資通安全宣導教育訓練課程

漢昕科技股份有限公司BCCS

資訊安全概念

- 資訊安全是保護資料及其相關系統免於未經授權的訪問、損毀、變更、洩漏、中斷、阻斷或破壞的過程和措施。
- 確保資訊的機密性、完整性及可用性，並遵循相關法規之規範，以提供業務持續運作環境，使其免於遭受內、外部的蓄意或意外之威脅。

資訊安全概念

機密性：確保只有經過授權才可以使用機敏資訊，防止資訊洩漏。

完整性：確保資訊在傳輸或儲存過程中，不受意外或故意的損毀、變更或竄改，保持資料的正確性和完整性。

可用性：確保資訊和相關資源在需要時，可被授權用戶使用，防止因系統故障、攻擊或其他因素而導致資訊不可用。

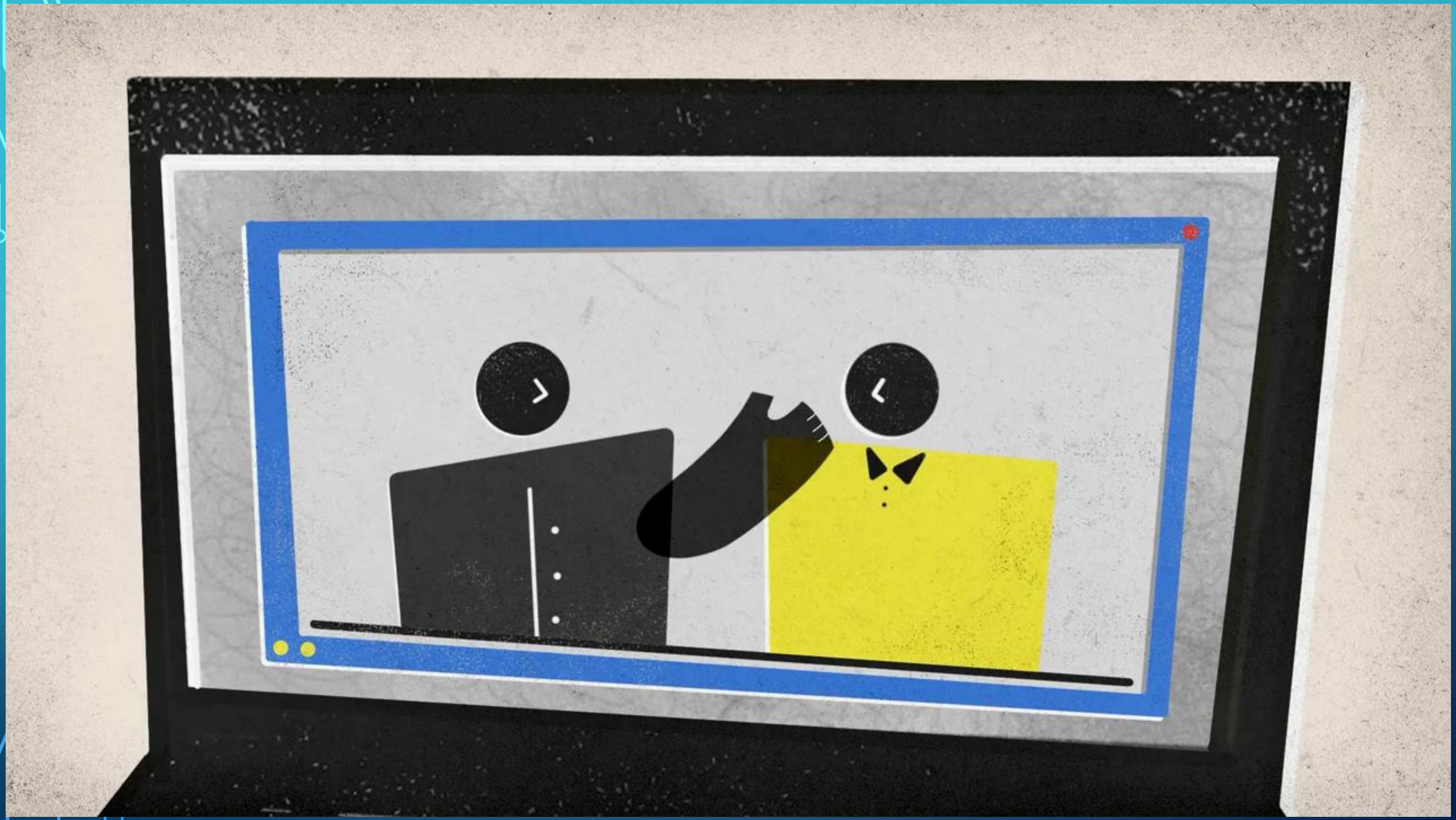
教育訓練的目的

- 資訊安全教育訓練的目的是在提供相關所需的知識與技能，讓大家能夠識別和應對資訊安全威脅，保護個人和單位的資訊資產。
- 協助單位建立資訊安全文化，有助於減少資訊安全事件的發生，維護單位內數位環境的穩定和安全性。

