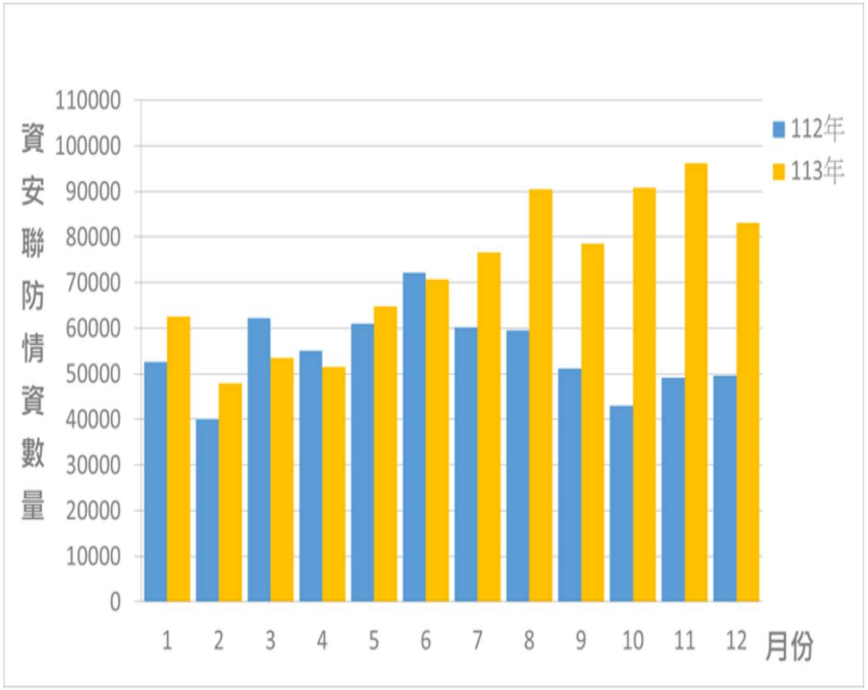
斷，先是航勤爆集體請假罷工
明強調，第一時間就啟動了防
量，也沒有會員資料遭不當使
劉彥伯說：「華航它透露的資
其實民航局的這個系統，(跟
又有塔台人員的控管。」

https://tw.news.yahoo.com/news%2F%E8%AD%89%E5%AF%A6%E9%81%AD%E5%8C%BF%E5%90%8D%E5%8B%92%E8%B4%96-%E8%8F%AF%E8%88%AA-%E6%9C%AA%E5%BD%B1%E9%9F%BF%E8%88%AA%E7%8F%AD-%E6%9C%83%E5%93%A1%E5%80%8B%E8%B3%87-043200394.html

113年政府資安威脅統計

- 聯防預警情資

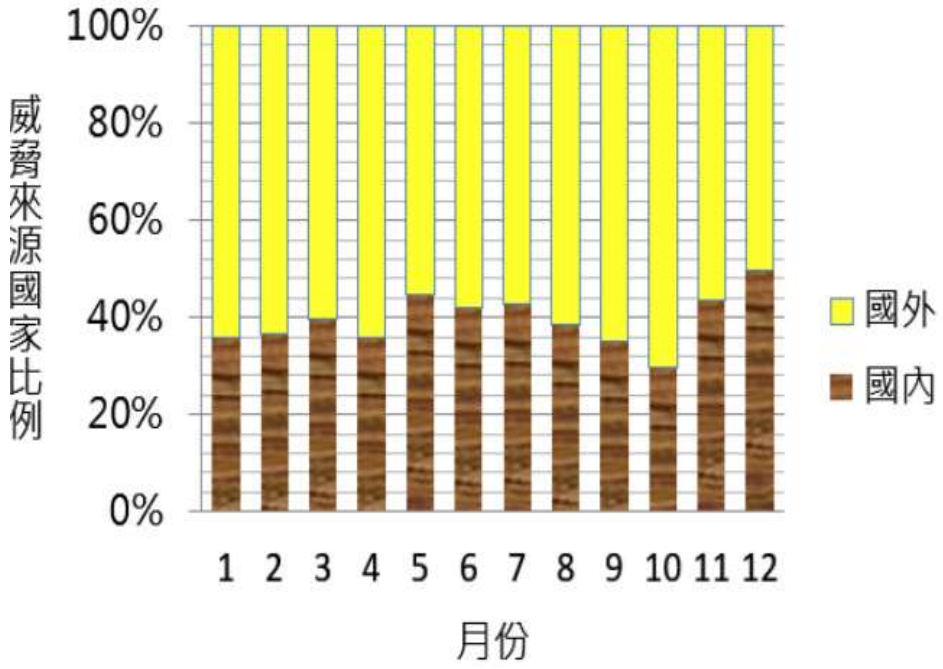


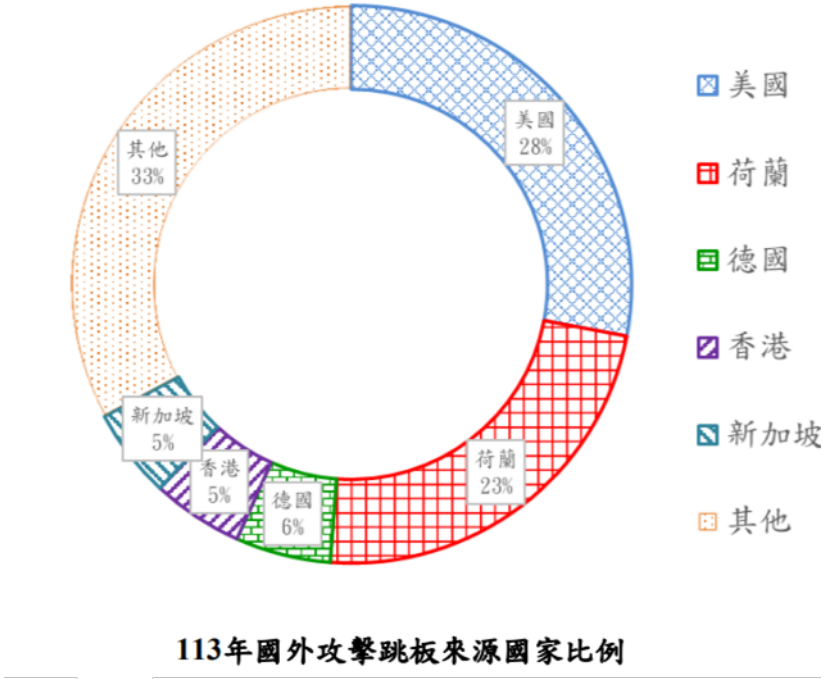


https://www-api.moda.gov.tw/File/Get/acs/zh-tw/ynSogYbKmbnxlFE

113年政府資安威脅統計(cont.)

- 攻擊跳板來源 IP





113年國外攻擊跳板來源國家比例

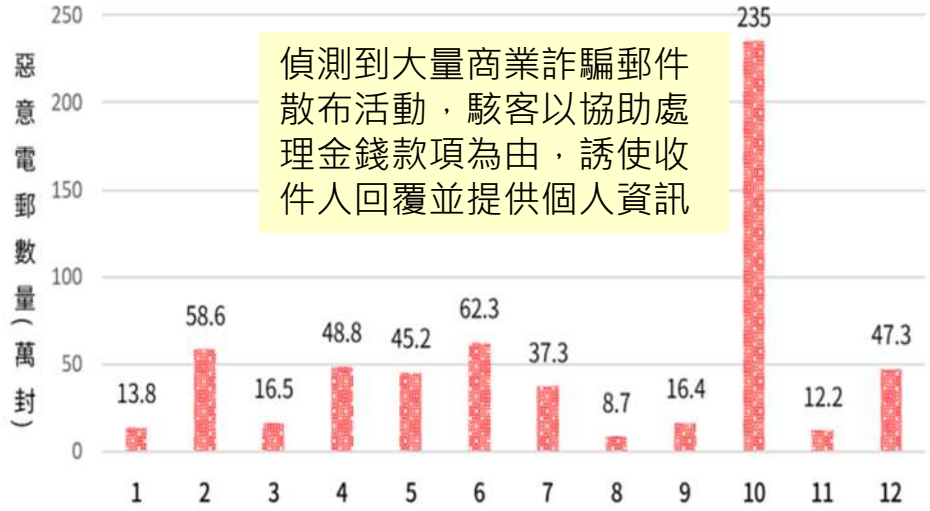
https://www-api.moda.gov.tw/File/Get/acs/zh-tw/ynSogYbKmbnxlFE

113年政府資安威脅統計(cont.)

❑ 惡意電子郵件

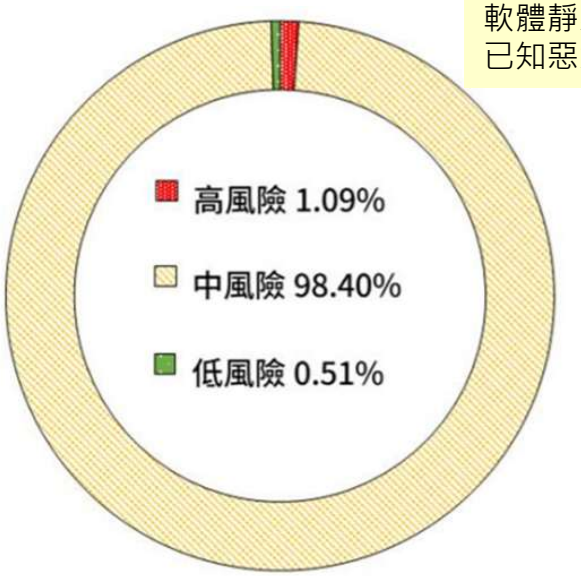
共檢測2餘億(229,111,770)封電子郵件，發現 可疑惡意電子郵件602餘萬(6,027,182)封，約占整體之2.63%

偵測到大量商業詐騙郵件散布活動，駭客以協助處理金錢款項為由，誘使收件人回覆並提供個人資訊



113年政府骨幹每月惡意電子郵件偵測數量

中、低風險之判定為惡意電子郵件內嵌可疑連結，經威脅情資比對 或附檔經防毒軟體靜態掃描，具有已知惡意態樣或特徵



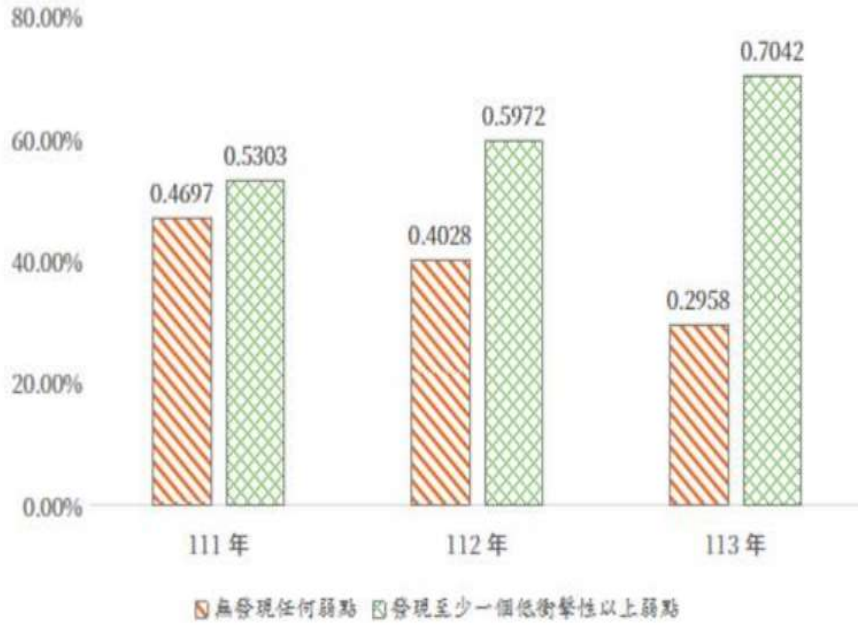
惡意電子郵件風險分布比例

https://www-api.moda.gov.tw/File/Get/acs/zh-tw/ynSogYbKmbnxlFE

113年政府資安威脅統計(cont.)