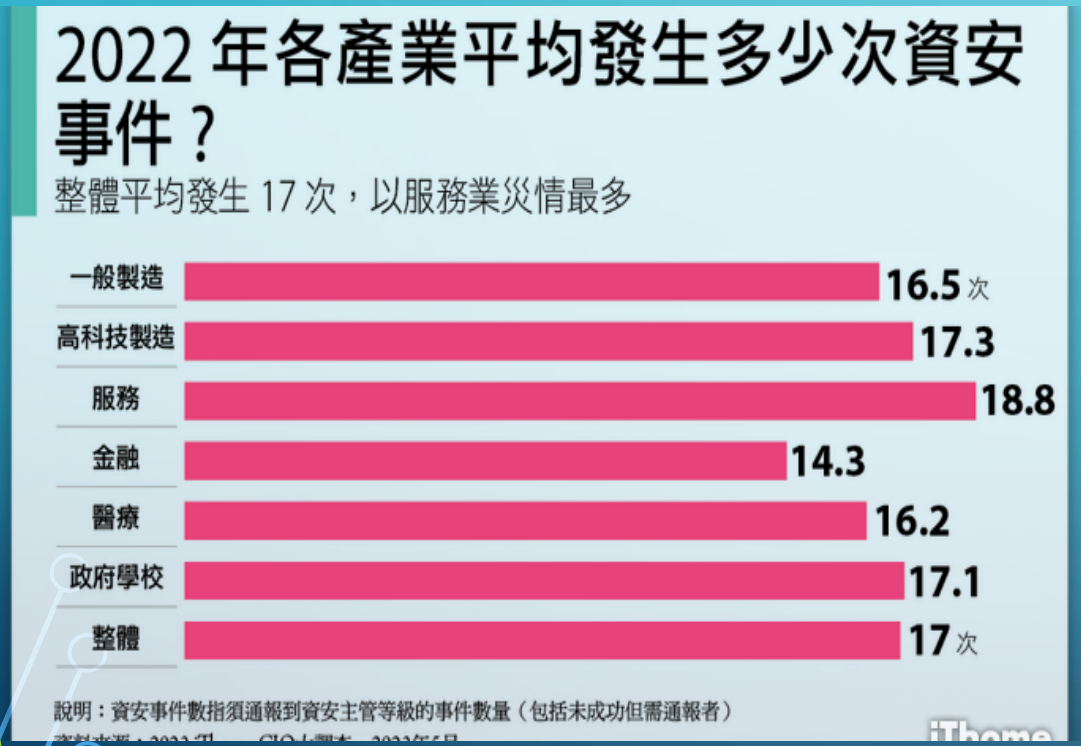
大綱

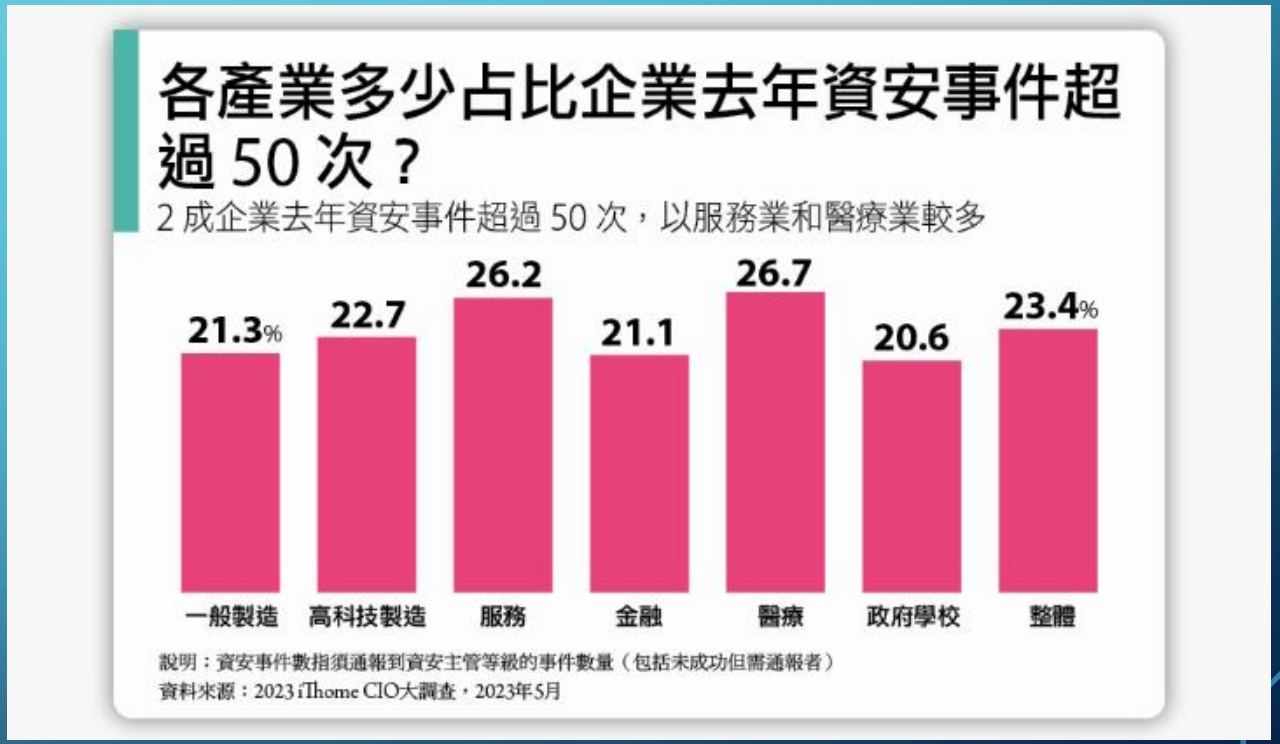
- 資訊安全威脅認知
- 認識釣魚手法
- 變臉詐騙
- 個人電腦與伺服器更新
- 資訊與物聯網設備密碼設置原則
- 禁用大陸廠牌之識別
- 資訊委外合約訂定與人員資格
- 個人資料使用與保護注意事項

資訊安全威脅認知



2022年產業資安事件統計





參考自：【iThome大調查系列1：2023資安大調查】2022年各產業資安事件多頻繁？多快復原？

近期重大資安事件

公部門、關鍵設施	
2021內政部戶政資料	駭客在暗網兜售2357筆戶役資料
2023華航	駭客勒贖、會員資料外洩
2023.3故宮	行政院證實數千件國寶約十萬張圖檔遭竊賤賣
科技	
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	大陸駭客展開持續滲透威脅(APT)行動
金融	
2021.11 7家證券、期貨商	駭客撞庫攻擊、客戶被異常下單
消費娛樂	
2023.1 iRent	40萬筆個資外洩
2023.1博客來、誠品等5家電商	遭刑事警察局點名高詐騙風險賣場
2023.2微風	90萬筆個資外洩

什麼是網路攻擊?

- 個人或組織基於惡意，故意嘗試入侵其他個人或組織的資訊系統，通常會藉由中斷受害者的網路尋求特定利益。
- 對企業或個人電腦造成損害、取得控制權或存取重要文件、資料。
- 常見的攻擊類型有以下幾種：
  - 惡意程式
  - 分散式阻斷服務(DDoS)
  - 殭屍網路
  - 勒索軟體
  - 物聯網攻擊
  - 網路釣魚
  - 變臉詐騙

惡意程式

- 會偽裝成受信任的電子郵件附件或程式(即加密的文件或檔案資料夾)，以利用病毒或允許駭客進入電腦網路。
- 設計目的是在終端用戶不知情的情況下對電腦、伺服器、客戶端或電腦網路及/或基礎設施造成損害或破壞。
- 常見的惡意程式有：木馬程式、間諜軟體、蠕蟲、病毒和廣告軟體。

快檢查有沒有！CHROME「32款惡意程式」洩個資百萬用戶受害

三立新聞網(2023年6月7日科技中心／魏君程報導)

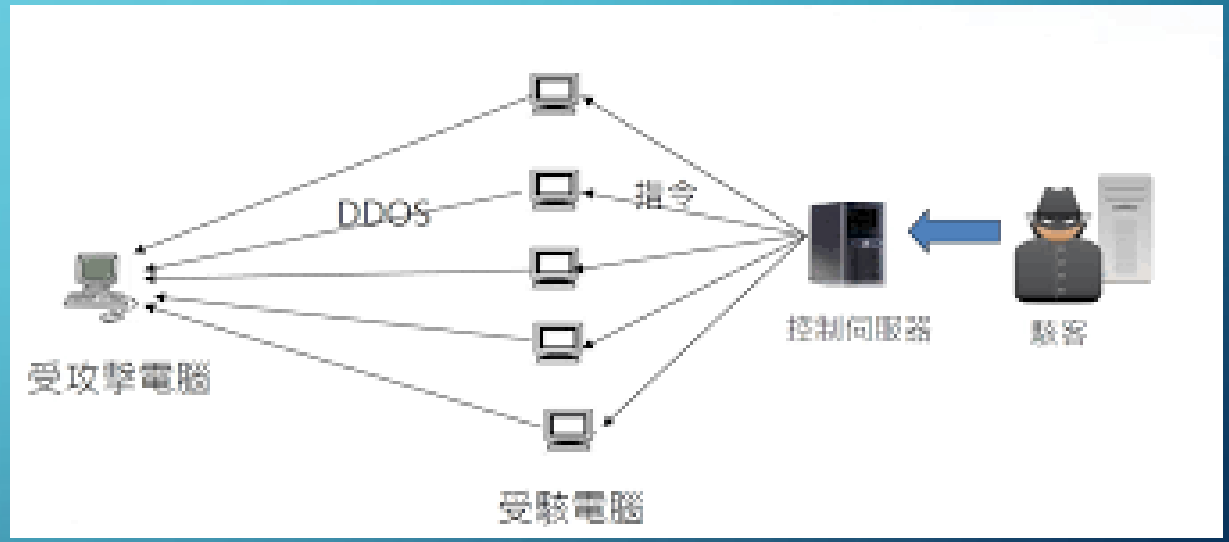
快刪！據資安網站指出，在Chrome應用商店中有32個惡意外掛程式，如果民眾下載恐怕會不同發送惡意郵件、付費連結，從而竊取個資，其總下載次數高達7500萬次，影響數百萬名用戶。

據資安網站《Avast》指出，在Chrome的應用商店當中，發現32款惡意的擴充程式，這些外掛的功能恐怕會偽裝成**廣告攔截器**、**下載器**、**瀏覽器主題**、記錄器等無害的模樣，讓用戶掉以輕心。

《Avast》指出，若是不小心下載這些惡意擴充，恐怕會害得用戶發送惡意郵件、付費連結，改變檢索細節等，進而竊取用戶的個資。

分散式阻斷服務(DDOS)

- 會將目標放在網站或伺服器，進行網路服務干擾。
- 會試圖耗盡應用程式或資源，利用異常流量湧入網站，導致網站無法正常運作，或直接下線。
- 攻擊手法都是以大量的無效請求進行網站的頻寬及資源消耗。
- 攻擊手法有幾個特點：
  1.事先無徵兆或跡象。
  2.攻擊來源非常廣泛。
  3.包含多種攻擊方式，手法複雜。
  4.攻擊瞬間，網路(封包)流量非常高。



計程車隊遭「惡意阻斷攻擊」APP叫車卡卡

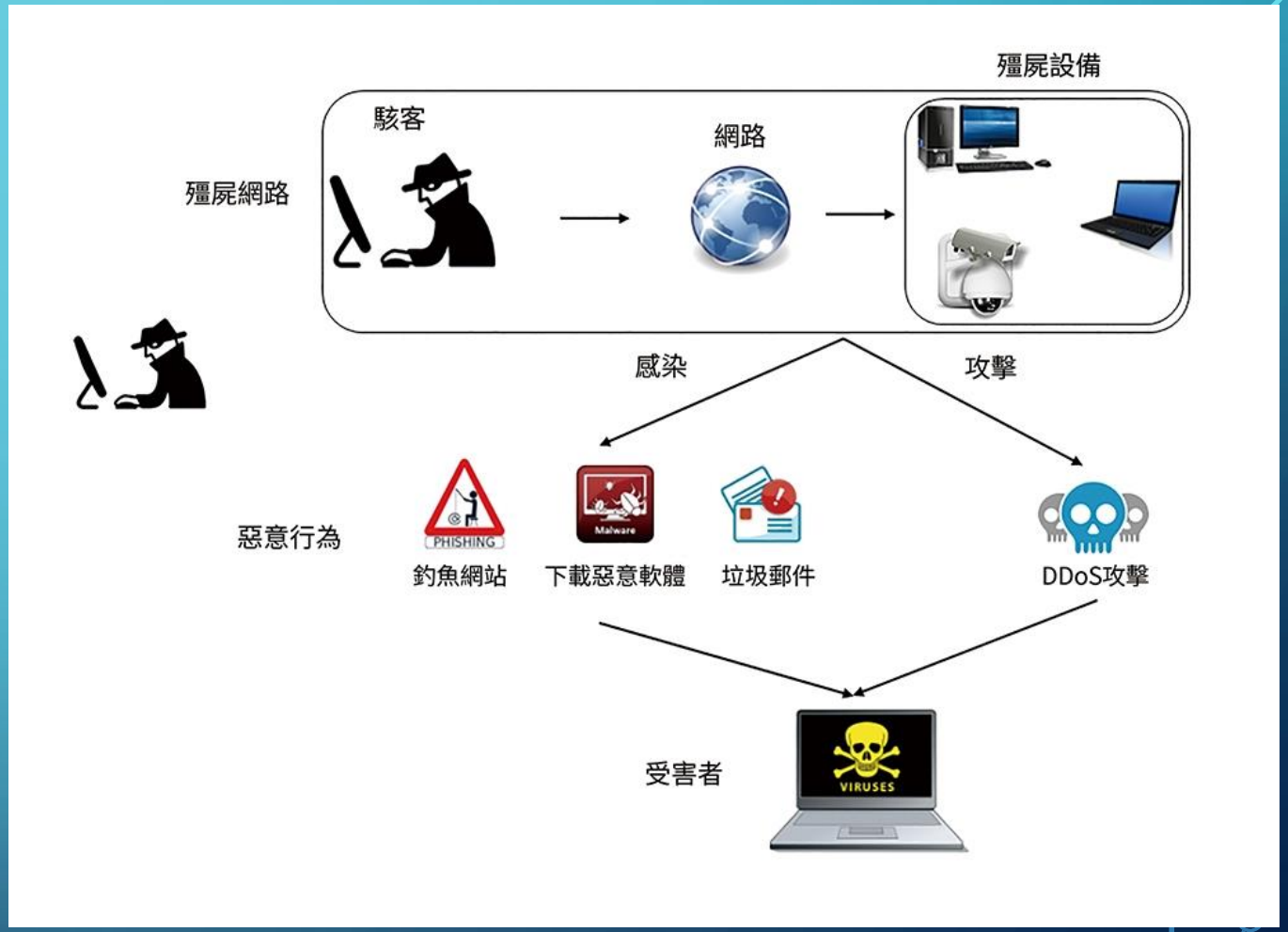
TVBS新聞網 (2023年6月23日)