❑ 網路攻防演練

71個機關3,459個對外系統，演練結果
發現50個機關對外資通系統存在弱點

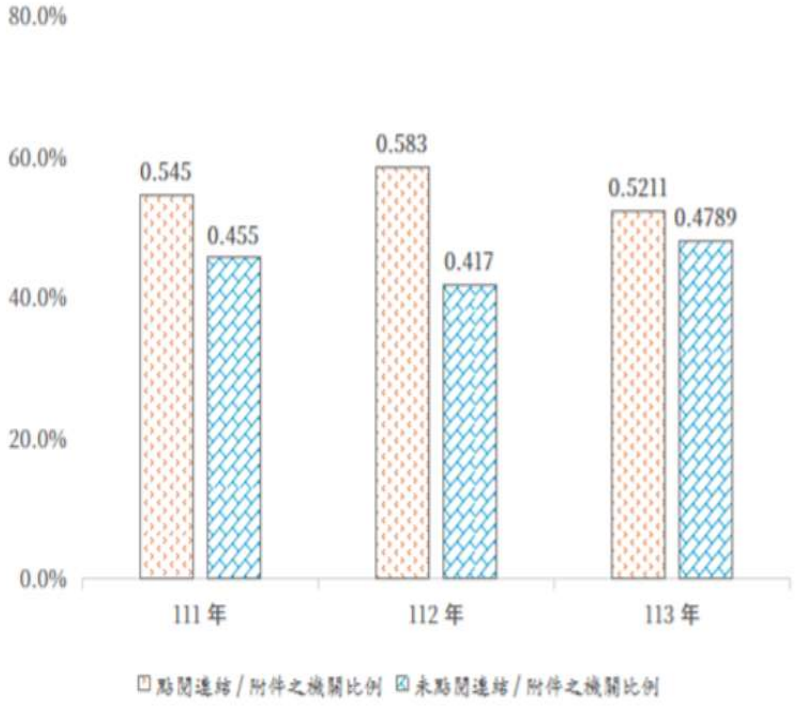


共發現554個弱點，重大衝擊性弱點
數量 92個，高衝擊性弱點數量195個

https://www-api.moda.gov.tw/File/Get/acs/zh-tw/ynSogYbKmbnxlFE

113年政府資安威脅統計(cont.)

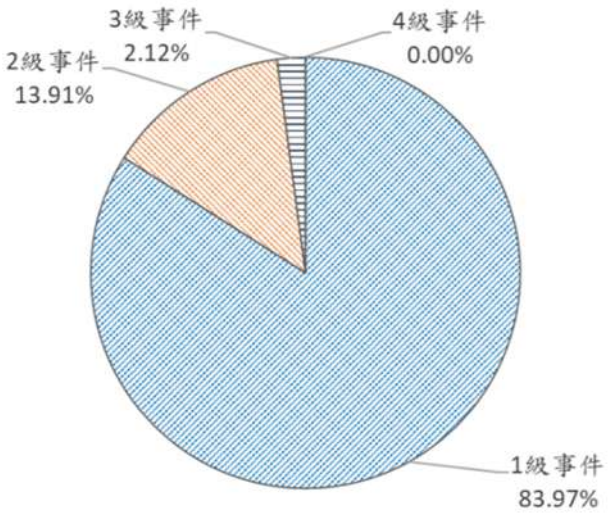
- 社交工程演練(71個機關，受測人數計有1萬9,986位)



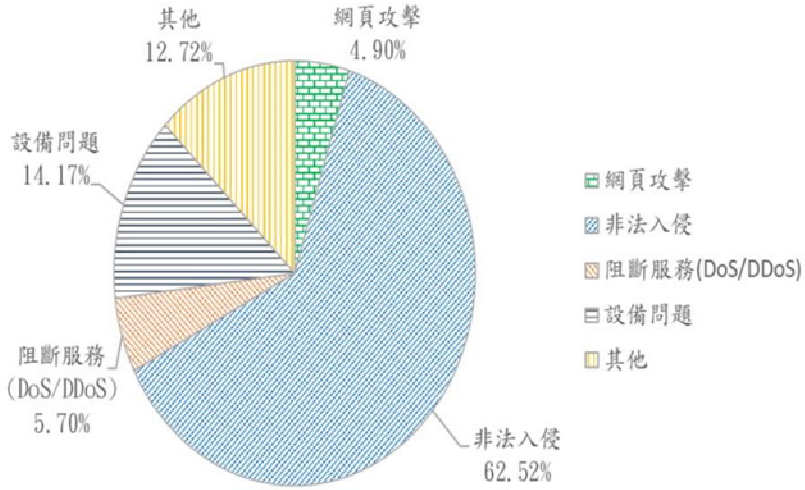
https://www-api.moda.gov.tw/File/Get/acs/zh-tw/ynSogYbKmbnxlFE

113年政府資安威脅統計(cont.)

- 資安事件通報



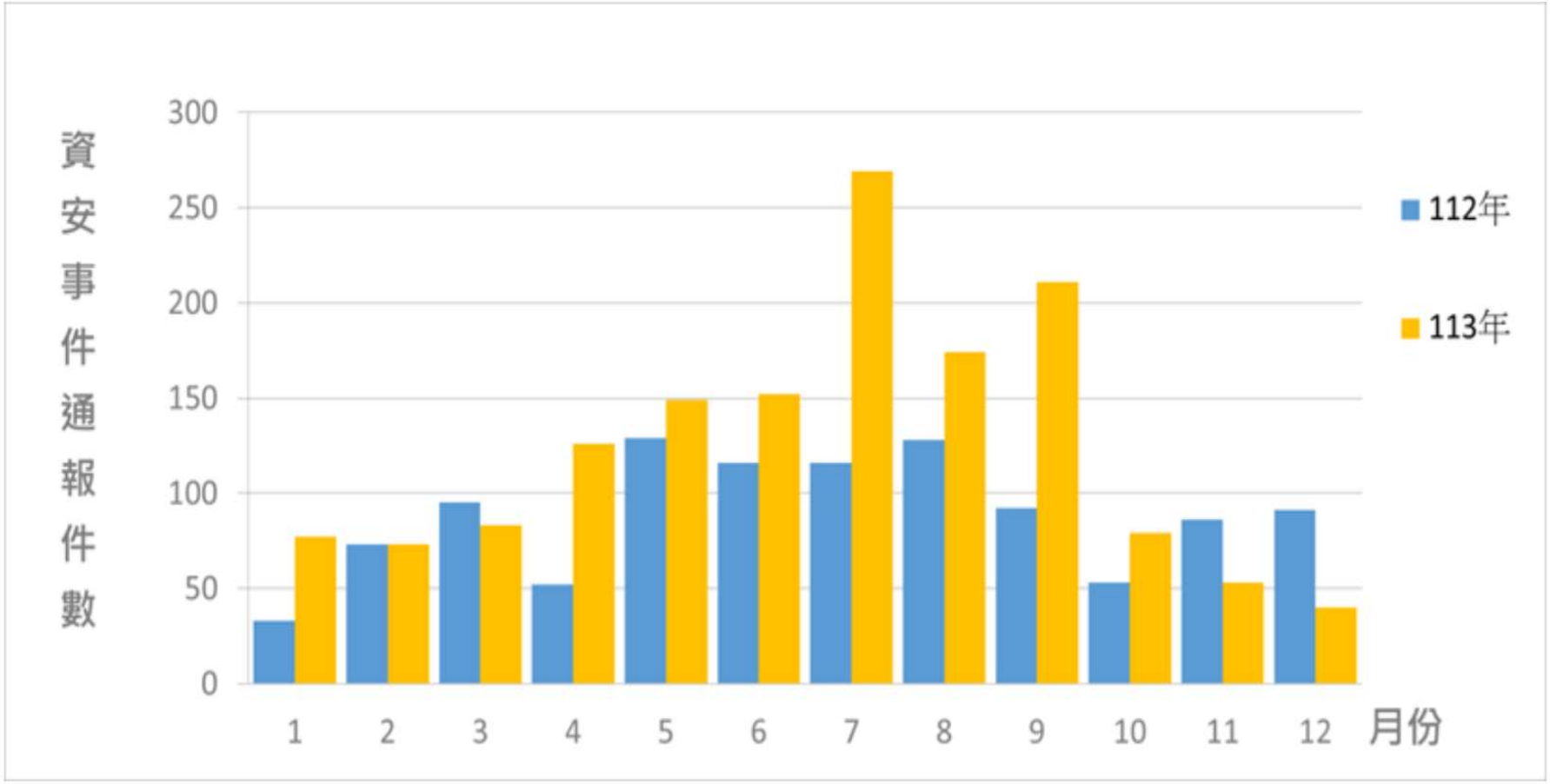
113年資安事件等級比例



113年資安事件類型比例

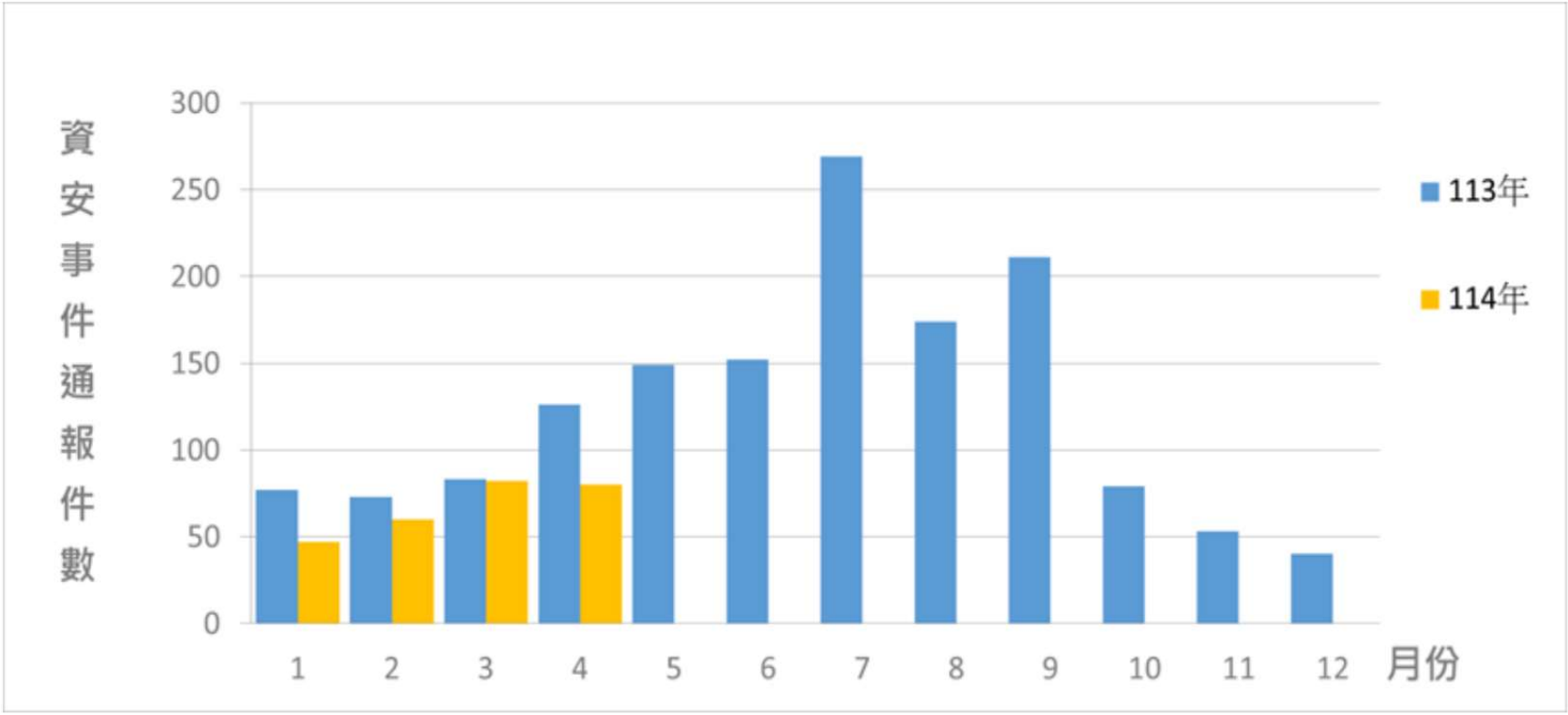
https://www-api.moda.gov.tw/File/Get/acs/zh-tw/ynSogYbKmbnxlFE

113年資安事件通報數量統計



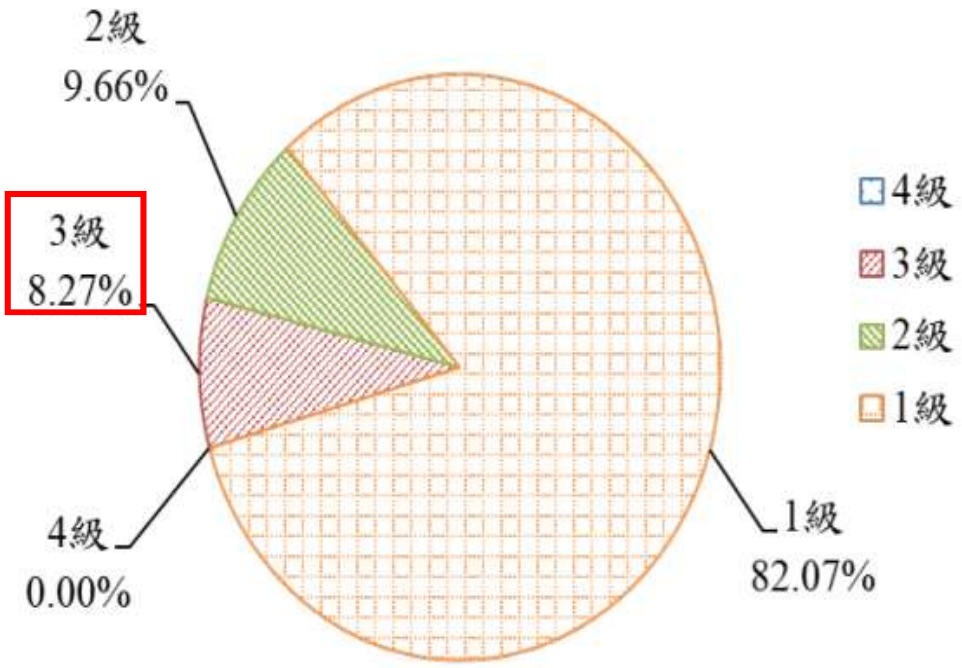
114年04月資安事件通報數量統計

本月資安事件通報數量共80件(較上月減少2件)，較去年同期減少36.51%，通報類型以非法入侵為主，占本月通報件數66.25%，其中多個機關資訊設備異常連線或疑似遭建立後門連結。近1年資安事件通報統計詳見圖2。