最近民眾透過App叫台灣大車隊的車，都會有程式當掉、進不去的狀況，業者公告，因他們近期不斷遭受阻斷式攻擊，已經升級系統來保護消費者資料，但有乘客反映，說他接到詐騙電話，問他是不是有搭車，對此大車隊強調，客戶資料沒外洩，資安專家曾說過，這叫「撞庫攻擊」。

記者林昫叡：「台灣大車隊他們最近貼出公告，說他們被針對性不斷使用阻斷服務攻擊，導致他們的會員如果要用App叫車，程式沒有辦法打開，會有延遲的狀況。」

殭屍網路

- 指多部電腦(通常位於私人網路)受到駭客、電腦病毒或木馬程式入侵，使駭客可以通聯與控制的方式，遠端控制大量受到感染的設備，構成「殭屍網路」，發動惡意攻擊。
- 殭屍網路不只能發動攻擊，還可以執行：分散式阻斷攻擊 服務、傳送大量垃圾訊息(郵件)、竊取資料及挖礦。



引用來源：《網管人》2019知己知彼方能因應　看清殭屍網路肆虐真相

利用TP-LINK路由器漏洞的新殭屍網路CONDI NETWORK現身

iThome (文/陳曉莉 | 2023-06-21發表)

資安業者Fortinet旗下FortiGuard Labs近日揭露了一個新的殭屍網路Condi Network，它利用已於今年3月修補的TP-Link Archer AX21漏洞CVE-2023-1389進行散布，在擴大感染規模的同時，也已推出DDoS服務。

CVE-2023-1389是個位於TP-Link路由器的安全漏洞，允許未經授權的駭客藉由其網路管理介面注入命令，TP-Link在今年1月收到通知，3月便藉由韌體更新修補了該漏洞，然而，駭客4月就利用該漏洞部署了Mirai殭屍網路病毒，Condi Network則是第二個利用該漏洞的殭屍網路。

安全研究人員指出，諸如**殭屍網路等惡意程式活動通常會持續探索擴張的方法，而最新的漏洞一直是最受駭客青睞的途徑之一**，強烈建議使用者應儘快部署安全更新。

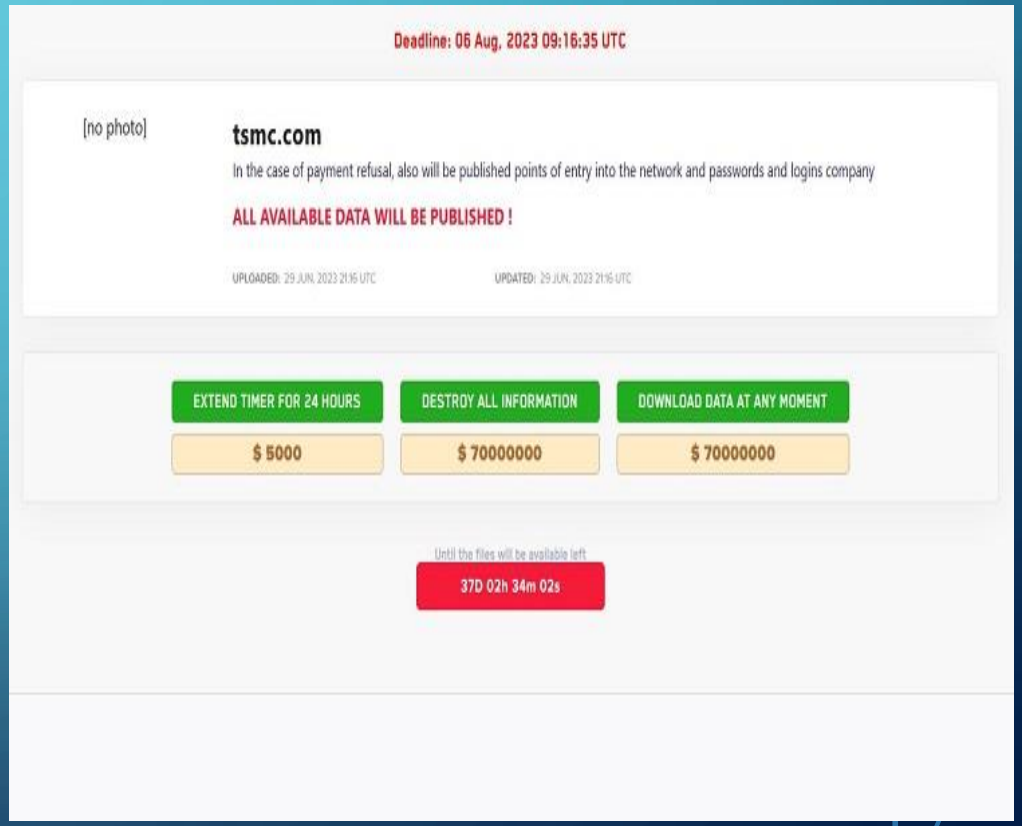
勒索軟體

- 一種惡意軟體或惡意程式碼，透過破壞或封鎖重要資料或系統的存取權來威脅受害者，直到對方支付贖金。
- 常用手法：
  - 不當遠端連線設定
  - 社交工程電子郵件
  - 電腦設備漏洞

【資安日報】6月30日，勒索軟體LOCKBIT聲稱入侵台積電，索討7千萬美元贖金

iThome(文/周峻佑 | 2023-06-30發表)

根據國內外新聞媒體6月30日上午的報導，勒索軟體LockBit聲稱攻擊了台積電（tsmc.com），並要脅若不付錢，他們將公布能夠進入該公司內部網路的帳號及密碼。駭客也開出價碼，要求銷毀資料，或是下載檔案的價碼為7千萬美元。