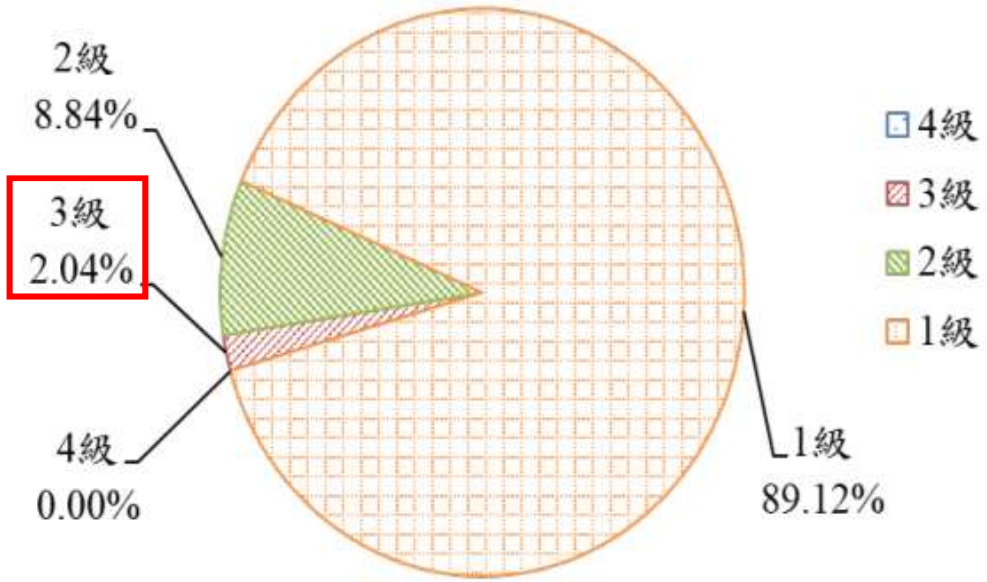
資料來源：行政院國家資通安全會報-資安月報

113年第4季通報資安事件等級比例



- 有管理人員不慎誤傳含有其他民眾之檔案予其他人或組態加密機制設計不佳，遭複製後得瀏覽相關個人資訊，因涉及敏感資訊外洩，故通報為 3 級。
- 供應廠商疏失，於例行性作業時，不慎將部分維運資訊上傳至公開服務網站，因該資訊於機關內部定義為敏感，通報為 3 級事件。

114年第1季通報資安事件等級比例



資料來源：行政院國家資通安全會報技術服務中心資通安全技術報告

- 某機關委外辦理公開活動時，將活動簡章置放於雲端空間供民眾掃描下載。惟該受委託廠商亦將活動報名參與者資料上傳至該雲端，因未設置適切地存取權限，致使用者於掃描 e-DM 上之二維條碼後連結至雲端時，發現能存取活動參與者之個人資料。
- 業務承辦人誤植他人電子郵件信箱，致個人敏感性檔案資料外洩

近期聯防情資彙整(cont.)

- 114年01月
  - 駭客**偽冒資安院**，對臺灣學術機構發動針對性社交工程電子郵件攻擊，以**「資安攻擊預警」**名義，要求收件人執行勒索軟體偵測工具，以因應勒索軟體攻擊活動，惟實則誘騙收件人下載與執行惡意附檔。
  - 某機關於辦理活動期間，將活動簡章存放於Google 雲端空間供民眾下載，惟承攬廠商亦將**包含個人資料之報名者資訊上傳至該雲端空間**，且存取權限設定未臻完善，致未授權之使用者得以存取相關資料，導致民眾個人資料外洩事件。
- 114年02月
  - 偽冒財政部名義並以**稅務調查**為由，對政府機關與台灣企業機構發動社交工程電子郵件攻擊，並針對具敏感資訊存取權限之財務人員，誘導開啟並點擊附檔內含之惡意連結。
  - 某機關發現同仁電腦執行不明程式，並對外產生異常連線。經調查發現攻擊者透過**求職網傳送之履歷夾帶惡意附件**，同仁因業務需求下載附件，發現疑似Excel試算表之檔案，惟該檔案實際上係Excel外掛元件(XLL)可執行檔，同仁執行檔案後，即觸發惡意程式執行，致電腦遭入侵並對外異常連線。

近期聯防情資彙整(cont.)

- 114年03月
  - 駭客偽冒企業之法律部門以**侵犯著作權法**為由，誘騙收件者點擊郵件內之釣魚連結並填寫表單進行申訴，以達竊取敏感資料目的。
  - 多個機關對外產生惡意程式特徵的連線，經機關調查，發現使用者經由搜尋引擎查找Line安裝軟體，**搜尋結果出現含有「line」字樣的.com網域之偽冒網站**，致使用者誤認為官方下載頁面，安裝夾帶後門程式之Line安裝檔。
- 114年04月
  - 駭客透過散播夾帶**程式資訊檔(Program Information File, PIF)之惡意程式垃圾郵件**，利用PIF隱藏副檔名之特性，誘使收件者誤認為一般文件，以提升開啟附件並連線惡意中繼站之成功率。
  - 部分機關使用防火牆設備，其**網頁管理介面存在後門連結**，該後門連結疑似為駭客利用已知重大漏洞入侵後所遺留，允許未經授權使用者透過特定網頁連結讀取設備內部檔案之系統配置、系統執行檔及設定檔等資訊。

公務、私人信箱不分的可能影響

資安成隱憂！公務信箱註冊外部網站 恐有帳密外洩風險

陳奕廷
2024年3月3日

（記者陳奕廷／綜合報導）為了要落實個資保護、防堵重要個資外洩，立法院在上個會期修法，明定要設立個資保護委員會，作為《個資法》的主管機關。去年底個資會的籌備處正式成立，將加速提出組織法規草案，力拚在114年8月前，能讓個資會正式成立。

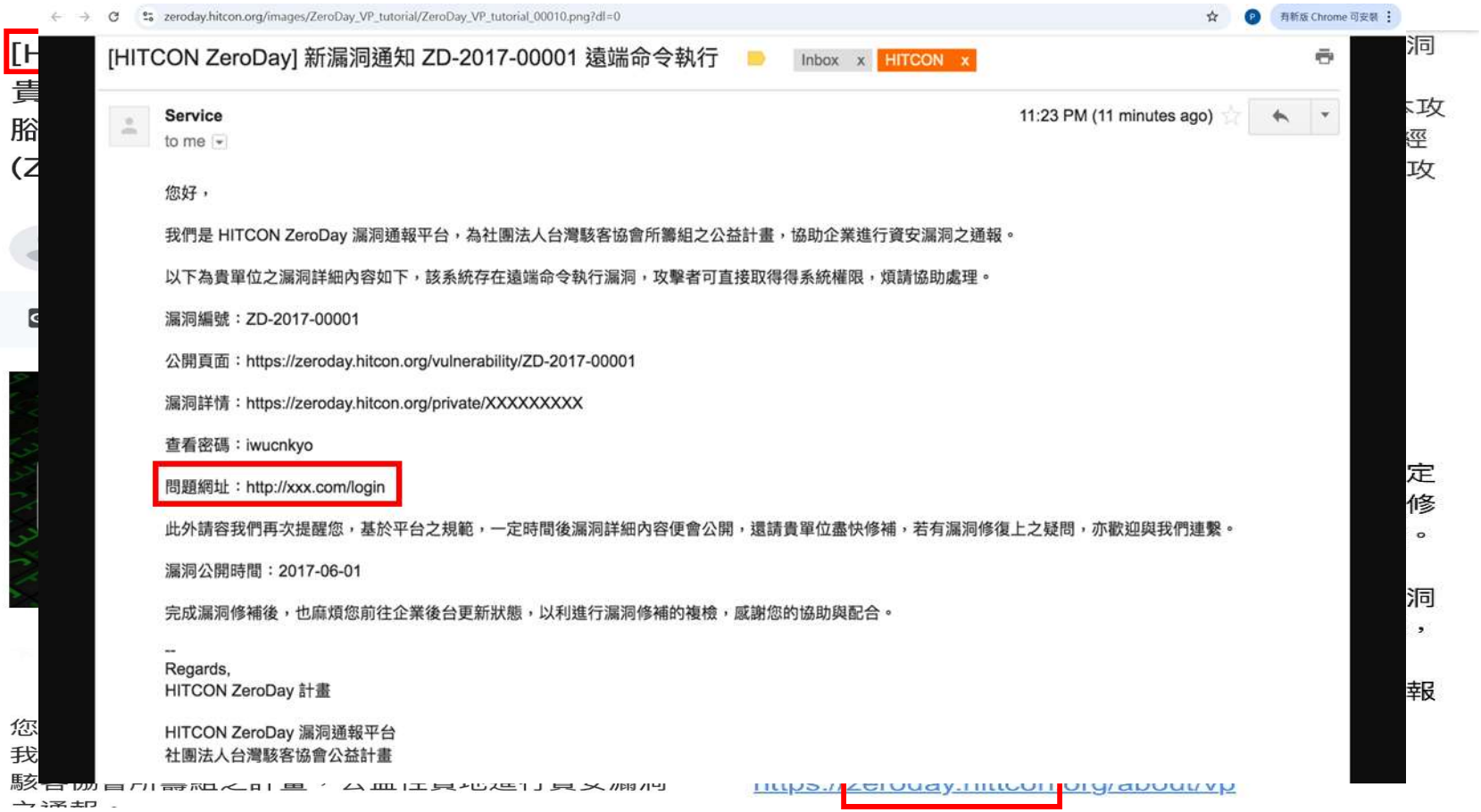
除了個資很重要以外，公司行號的資安問題也備受矚目！數位部資安署最新一期資安月報指出，呼籲公務人員不要使用公務信箱註冊在非公務外部網站，且帳號密碼也應該跟公務系統不同，避免外部網站遭駭後，可能導致帳號密碼外洩等資安風險。

資安署解釋，如果外部網站遭駭，駭客可能從公務信箱發現是公務人員，相關帳號、密碼及使用者個資等資料都將同步曝險，若個人使用在外部服務的密碼又跟公務系統相同，就可能有資安風險。使用者的電腦系統及軟體也應該定期更新及掃毒，以維護資通安全。

此外，在事前聯防監控部分，月報指出，今年1月政府機關資安聯防情資共6萬2578件，較去年12月增加1萬2997件，分析可辨識的威脅種類，第1名為資訊蒐集類（31%），主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類（23%），主要是嘗試入侵未經授權的主機；再來為資訊內容安全類（15%），大多是系統遭未經驗證存取或影響資訊機敏性。

https://tw.news.yahoo.com/

假冒漏洞通報的社交工程信件



近期校園資通安全事件案例

台灣學術網路危機處理中心

https://cert.tanet.edu.tw/

SEO中毒攻擊事件

https://portal.cert.tanet.edu.tw/docs/pdf/2025010801015757363564577204841.pdf

❑ 事件簡介

2024/11 初使用 Google 搜尋指令查詢「site:edu.tw “投資”” 當沖” 」或「site:edu.tw “鬥地主” 」，在搜尋結果頁發現許多學校網站出現大量不相關或不當連結的資訊。

2024/11/7~2024/11/26 期間共有 33 間學校受影響，其中 18 間大學、4 間高中、3 間職業學校、1 間國中、5 間小學、2 個網路中心，而且大部分學校使用 XAMPP 架站。

發文日期：中華民國113年11月15日
發文字號：臺教資通字第1132704350號
速別：普通件
密等及解密條件或保密期限：
附件：Google搜尋中出現不當文字及連結補充說明
(A09000000E_1132704350_senddoc2_Attach1.pdf)

主旨：為協助處理部分學校於Google搜尋中出現不當文字及連結，請依說明一處理，請查照並轉知所屬學校。

說明：

一、為處理旨揭問題，建請依下列說明處理：

(一)建請學校自行檢視Google搜尋網站之關鍵字，如已被攻擊者，須清除SEO中毒攻擊，可至Google console search服務申請「移除網址」以刪除Google搜尋出現之

SEO中毒攻擊事件(cont.)

https://portal.cert.tanet.edu.tw/docs/pdf/202501080101575736356457720484 1.pdf

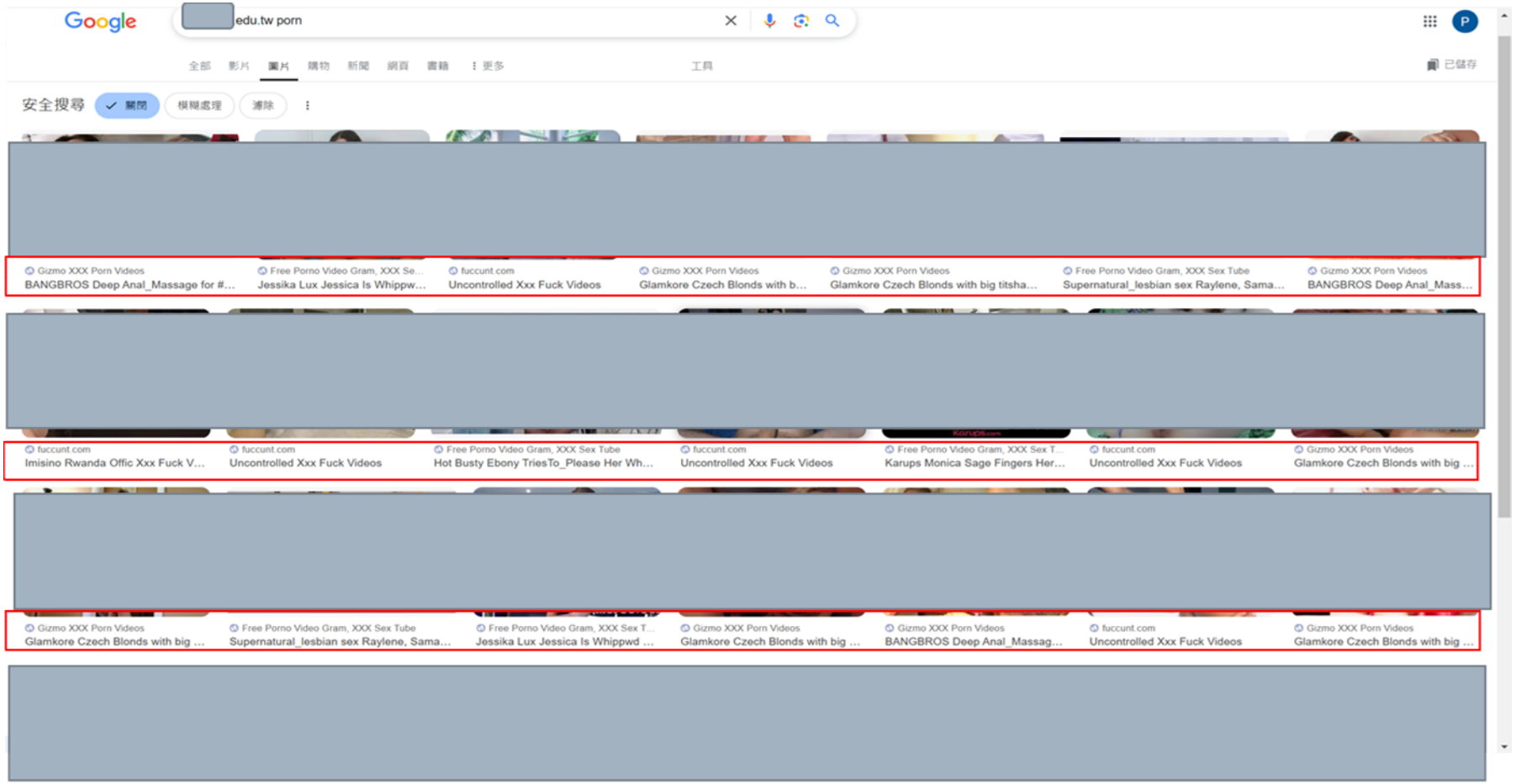
- SEO 中毒攻擊與 CVE-2024-4577 漏洞
  - SEO 中毒攻擊是指利用 google Search 的搜尋演算法特性，使用黑帽 SEO技術，讓攻擊者自我設計的惡意網站於 Google 上排名升高，導致使用者可能信任並訪問惡意網站。
  - CVE-2024-4577 漏洞是因 PHP 忽略 Windows 作業系統內部對字元編碼轉換的最佳化對應，導致未認證的攻擊者可透過特定的字元序列繞過舊有的保護；並透過參數注入等攻擊在遠端 PHP 伺服器上執行任意程式碼。導致漏洞觸發有兩種可能情形:(1)將 PHP 設置於 CGI 模式下執行(2)將 PHP 執行檔曝露於 CGI 資料夾，即使未透過 CGI 模式執行 PHP，也會曝露相關風險。

防護建議

https://portal.cert.tanet.edu.tw/docs/pdf/202501080101575736356457720484 1.pdf

- 如確認已遭到 SEO 中毒攻擊，建議至 Google Search Console 服務申請「管理帳號」與申請「移除網址」，來清除 Google 搜尋結果產生的錯誤資訊。
- 建議網站管理者設定帳戶之密碼時，加強密碼強度。
- 因為 CVE-2024-4577 漏洞影響所有安裝在 Windows 作業系統上的 PHP 版本，另因 PHP 8.0 分支、PHP 7 以及 PHP 5 官方已不再維護，建議使用這些版本的網站管理者升級到最新 PHP 官方仍有維護 之版本，或採取相應的緩解措施。
- 對於無法升級的系統，可以考慮其他暫時緩解措施，如修改 Rewrite規則以阻擋攻擊或取消 PHP CGI 的功能。
- 因 PHP CGI 是一個過時且有問題的架構，建議網站管理者評估遷移到更安全的架構（例如 Mod-PHP、FastCGI 或 PHP-FPM）的可能性。
- 網站管理者如確認網站未使用到 PHP CGI 功能，可修改 Apache Httpd 設定檔，以避免暴露弱點。

清除 Google 搜尋結果產生的錯誤資訊



不當連結資訊不限於「投資」「當沖」

- 「poker」,「gamble」,「porn」,「solt」

CVE 漏洞利用之勒索軟體攻擊事件

https://portal.cert.tanet.edu.tw/docs/pdf/20240703100756567790891359 95.pdf

- 事件簡介
  - PHP 為最常見網站使用語言之一，資料顯示全球有近八成網站使用該語言撰寫而成。資安公司戴夫寇爾研究人員在 2024/05/07 發現 PHP 存在引數注入(Argument Injection)漏洞(CVE-2024-4577)，未經身分鑑別之遠端攻擊者可透過特定字元序列繞過舊有 CVE-2012-1823 弱點修補後之保護，並透過引數注入等攻擊於遠端 PHP 伺服器上執行任意程式碼。在 2024/06/06 PHP 開發商發布新版本 8.3.8、8.2.20 與 8.1.29 來修補此露洞。在 2024/06/08 學術網路中有多所學校遭受勒索軟體攻擊，發生該漏洞利用的事件。

PHP 的 Windows 版本漏洞問題

PHP 的 Windows 版本存在漏洞 黑客可遠端執行任意程式碼及資料篡改

文: 編輯部 / 新聞中心

文章索引： IT快訊

【極危險 ⚠ 】台灣電腦網路危機處理暨協調中心 7 日公告，Windows 作業系統上的 PHP 版本存在嚴重漏洞、漏洞識別碼為(CVE-2024-4577)，遠端攻擊者可利用這些漏洞，於目標系統觸發遠端執行任意程式碼及資料篡改，PHP 官方已於 2024 年6月6日在網站上發佈修補版本，建議使用者儘速更新。

此漏洞源於 PHP 設計未注意到 Windows 作業系統字元編碼轉換的Best-Fit 特性，使得未經身分鑑別之遠端攻擊者可透過特定字元序列繞過CVE-2012-1823之保護，並透過引數注入(Argument Injection)等攻擊，於遠端PHP 伺服器上執行任意程式碼。

此漏洞影響所有安裝在 Windows 作業系統上的 PHP 版本，包括：

PHP 8.3 版本低於 8.3.8
PHP 8.2 版本低於 8.2.20
PHP 8.1 版本低於 8.1.29
另因PHP 8.0 分支、PHP 7 以及 PHP 5 官方已不再維護，建議使用這些版本的網站管理員更換成PHP官方仍有維護之版本，或採取相應的緩解措施。

若需確認網站是否受影響，管理員可以檢查 Apache HTTP Server 的設定，當網站設定在CGI 模式下執行PHP或將 PHP 執行檔暴露在外時，該伺服器將容易成為攻擊的目標。需特別注意的是，若使用 XAMPP for Windows 預設安裝配置，也會受此漏洞影響。

研究團隊指出，當 Windows 作業系統設置為繁體中文、簡體中文或日文語系時，未經授權的攻擊者可以直接在遠端伺服器上執行任意程式碼。雖然其他語系的 Windows 系統也可能存在風險，但具體影響範圍仍需使用者自行檢查並盡早更新 PHP 版本。

PHP 官方目前已發布最新版本(8.3.8、8.2.20 和 8.1.29)來修復此漏洞，強烈建議所有使用者立即升級至最新版本，以確保系統安全。對於無法升級的系統，管理員可以考慮其他暫時緩解措施，如修改Rewrite 規則以阻擋攻擊或取消 PHP CGI的功能。

此外，PHP CGI 已被認為是一種過時且易受攻擊的架構，建議使用者評估並遷移至更為安全的 Mod-PHP、FastCGI 或 PHP-FPM 等架構。

資料來源：https://https://www.hkepc.com/

預防建議

https://portal.cert.tanet.edu.tw/docs/pdf/20240703100756567790891359 95.pdf

- 由於 CVE-2024-4577 漏洞影響所有安裝在 Windows 作業系統上的PHP 版本，另因 PHP 8.0 分支、PHP 7 以及 PHP 5 官方已不再維護，建議使用這些版本的網站管理員更換成 PHP 官方仍有維護之版本，或採取相應的緩解措施。
- 對於無法升級的系統，可以考慮其他暫時緩解措施，如修改 Rewrite規則以阻擋攻擊或取消 PHP CGI 的功能。
- 由於 XAMPP 尚未針對此漏洞釋出相對應的更新安裝檔，使用者如確認自身未使用 PHP CGI 功能，可修改 Apache Httpd 設定檔，以避免暴露弱點。
- 因 PHP CGI 被公認為是一種過時且易受攻擊的架構，建議使用者評估並遷移至更為安全的 Mod-PHP、FastCGI 或 PHP-FPM 等架構。

現在官網可下載的XAMPP版本

https://www.apachefriends.org/zh_tw/download.html

XAMPP for **Windows** 8.0.30, 8.1.25 & 8.2.12

版本		校驗碼			大小
8.0.30 / PHP 8.0.30	包含什麼內容？	md5	sha1	下載 (64 bit)	144 Mb
8.1.25 / PHP 8.1.25	包含什麼內容？	md5	sha1	下載 (64 bit)	148 Mb
8.2.12 / PHP 8.2.12	包含什麼內容？	md5	sha1	下載 (64 bit)	149 Mb

需求　更多下載 »

Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms here.

XAMPP for **Linux** 8.0.30, 8.1.25 & 8.2.12

版本		校驗碼			大小
8.0.30 / PHP 8.0.30	包含什麼內容？	md5	sha1	下載 (64 bit)	151 Mb
8.1.25 / PHP 8.1.25	包含什麼內容？	md5	sha1	下載 (64 bit)	153 Mb
8.2.12 / PHP 8.2.12	包含什麼內容？	md5	sha1	下載 (64 bit)	151 Mb

需求　更多下載 »

XAMPP for **OS X** 8.0.28, 8.1.17 & 8.2.4

版本		校驗碼			大小
8.0.28 / PHP 8.0.28	包含什麼內容？	md5	sha1	下載 (64 bit)	150 Mb
8.1.17 / PHP 8.1.17	包含什麼內容？	md5	sha1	下載 (64 bit)	151 Mb
8.2.4 / PHP 8.2.4	包含什麼內容？	md5	sha1	下載 (64 bit)	150 Mb

需求　更多下載 »

A Native installer installs MariaDB, PHP, Perl, etc. directly onto your macOS system. It supports intel (x64) or Apple M1 (arm64) CPUs.