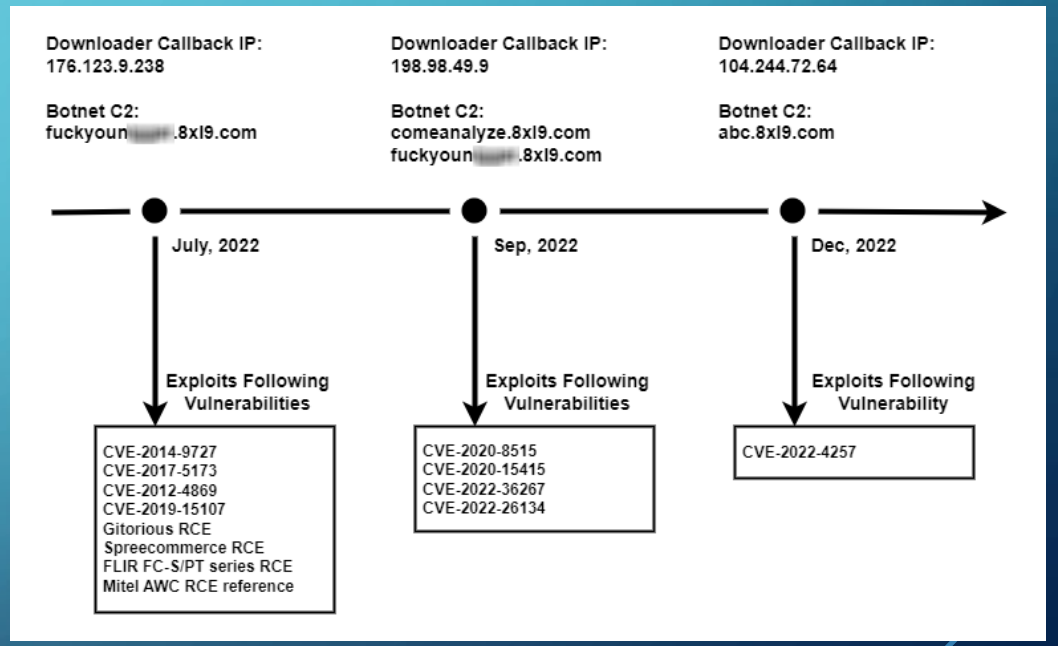
物聯網攻擊

- 物聯網設備（IoT）讓人們的日常生活充滿更多的可能性。
- 物聯網設備也非常容易受到駭客攻擊，這些設備的運算能力和儲存空間雖然有限，但在廠商專注於功能與外觀的情況下，往往忽略了設備的安全性。
- 用戶通常不會修改物聯網設備的密碼，導致設備的預設密碼仍然有效，再加上使用相同的預設用戶名稱與密碼，這代表幾乎任何人都能登入。

【資安日報】2023年2月17日，殭屍網路V3G4針對13個物聯網裝置漏洞而來、臺灣組織IIS伺服器遭到惡意軟體FREBNIIS鎖定

iThome(文/周峻佑 | 2023-02-17發表)

資安業者Palo Alto Networks揭露自2022年7月出現的殭屍網路V3G4，該殭屍網路病毒是Mirai變種，鎖定**電話交換機**（PBX）**系統**FreePBX的漏洞CVE-2012-4869、**視訊監控系統**AVM Fritz!Box漏洞CVE-2014-9727、居易Vigor**路由器漏洞**CVE-2020-8515、CVE-2020-15415，以及**Atlassian Confluence協作平台漏洞**CVE-2022-26134等13個弱點，其目標的共通點就是執行Linux作業系統的連網裝置，一旦裝置感染了殭屍網路病毒，就會被駭客控制，且很有可能用於DDoS攻擊。



認識釣魚手法

認識釣魚手法

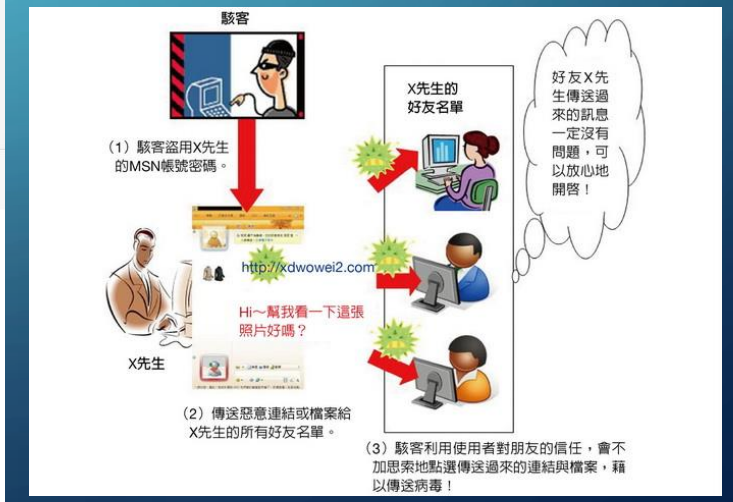
- 釣魚（Phishing）是一種詐騙手法，詐騙者通過冒充信任的寄件人或組織來欺騙受害者提供個人敏感信息，如帳戶資料、密碼、信用卡號碼等。
- 一般是指駭客利用電子郵件或訊息，來騙取使用者或企業資訊的社交工程技巧。
- 這類電子郵件通常會謊稱他們懷疑你的帳號遭受盜用，或是提供一些好康訊息，要求你點開郵件內的連結來確認帳號合法性，而這些連結通常有兩個作用：
  1. 將你帶到某個與原網頁極為相似的網站，當你在這個網頁上輸入自己的資訊時，駭客就可以蒐集到你的帳號跟密碼。
  2. 下載惡意程式到你的電腦，用於後續發動攻擊；有時是勒索病毒，會將硬碟上的檔案加密後勒索贖金。

常見的釣魚手法

- 偽冒電子郵件（Phishing emails）：詐騙者發送看似來自信任的公司或組織的電子郵件，要求受害者點擊連結或提供個人信息。這些電子郵件通常會冒用銀行、社交媒體平台、電子支付服務等知名品牌。
- 偽冒網站（Phishing websites）：詐騙者建立看似合法的網站，與真實的網站外觀相似，以騙取受害者的登錄資訊。他們可能會通過偽造的登錄頁面或彈出式視窗要求受害者提供帳戶名稱和密碼。

常見的釣魚手法

- 社交工程（Social engineering）：詐騙者利用心理學和欺騙手法，通過電話、簡訊、社交媒體等方式與受害者互動，以獲取個人信息。他們可能假裝是銀行員工、客戶服務代表或IT支援人員，試圖誘使受害者提供敏感資料。
- SMS釣魚（Smishing）：詐騙者通過短信向受害者發送詐騙簡訊，試圖引誘他們進行操作或訪問惡意網站。這些簡訊通常聲稱是來自銀行、快遞公司或獎品抽獎等。