此漏洞影響所有安裝在 Windows 作業系統上的 PHP 版本，包括：

PHP 8.3 版本低於 8.3.8
PHP 8.2 版本低於 8.2.20
PHP 8.1 版本低於 8.1.29

另因PHP 8.0 分支、PHP 7 以及 PHP 5 官方已不再維護，建議使用成PHP官方仍有維護之版本，或採取相應的緩解措施。

IoT 設備資安防護指南

https://portal.cert.tanet.edu.tw/docs/pdf/2022110404114040719862739608309.pdf

- 這是個萬物聯網的時代

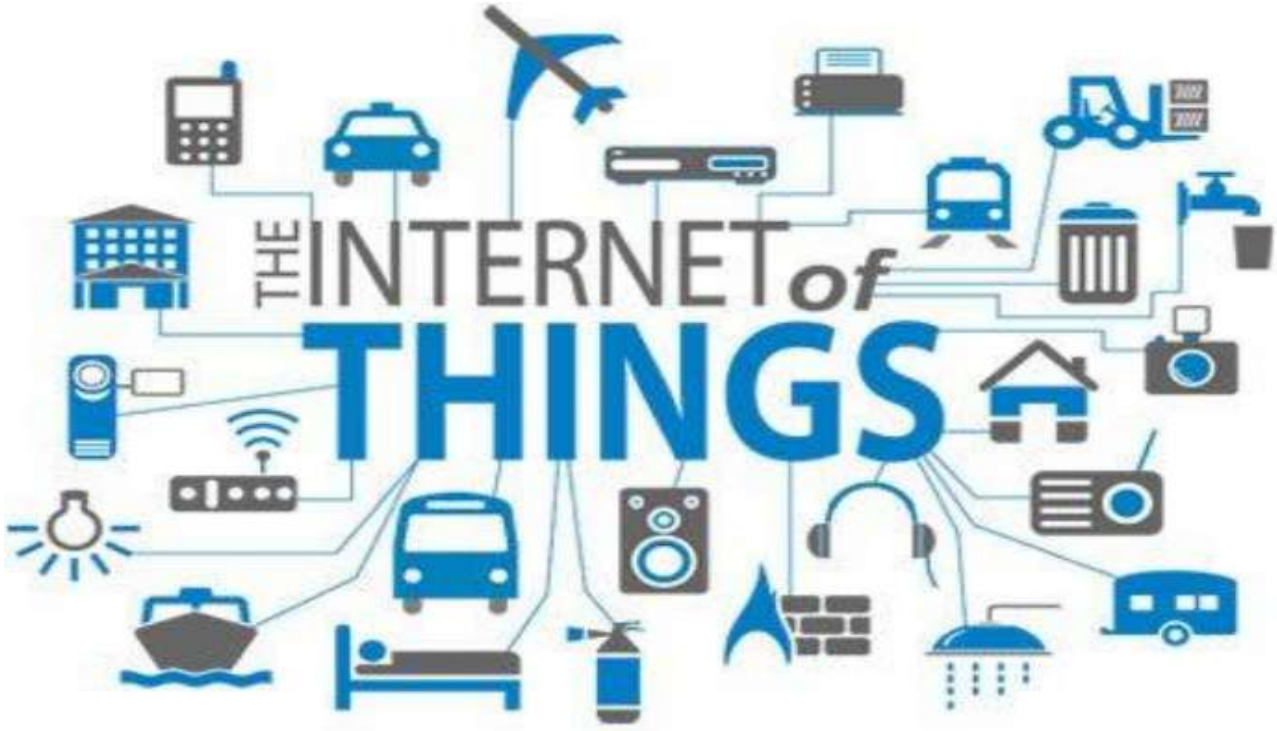


圖 1. IoT 概念圖(圖片來源：http://www.business2community.com/)

資通安全網路月報(110年11月)

- 近期駭客以詢價為主旨，寄送**含有惡意程式下載連結之郵件攻擊台灣政府機關**，郵件內含透過通話軟體平台作為惡意檔案下載站之連結，企圖欺騙收件人下載遠端存取木馬程式。該攻擊手法有別以往利用電子郵件附檔方式，而是透過合法之通話軟體平台企圖躲避掃描偵測，並誘騙使用者將偽裝成一般文件檔案之惡意程式下載至電腦中執行
- 近期偵測發現駭客利用**網路儲存設備**之漏洞入侵並植入挖礦程式，占本月通報26.37%。

OWASP IOT Top 10

編號	項目
I1	弱密碼、可猜測密碼或裝置預設密碼(Weak, Guessable, or Hardcoded Passwords)
I2	不安全的網路服務(Insecure Network Services)
I3	不安全的環境設定介面(Insecure Ecosystem Interfaces)
I4	缺乏安全的更新機制(Lack of Secure Update Mechanism)
I5	使用不安全或已遭棄用的組件(Use of Insecure or Outdated)
I6	不充分的隱私保護(Insufficient Privacy Protection)
I7	不安全的資料傳輸和儲存(Insecure Data Transfer and Storage)
I8	缺乏設備管理(Lack of Device Management)
I9	不安全的預設設定(Insecure Default Settings)
I10	缺乏實體安全強化(Lack of Physical Hardening)

校園常見物聯網設備及其可能面臨的風險

https://portal.cert.tanet.edu.tw/docs/pdf/202211040411404071986273960830 9.pdf

- 印表機(事務印表機)
  - 現今的印表機及辦公室使用的事務印表機大部份都可以連網且有提 供網頁服務供設定使用，於 2017 年 2 月因印表機使用之 Port 9100 遭 利用，列印出勒索訊息之事件，及部份印表機提供網頁服務無管控設定，遭更換網頁等，皆是目前印表機常見的風險。

校園常見物聯網設備及其可能面臨的風險(cont.)

https://portal.cert.tanet.edu.tw/docs/pdf/202211040411404071986273960830 9.pdf

- 網路攝影機(監控系統)
  - 目前眾多網路攝影機可能使用公板及共用系統進行建構，於 2016 年 9 月時因攝影機遭入侵造之 Mirai Botnet 形成，之後造成全球性 DDoS 攻擊盛行。其原因在於網路攝影機使用之後端連線服務預設開啟，且 使用預設帳密，更因系統限制無法修改預設帳號密碼，僅能透過韌體更新方式關閉後端連線服務。另外，因網路攝影機本身即是提供監控 服務，且多數皆有提供網頁服務。在未修正預設帳密的狀態下，可藉由網頁服務來取得監控端影像，造成環境資訊外洩的可能性。

輕易可見的預設帳密資訊

lanthing.com/2018/04/05/監控主機-預設密碼/

監控主機 預設密碼

2018-04-05 aher625 0 支援與下載,

可取 iwatch DVR 2 帳號：admin 密碼：123456

socatch

大華 gDMSS Lite 帳號： admin 密碼 ：admin

gDMSS Plus（收費版本）

大華 搖頭機 Easy4ip 帳號： admin 密碼 ：admin

昇銳 super Live pro 帳號：:admin 密碼：123456

hisharp 帳號：:admin 密碼：123456

昇銳n9000介面

super Live plus 帳號：:admin 密碼：123456

遠安電通 viewcam 帳號：:admin 密碼： 空白

深微 tapcms 帳號：aa 密碼：11

海康 ivms-4500 帳號：:admin 密碼：888888

新版本 帳號：:admin 密碼：hk888888

慧友TUTIS Remote 帳號：:admin 密碼：00000000

利凌 ahd NetViewer 帳號：:admin 密碼：1111

雄邁 vMEyeSuper 帳號：:admin 密碼： 空白

雄邁 vMEyeCloud 帳號：:admin 密碼： 空白

馥鴻AHD: VacronViewer 帳號：:admin 密碼： 空白

馥鴻4-8路Castillo Playe 帳號：admin 密碼 ：admin

馥鴻16路TMEye 帳號：admin 密碼 ：admin

禾蒼VS Viewer Pro II 帳號：admin 密碼 ：admin

漢邦高科RealViewPro 帳號：:admin 密碼：888888

群洲電子CDOUBLES

杭特Iprosecu A.MV2 帳號：admin 密碼 ：admin

環名 Aquila 帳號：:admin 密碼：123456

陞泰 Eagle Eyes 帳號： admin 密碼 ：admin

CP Plus gCMOB 帳號： admin 密碼 ：admin

校園常見物聯網設備及其可能面臨的風險(cont.)

https://portal.cert.tanet.edu.tw/docs/pdf/2022110404114040719862739608309.pdf

- 網路附加儲存設備(Network Attached Storage, NAS)
  - 因為資料備份的需求，有越來越多的學校添購 NAS 設備以因應其需求。而當 NAS 設備安裝上線時，針對預設帳號密碼未進行相對應的處 理，因此可能遭有心人士取得內部資料。同時因 NAS 系統本身可能存在相關漏洞，因此亦需定時檢查更新，以修補相關漏洞。


新聞

研究人員揭露威聯通NAS作業系統漏洞，並指出15個漏洞僅有4個完成修補

資安業者watchTowr去年底開始向NAS廠商威聯通（QNAP）通報資安漏洞，數量多達15個，但該公司僅針對其中一小部分做出修補，他們在上週揭露此事。對此，威聯通發布公告說明他們處理的情形

https://www.ithome.com.tw/news/163034

文/ 周峻佑 | 2024-05-22 發表

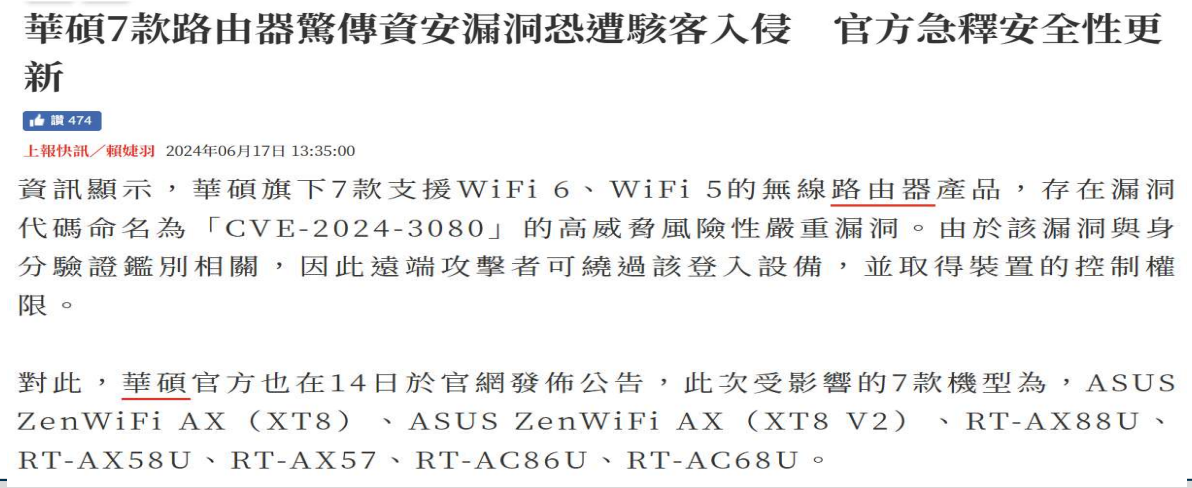
NAS設備使用原則

- 帳號管理與清查
- 密碼原則建立與執行
- 依存放檔案的性質或重要程度，建立必要的存取限制
- 宜盡量避免開放校外存取
- 若有建立自動化備份機制，應定期檢視資源和運轉情形
- 定期執行元件更新，並檢視存取紀錄

校園常見物聯網設備及其可能面臨的風險(cont.)

https://portal.cert.tanet.edu.tw/docs/pdf/2022110404114040719862739608309.pdf

- 無線網路分享器(Wireless AP)
  - 由於網路使用頻繁，校園內設置無線網路分享器也日漸增多。這些設 備之 Web 管理平台預設帳號密碼若未變更，則可能讓設備變成駭客對 外攻擊之 VPN 中繼站。此外，分享器可能存在漏洞，需定時檢查更 新，以修補相關漏洞。



華碩7款路由器驚傳資安漏洞恐遭駭客入侵　官方急釋安全性更新

讚 474

上報快訊／賴婕羽　2024年06月17日 13:35:00

資訊顯示，華碩旗下7款支援WiFi 6、WiFi 5的無線路由器產品，存在漏洞代碼命名為「CVE-2024-3080」的高威脅風險性嚴重漏洞。由於該漏洞與身分驗證鑑別相關，因此遠端攻擊者可繞過該登入設備，並取得裝置的控制權限。

對此，華碩官方也在14日於官網發佈公告，此次受影響的7款機型為，ASUS ZenWiFi AX（XT8）、ASUS ZenWiFi AX（XT8 V2）、RT-AX88U、RT-AX58U、RT-AX57、RT-AC86U、RT-AC68U。

https://www.upmedia.mg/news_info.php?Type=24&SerialNo=204116

校園常見物聯網設備及其可能面臨的風險(cont.)

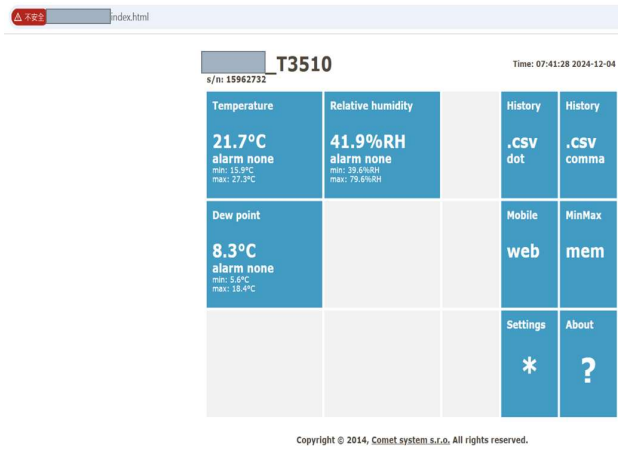
https://portal.cert.tanet.edu.tw/docs/pdf/2022110404114040719862739608309.pdf

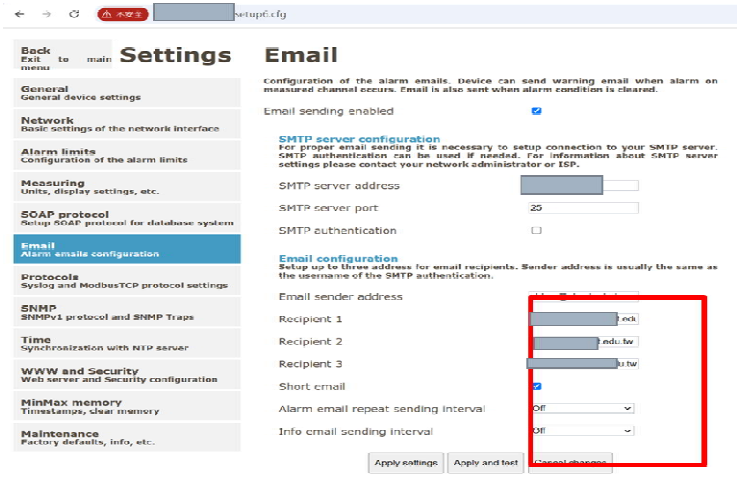
- 數位電子看板(Digital Signage)
  - 電子看板是在學校內常會看到的公告用具，管理者可透過 Web 管理平 台將所要公告的內容放入，再讓電子看板進行輪播。由於其連接網路， 又設置於大眾看得到之位置，若讓有心人士利用，則可能遭受內容置 換攻擊。因此，電子看板的資安防護措施是很重要的，尤其在加強 Web 管理平台之密碼強度方面。

校園常見物聯網設備及其可能面臨的風險(cont.)

https://portal.cert.tanet.edu.tw/docs/pdf/2022110404114040719862739608309.pdf

- 能源管理系統(Energy Management System, EMS)
  - 有些學校使用校園能源管理系統來管理與監控各建築物的空調與供電的使用量，也透過該系統有效掌握各建築物之營運成本。然而此類 型系統因使用 Web 管理平台提供管理者檢視資訊，若預設密碼未變更 或使用弱密碼，則將造成駭客登入能源管理系統進行操作或竊取資訊。

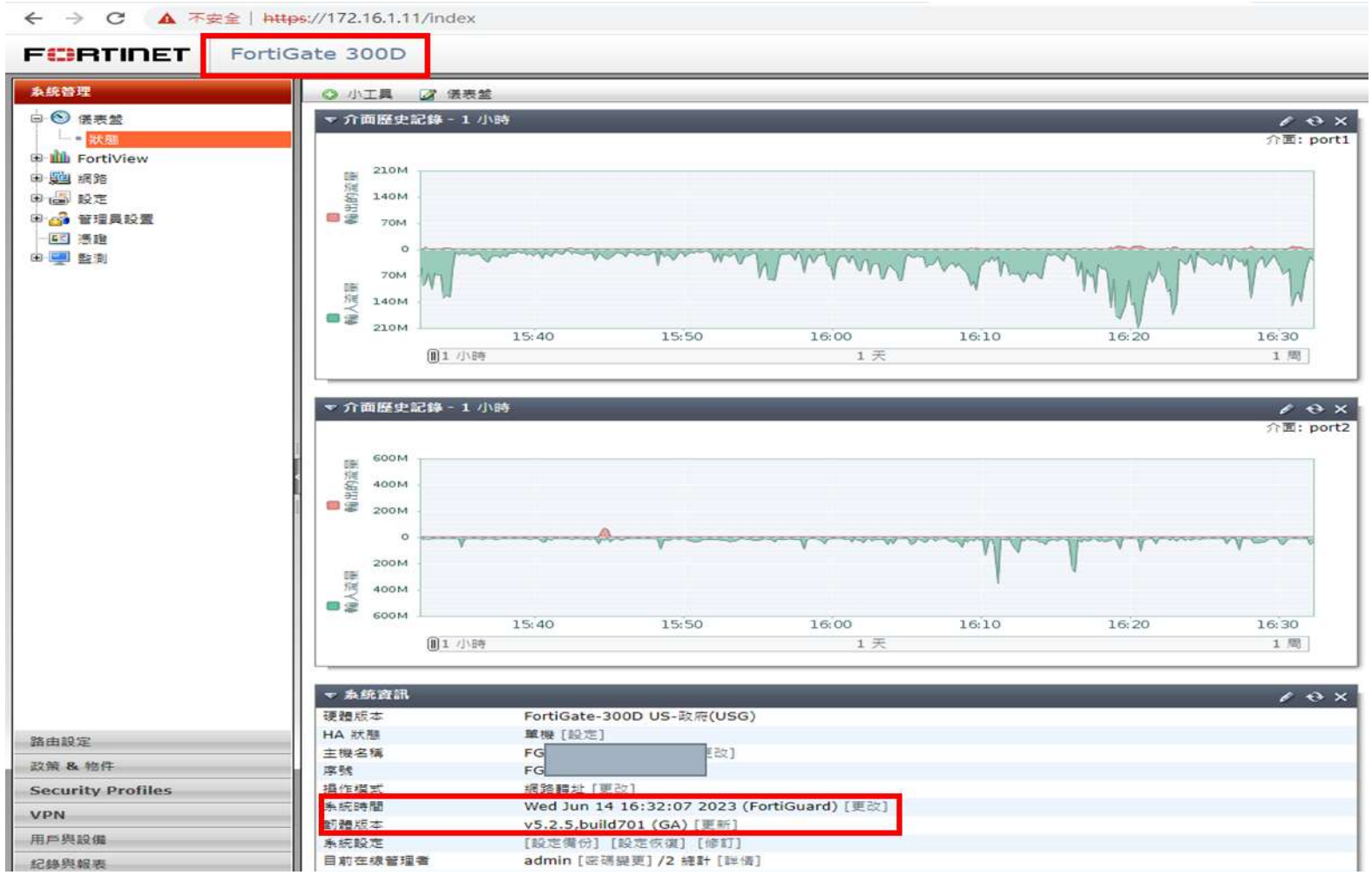




校園物聯網設備管控

- 設備清查
  - 設備盤點
  - 大陸廠牌設備限制與汰除
- 網路限制與管控
  - 關閉不必要的服務埠
  - 限制與防護網路存取
- 存取管控
  - 變更預設密碼與帳號(若可行的話)
  - 落實密碼原則(複雜度、長度、變更週期等)
- 漏洞修補與系統更新

一張不起眼的校園防火牆截圖



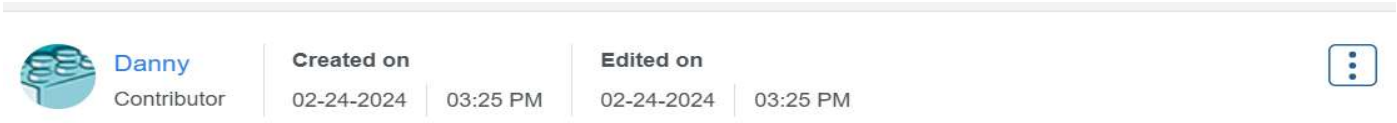
Fortinet End of Service Life

https://www.topgun-tech.com/end-of-service-life/fortinet/

FortiGate-400D-USG	5/29/2023
FortiWiFi-60D-POE	6/24/2023
FortiGate-200D-POE	7/15/2023
FortiGate-200D-POE-USG	7/15/2023
FortiWiFi-92D	7/15/2023
FortiGate-100D	7/26/2023
FortiGate-60D	9/23/2023
FortiGate-60D-LENC	9/27/2023
FortiGate-300D	10/11/2023
FortiGate-300D-LENC	10/11/2023
FortiGate-90D	10/14/2023
FortiGate-90D-LENC	10/14/2023
FortiWiFi-90D	10/14/2023
FortiWiFi-90D-Gen2-J	10/14/2023
FortiWiFi-90D-I	10/14/2023
FortiWiFi-90D-K	10/14/2023
FortiWiFi-60D-3G4G-VZW	10/14/2023
FortiWiFi-60D03G4G-VZW-USG	10/14/2023
FortiGate-60D-3G4G-VZW	10/14/2023

FortiOS - End of Life Overview

https://community.fortinet.com/t5/Support-Forum/FortiOS-End-of-Life-Overview/m-p/301142



Danny
Contributor

Created on
02-24-2024 | 03:25 PM

Edited on
02-24-2024 | 03:25 PM

FortiOS - End of Life Overview

Does Fortinet provide a general overview of EOL dates for all FortiOS releases like this?

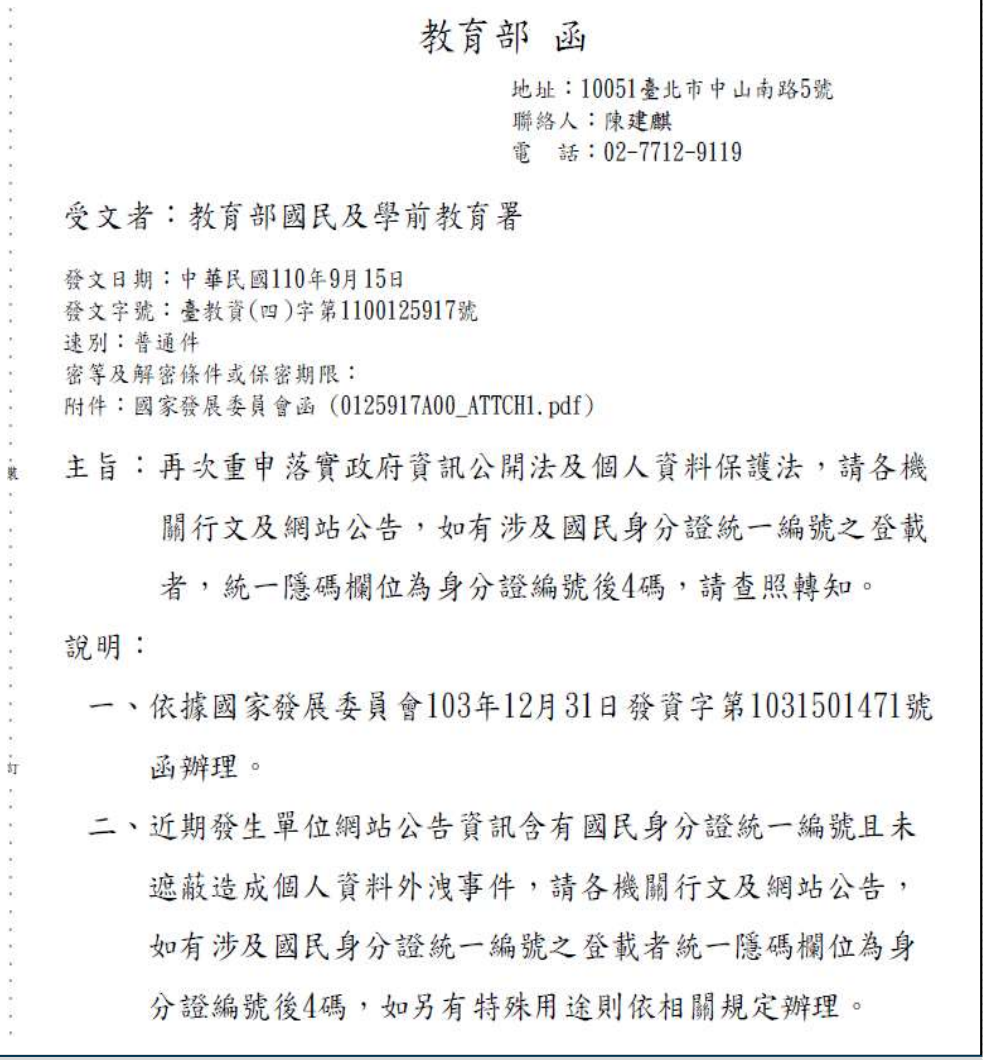
Release	Released	End of Engineering Support	End of Support
7.4	9 months ago (11 May 2023)	Ends in 2 years (11 May 2026)	Ends in 3 years and 8 months (11 Nov 2027)
7.2	1 year and 10 months ago (31 Mar 2022)	Ends in 1 year (31 Mar 2025)	Ends in 2 years and 7 months (30 Sep 2026)
7.0	2 years and 11 months ago (30 Mar 2021)	Ends in 1 month and 6 days (30 Mar 2024)	Ends in 1 year and 7 months (30 Sep 2025)
6.4	3 years and 10 months ago (31 Mar 2020)	Ended 10 months ago (31 Mar 2023)	Ends in 7 months (30 Sep 2024)
6.2	4 years and 11 months ago (28 Mar 2019)	Ended 1 year and 11 months ago (28 Mar 2022)	Ended 4 months and 4 weeks ago (28 Sep 2023)
6.0	5 years and 11 months ago (29 Mar 2018)	Ended 2 years and 11 months ago (29 Mar 2021)	Ended 1 year and 4 months ago (29 Sep 2022)

5.x???