常見的釣魚手法

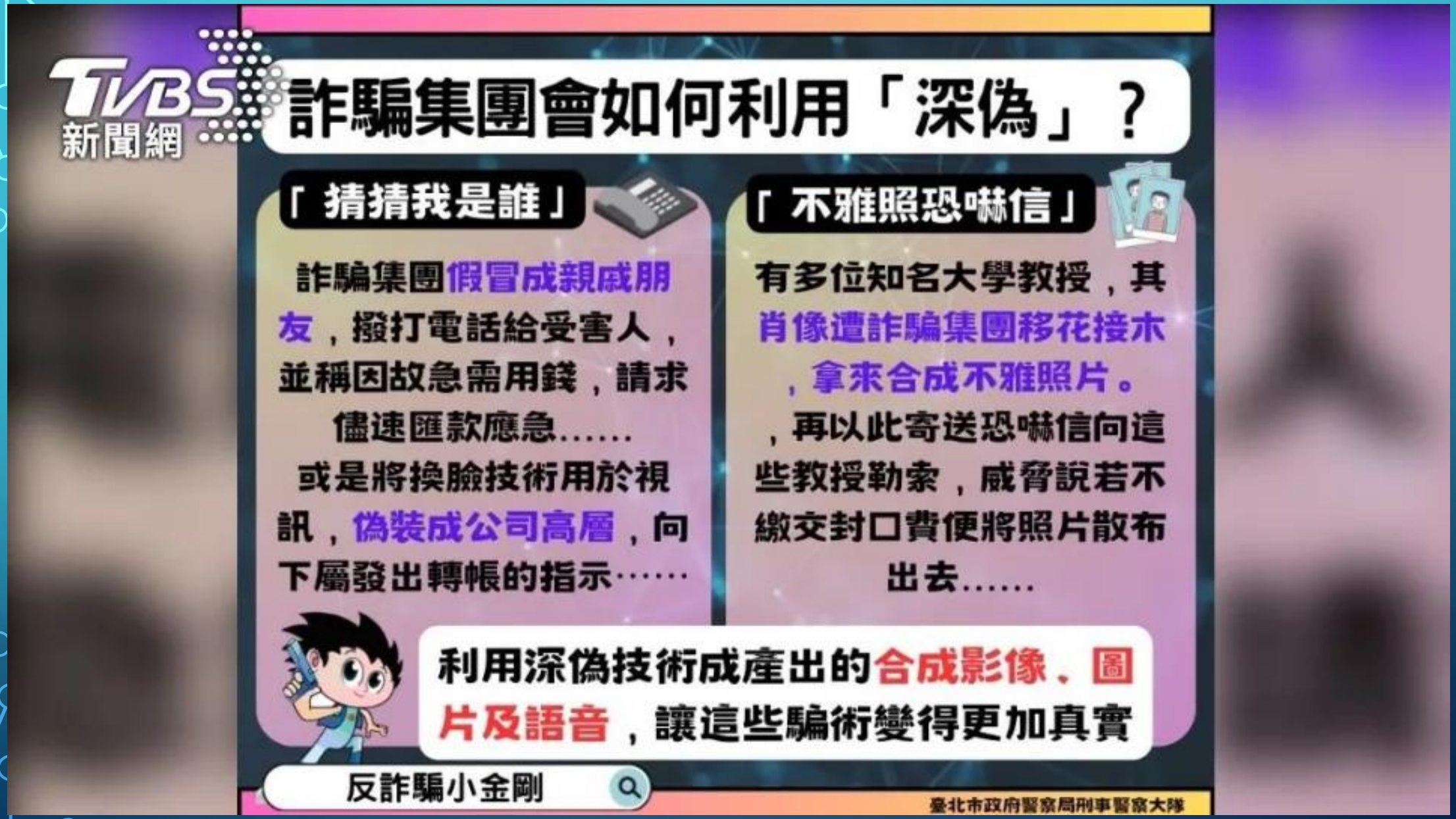
- 偽造應用程式（Phishing apps）：詐騙者開發偽造的應用程式，通過應用程式商店或第三方網站進行分發，以引誘用戶下載並提供個人信息。這些應用程式可能冒用知名品牌的標誌和介面，從而欺騙受害者。

圖：取自<自由時報 2023/4/15 假冒台新證券App誘投資詐2500萬>

圖：取自<ETTODAY財經雲 2023/1/20凱基證券驚傳「假APP詐騙」！公司張貼對比圖提醒：已經報案>

如何保護自己免受釣魚攻擊

- 對任何來自不明來源的電子郵件、簡訊或其他通訊方式保持警惕。謹慎點擊連結或下載附件。
- 確保你只在安全、加密的網站上輸入個人敏感信息，特別是銀行和金融相關的網站。
- 驗證電子郵件或簡訊的發送者的身份，特別是在提供個人資訊之前。請直接聯繫相關機構或公司，而不是通過提供的連結或號碼回復。
- 使用高強度的密碼並定期更改。不要在不同的網站使用相同的密碼。
- 安裝並定期更新防毒軟體和防火牆，以檢測和阻止釣魚攻擊。
- 保持對釣魚攻擊手法的了解，以便能夠識別潛在的風險和威脅。


TVBS 新聞網
詐騙集團會如何利用「深偽」？
「猜猜我是誰」
詐騙集團假冒成親戚朋友，撥打電話給受害人，並稱因故急需用錢，請求儘速匯款應急……
或是將換臉技術用於視訊，偽裝成公司高層，向下屬發出轉帳的指示……
「不雅照恐嚇信」
有多位知名大學教授，其肖像遭詐騙集團移花接木，拿來合成不雅照片。
，再以此寄送恐嚇信向這些教授勒索，威脅說若不繳交封口費便將照片散布出去……
利用深偽技術成產出的合成影像、圖片及語音，讓這些騙術變得更加真實
反詐騙小金剛
臺北市政府警察局刑事警察大隊

深偽技術(Deepfake)

- 深偽技術「Deepfake」又稱「深度偽造」，是以深度學習「Deep Learning」和偽造「Fake」的混成詞。
- 專指基於人工智慧的人體圖像合成技術的應用，此種技術可將現有的圖像或是影片疊加到目標圖像或是影片上，以製作能夠以假亂真的假媒體。
- 可以將A君的臉部特徵、表情和動作運用到B君的身上，使其看起来好像是A君在說話或做出某些動作。
- 26歲百萬 YouTuber 小玉利用 Deepfake 技術，將包含黃捷、鄭家純（雞排妹）、高嘉瑜等名人的臉合成在A片女優身上，移花接木的性愛影片，造成百人受害，不法所得逾新台幣上千萬元。