常見校園個資事件

個資揭露建議事項

- 個資當用則用，不必因噎廢食，但仍應考量：
  - 是否屬必要揭露之資訊
  - 是否對當事人可能造成負面影響或困擾
  - 是否為其他服務/系統之可用資訊
  - 與其他揭露資訊組合是否成為可識別當事人個資(間接識別)
  - 是否有揭露的期效
  - 除網頁內容、檔案之移除外，仍須確認Google Cache



教育部 函

地址：10051臺北市中山南路5號
聯絡人：陳建麒
電　話：02-7712-9119

受文者：教育部國民及學前教育署

發文日期：中華民國110年9月15日
發文字號：臺教資(四)字第1100125917號
速別：普通件
密等及解密條件或保密期限：
附件：國家發展委員會函（0125917A00_ATTCH1.pdf）

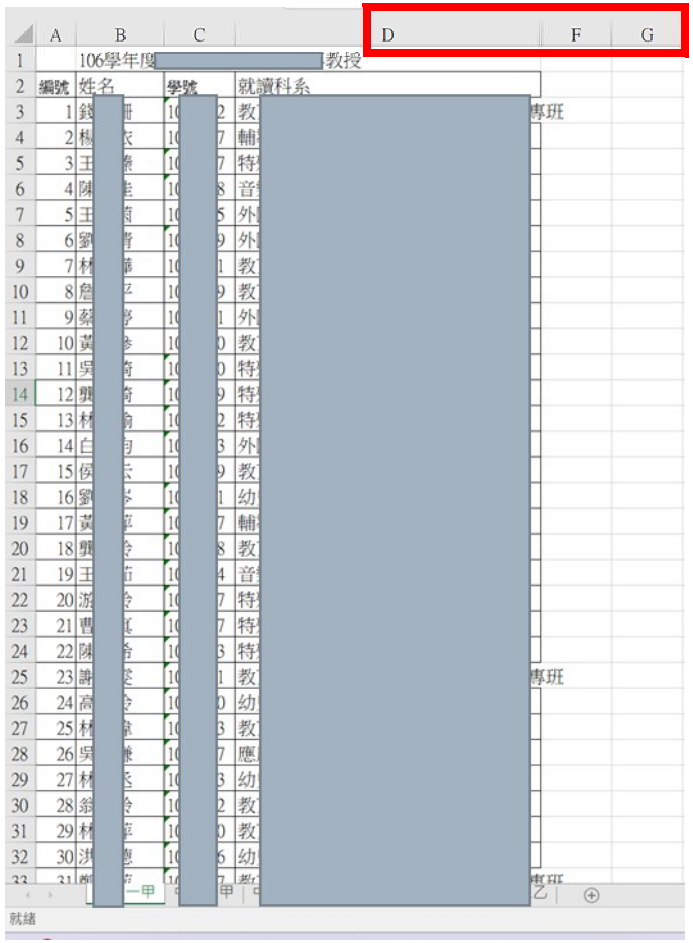
主旨：再次重申落實政府資訊公開法及個人資料保護法，請各機關行文及網站公告，如有涉及國民身分證統一編號之登載者，統一隱碼欄位為身分證編號後4碼，請查照轉知。

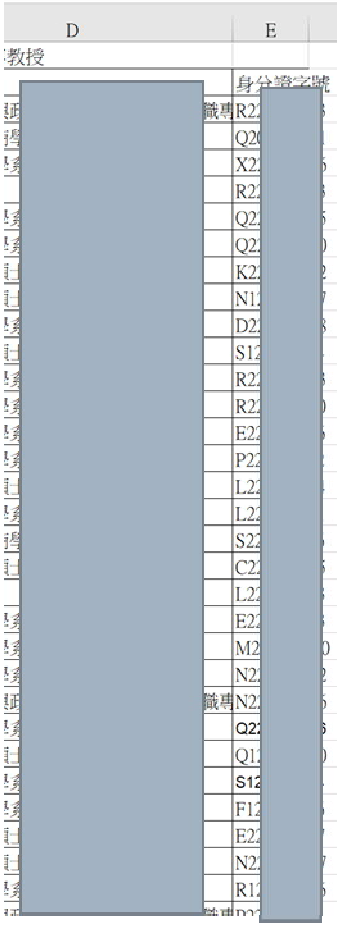
說明：

一、依據國家發展委員會103年12月31日發資字第1031501471號函辦理。

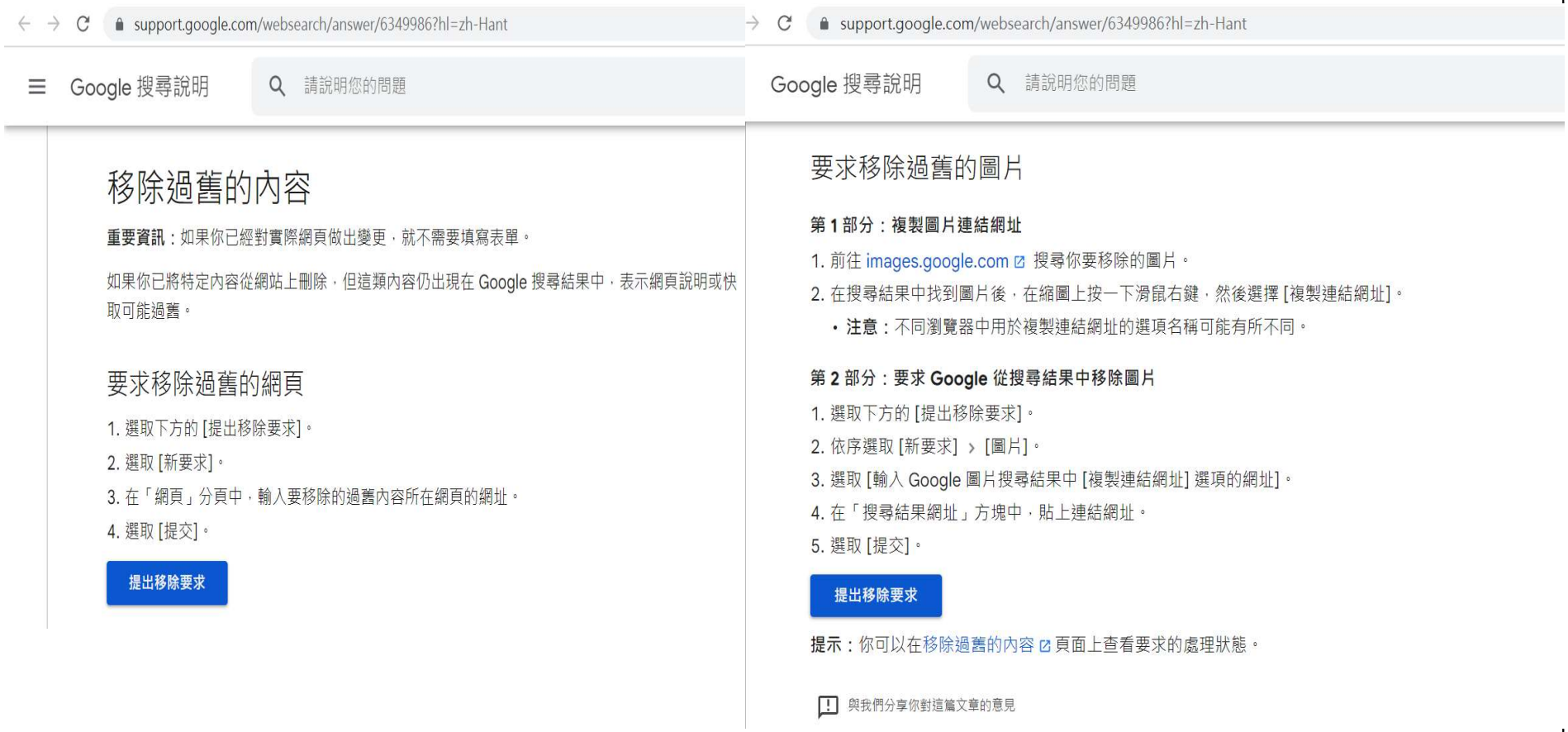
二、近期發生單位網站公告資訊含有國民身分證統一編號且未遮蔽造成個人資料外洩事件，請各機關行文及網站公告，如有涉及國民身分證統一編號之登載者統一隱碼欄位為身分證編號後4碼，如另有特殊用途則依相關規定辦理。

有一種看不到是你以為別人看不到





向Google申請移除Cache紀錄



看似安全的遮罩檔案

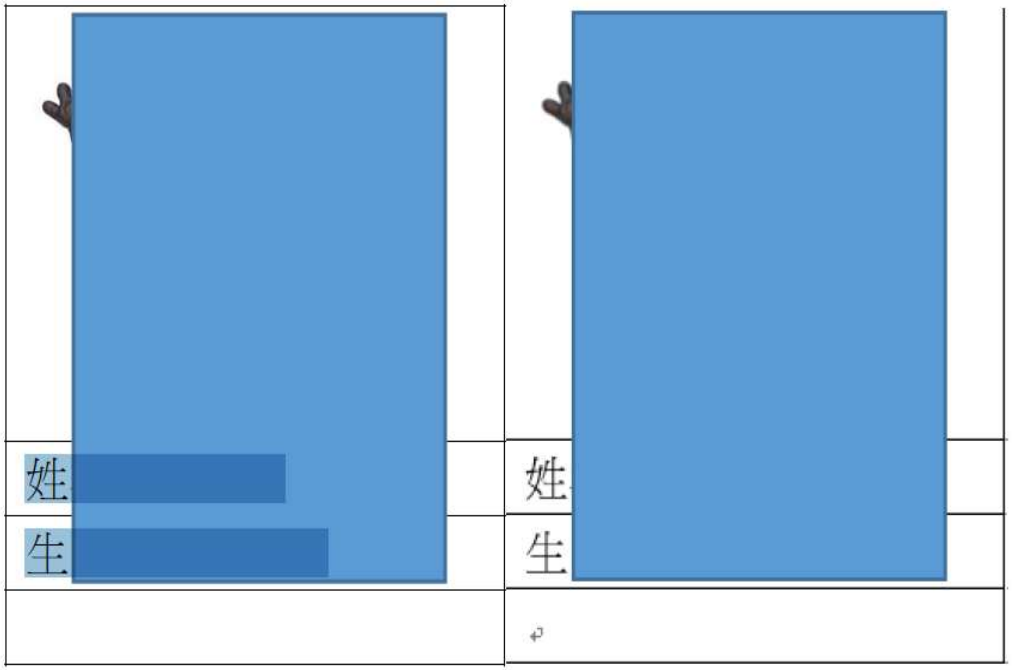
烘焙業者須具備文件

具有商業登記之前店後廠小型烘焙業

> 技術士證(持證比例30%)

PDF檔案遮罩動作需確實

- 先用圖片編輯軟體處理後再貼至文書編輯軟體中
- PDF檔案保全設定**(不全然有效)**
  - 檔案→內容→保全→保全方式→密碼保全→權限→限制編輯和列印文件→變更權限密碼
- **盡量避免使用含敏感個資的真實資料**



臺教資(四)字第1100122001號

(110年9月8日)

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。」

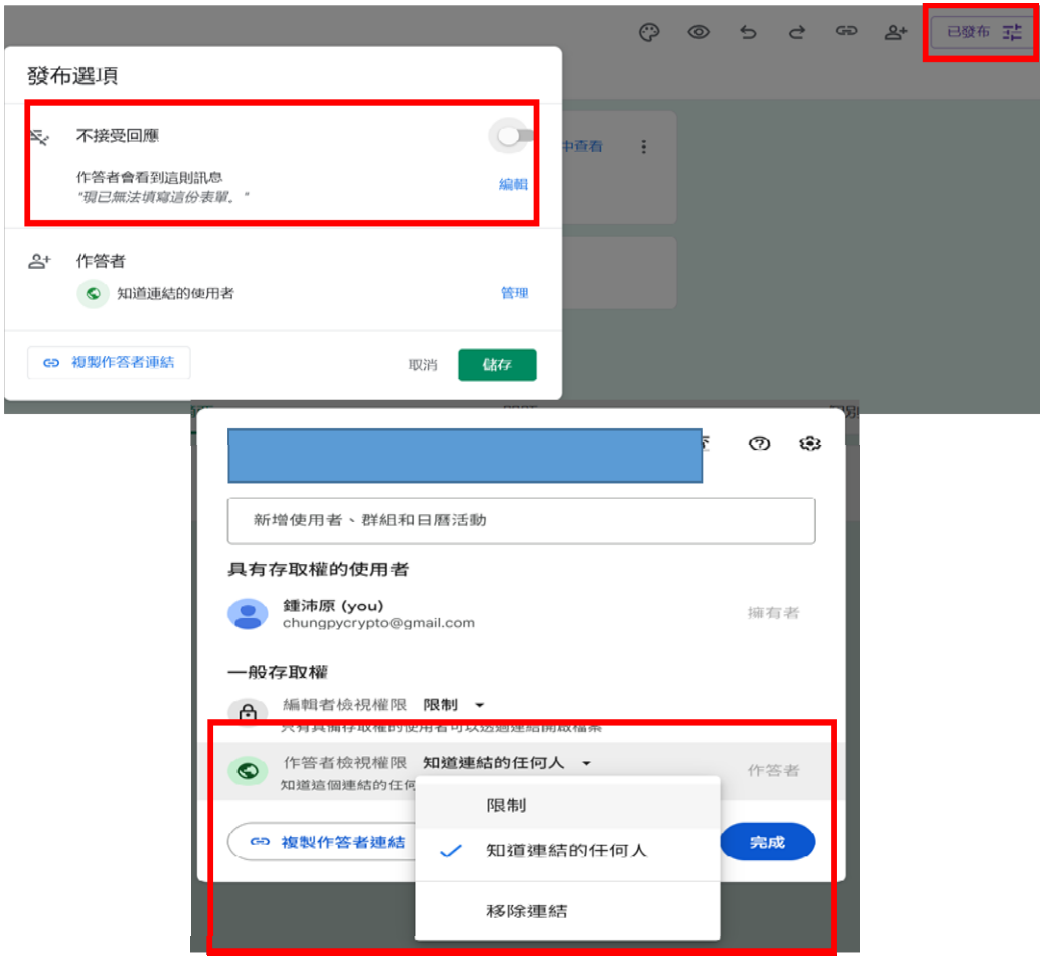
(二)個人資料保護法第41條第1項「違反個人資料保護法有關特種資料的蒐集、處理或利用規定，足生損害於他人者，處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金。」