如何識別深度偽造？

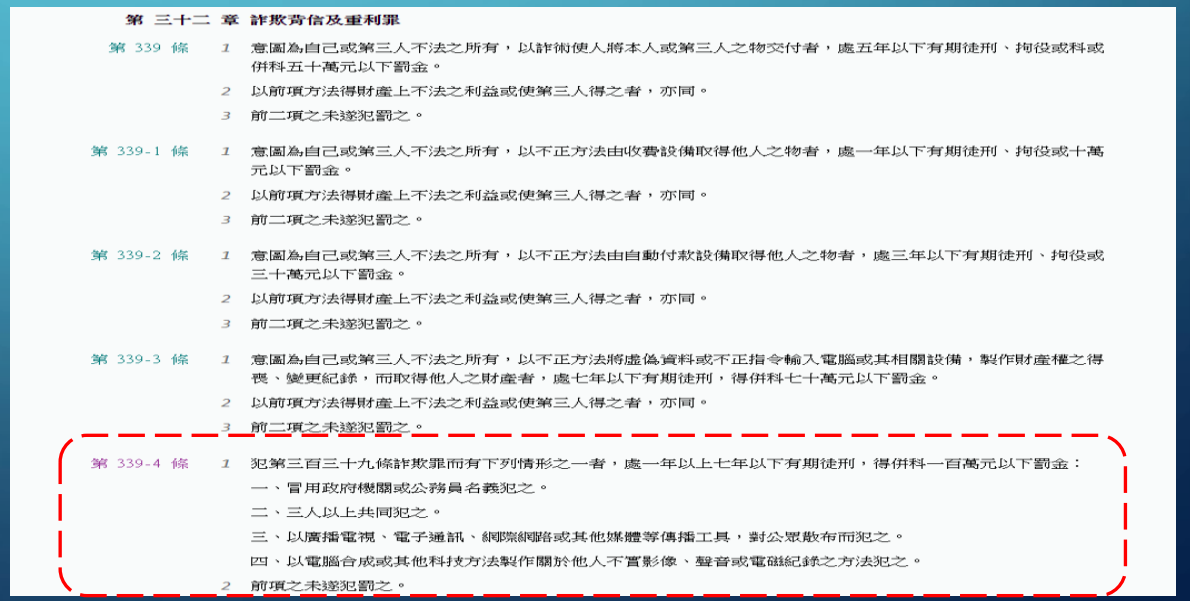
- **明顯的視覺瑕疵**：深偽影片中，疊加部分的接合處是否有明顯瑕疵為重要的判斷依據，在臉部輪廓的邊緣有時也會出現不自然的紋理。即使是製作精良的深偽影片中，在背景區域或是影片跨幀時，人物的輪廓都可能會有模糊或是失真的情形出現。
- **非臉部特徵不精確**：如果影片中出現的是一位公眾人物，可以試著使用找尋這個人的圖像來做比對，看看在主要臉部特徵以外的地方，例如手部、頭髮、體型等，這些可能沒有被改變。
- **不自然的肢體動作**：以現行技術而言，當影片中的人物沒有太多動作時，深度偽造看起來較有說服力。如果影片人物的身體和頭部看起來異常僵硬，這就可能是一個跡象，表示影片的創作者只有讓深度學習 AI 輕鬆將圖像合成到人物的臉上，而沒有處理太多肢體動作的部分。

如何識別深度偽造？

- **難以令人信服的聲音**：深偽技術正在迅速發展，但就目前而言，訓練電腦創造模擬音訊，似乎比合成令人信服的深偽圖像和影片產出的效果要差。深度偽造的創造者如果想讓對象人物說話，必須在兩個選項中做出選擇——或是使用人工智慧生成的聲音，或是使用能夠模仿材料來源的演員。可將影片聲音與名人或政治人物講話的音訊進行比較，可能就會注意到某些差異。

刑法修正三讀 電腦合成深偽影像聲音詐騙最重關7年罰百萬

- 為遏止詐騙集團用電腦合成等方法製作不實影像詐欺，立法院5月16日通過刑法修正案，在刑法第三十二章詐欺背信及重利罪中，增訂第339-4條「製作他人不實影像行騙，以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄詐欺罪」，可處一年至七年有期徒刑，得併科一百萬元以下罰金。



第 三十二 章　詐欺背信及重利罪

第 339 條　1　意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。
2　以前項方法得財產上不法之利益或使第三人得之者，亦同。
3　前二項之未遂犯罰之。

第 339-1 條　1　意圖為自己或第三人不法之所有，以不正方法由收費設備取得他人之物者，處一年以下有期徒刑、拘役或十萬元以下罰金。
2　以前項方法得財產上不法之利益或使第三人得之者，亦同。
3　前二項之未遂犯罰之。

第 339-2 條　1　意圖為自己或第三人不法之所有，以不正方法由自動付款設備取得他人之物者，處三年以下有期徒刑、拘役或三十萬元以下罰金。
2　以前項方法得財產上不法之利益或使第三人得之者，亦同。
3　前二項之未遂犯罰之。

第 339-3 條　1　意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人之財產者，處七年以下有期徒刑，得併科七十萬元以下罰金。
2　以前項方法得財產上不法之利益或使第三人得之者，亦同。
3　前二項之未遂犯罰之。

第 339-4 條　1　犯第三百三十九條詐欺罪而有下列情形之一者，處一年以上七年以下有期徒刑，得併科一百萬元以下罰金：
一、冒用政府機關或公務員名義犯之。
二、三人以上共同犯之。
三、以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散布而犯之。
四、以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄之方法犯之。
2　前項之未遂犯罰之。