線上表單的評估原則

- 資料是否有**必要/適合**透過線上表單蒐集？
- 表單的使用期限？
- 表單的編輯/讀取權限的分享？
- 含個人資料表單資料的刪除時機？

權限設定


問題
回覆 17
設定
簡報
管理表單和回覆的顯示方式
表單呈現方式
顯示進度列
隨機決定問題順序
提交表單後
確認訊息
我們已經收到你回覆的表單
編輯
顯示連結以傳送更多回覆
查看結果摘要
與作答者分享結果摘要。重要詳細資訊
限制:
停用所有作答者的自動儲存功能


已發布
發布選項
不接受回應
作答者會看到這則訊息
"現已無法填寫這份表單。"
編輯
作答者
知道連結的使用者
管理
複製作答者連結
取消
儲存
新增使用者、群組和日曆活動
具有存取權的使用者
鍾沛原 (you)
chungpycrypto@gmail.com
擁有者
一般存取權
編輯者檢視權限 限制
作答者檢視權限 知道連結的任何人
作答者
限制
知道連結的任何人
移除連結
複製作答者連結
完成

權限設定務必落實


問題
回覆 24
設定
「2024 」報名表
您好:
這是國立 教授主持的 科技部計畫
歡迎您報名擔任研究參與者!
以下為此項研究實驗的相關資訊:
【研究內容】包含虛擬教室體驗、問卷及接受訪談
(所有問卷資料、個人隱私及權益將嚴格保密)
【研究參與者條件】
為下列二所學校中任一所之學生
國立 大學 / 國立 大學 / 國立 大學 / 大學
並符合以下條件之一:
1. 有修習教育學程(中學普通教師資格)的大三到大五師資生。
2. 「特殊教育學系」大三到大五的學生。
且之前未參加過 教授團隊舉辦之虛擬教室VR研究實驗
【實驗時間】
【實驗地點】
【參與報酬】7-11禮券 300 元
如有特殊需求可於備註填寫,
請您填寫以下報名表,我們將會在收到報名表後與您聯繫
如有任何問題,可來信至以下聯絡人進行詢問!
聯絡人: 小姐
聯絡信箱: @gmail.com
一、您的姓名 *
簡答文字
將編輯者新增至「「2024 研究」報名表」
新增使用者、群組和日曆活動
具有存取權的使用者
mail.com
擁有者
gmail.com
編輯者
一般存取權
知道連結的任何人
任何知道這個連結的網際網路使用者都能編輯
編輯者
編輯者可以查看及刪除表單回應
複製作答者連結
完成

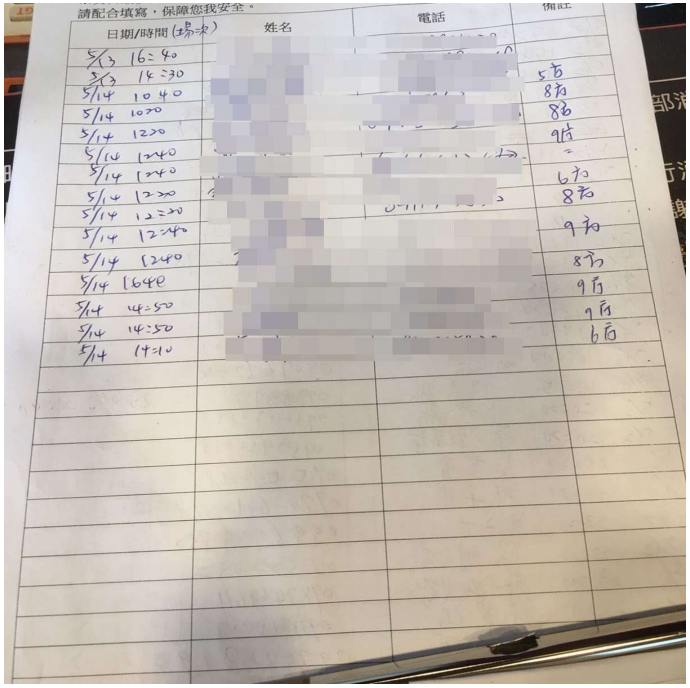
你知道比Google表單更可怕的是甚麼嗎?

利用Google drive蒐集個資的適切性？!

「COVID-19(武漢肺炎)」防疫新生活運動：實聯制措施指引

修訂日期：2020/05/29

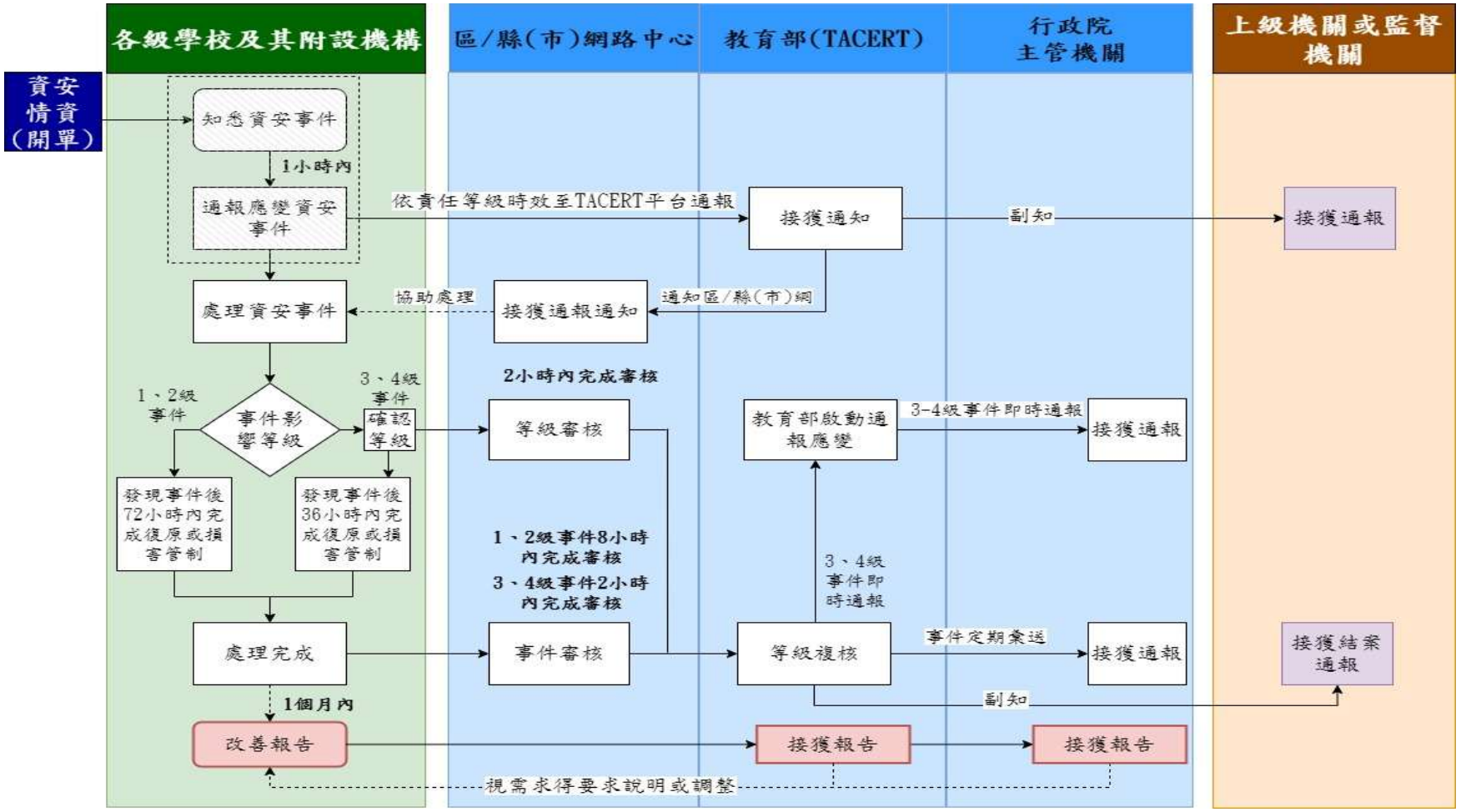
三、機關為蒐集、處理及利用個人資料，得以紙本或電子方式為之，且皆應善盡資料安全維護義務，採行適當之技術上及組織上安全措施，並指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。例如以紙本供當事人填具個人資料時，應以遮蔽或其他適當方式保護填寫者之個人資料，避免後填寫者得閱覽先填寫者之個人資料。



雲端服務使用安全

- 不過度蒐集個資
- 避免可能的個資外洩/揭露(例如可以看到其他上傳者的個資)
- 最小權限原則及最小授權存取
- 掌握功能設定並反覆確認
- 作業期間過後應予關閉或移除紀錄
- **不是只有注意Google表單就夠了!!**

臺灣學術網路各級學校
資通安全通報應變作業程序



資通安全事件等級-4級事件

- 符合下列任一情形者，屬4級事件：
  - 一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。
  - 一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。
  - 涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

資通安全事件等級-3級事件

- 符合下列任一情形者，屬3級事件：
  - 未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。
  - 未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。
  - 未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

魔鬼藏在細節中

- 資通安全事件通報及應變辦法總說明
  - 所定核心業務，依資通安全管理法施行細則第七條第一項之規定認定；所定核心資通系統，依該細則第七條第二項之規定認定，併予敘明。
  - 所稱一般公務機密，參考行政院訂定之文書處理手冊第五十一點規定，係指公務機關持有或保管之資訊，除國家機密外，依法令或契約有保密義務者。
  - 所稱敏感資訊，指包含**個人資料**等**非一般公務機密或國家機密**之資訊，**如遭洩漏可能造成機關本身或他人之損害或困擾**，而具保護價值之資訊。
  - 所稱國家機密，依國家機密保護法第二條規定，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依該法核定機密等級者。

結論

不斷增長的帳密資料庫

駭客公布近百億組密碼外洩資料集RockYou2024，疑為3年前流出資料持續維護、更新而成

資安新聞網站Cybernews揭露一批筆數接近百億的資料外洩事故「RockYou2024」，但特別的是，這些資料是以3年前的「RockYou2021」為基礎，不斷加入新的外洩資料彙整而成

文/ 周峻佑 | 2024-07-10 發表

讚 7 分享

Presented by iThome

Cybernews將這批資料與自己的外洩密碼檢查工具進行比對，確認當中含有先前與最新資料外洩事故所流出的密碼。值得留意的是，研究人員認為，這批資料並非突然出現，源自3年前他們發現的RockYou2021外洩資料庫延伸，當時約有84億明文密碼資料曝光。

換言之，維護這批資料的駭客，3年後的現在，總共新增15億組資料，單是這些新內容，大約占RockYou2024的15%。而這是在研究人員1月揭露高達260億筆資料的大型外洩資料庫「資料外洩之母（Mother of all Breaches，MOAB）」之後，另一起今年發現的大規模資料外洩事故。

https://www.ithome.com.tw/news/163863

不要以為新聞事件不會發生在自己身上

盜用500名高鐵會員TGo點數 2嫌裁定羈押禁見

2024-10-25 18:15 聯合報／記者王聖駿／台北即時報導

＋檢察官

分享 1　分享

男子鄭宇軒盜用500名高鐵會員TGo點數，今年9月被捕，台北地檢署檢察官郭盈君追查發現屬集團式犯罪，鄭與共犯游哲銘聯手盜領點數，並侵入國泰「小樹點」兌換網站盜用會員點數，再利用「車手」前往兌換高價3C商品，不法獲利數十萬元。

檢調人員昨天前往鄭、游等被告住處共12個地點搜索，同步約談8人到案，昨天深夜將犯罪嫌疑人移送複訊，檢察官漏夜偵訊後，認游涉犯妨害電腦使用罪，鄭涉犯詐欺罪，向法院聲請羈押禁見2人，台北地院審理，今天裁准。

https://udn.com/news/story/7321/8316506

結論

- 推陳出新的社交工程手法，挑戰個人的資安素養。
- 新科技、新應用可能導致新的資安/個資風險。
- 資安/個資保護是一條漫長且持續的道路。


QUESTIONS
ANSWERS