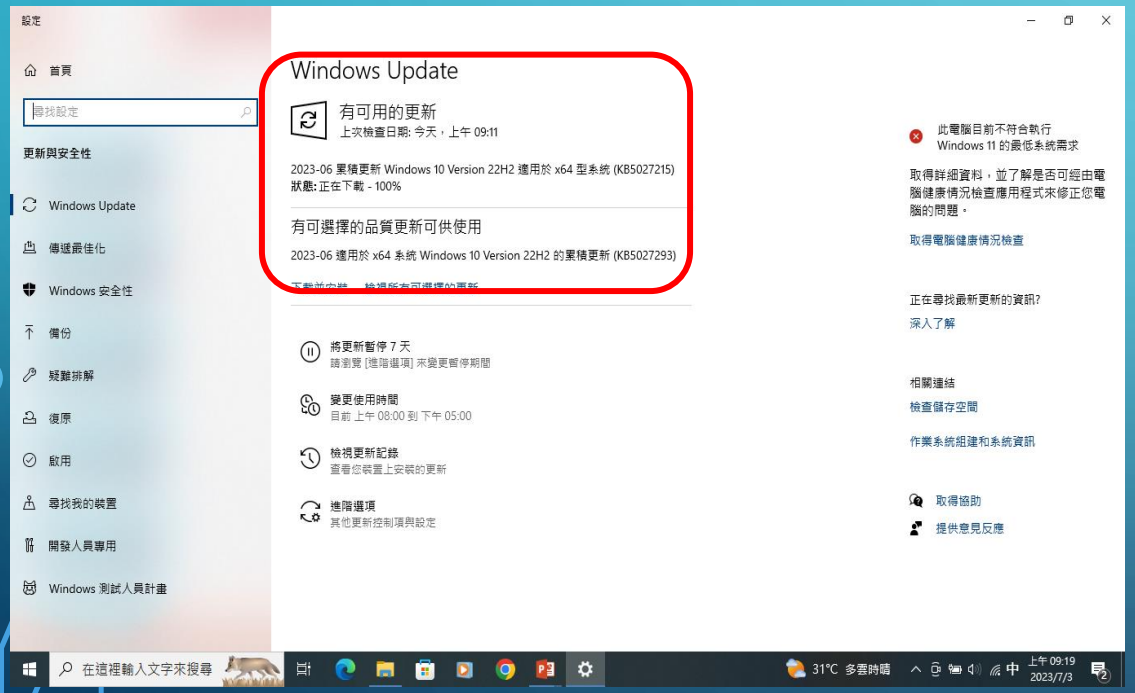
個人電腦與伺服器更新

為何要定期更新個人電腦及伺服器?

- 為確保資訊安全，定期更新個人電腦及伺服器是一種保護安全性，提升效率，避免因為漏洞導致被駭的重要做法。
- 以下將說明執行個人電腦及伺服器更新的做法，提供參考：

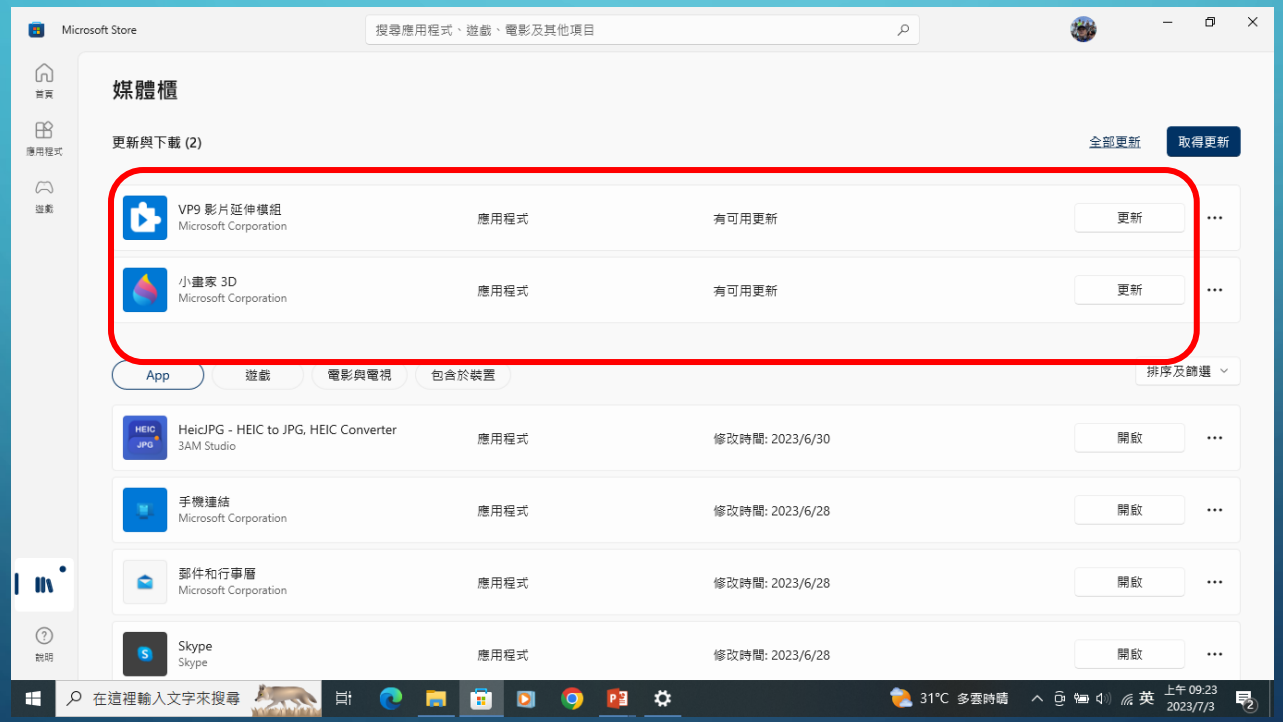
個人電腦更新

- 系統更新：定期檢查作業系統(如Windows、MacOS)的更新，可以通過自動更新功能或手動下載並安裝最新安全性和版本更新。



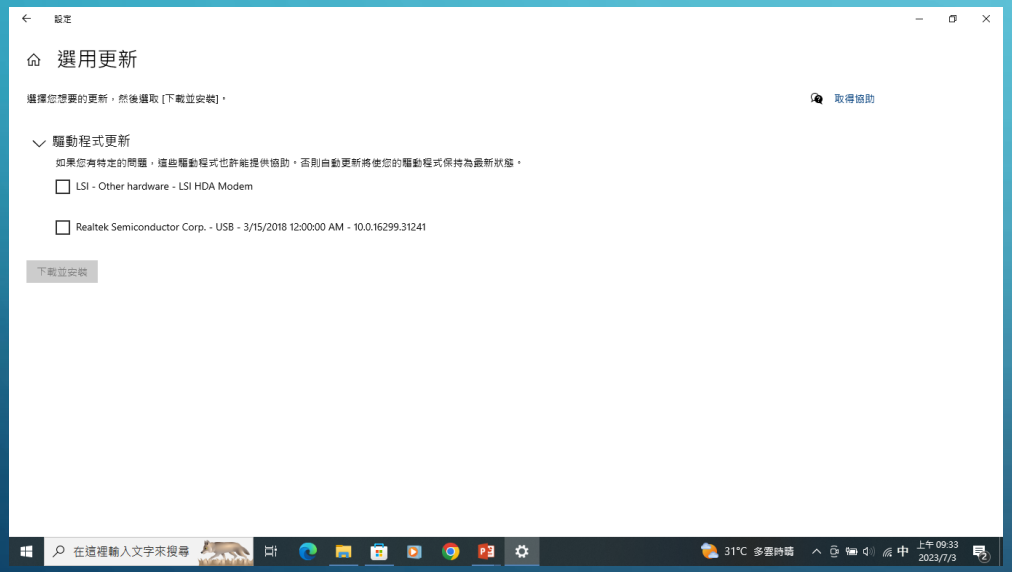
個人電腦更新

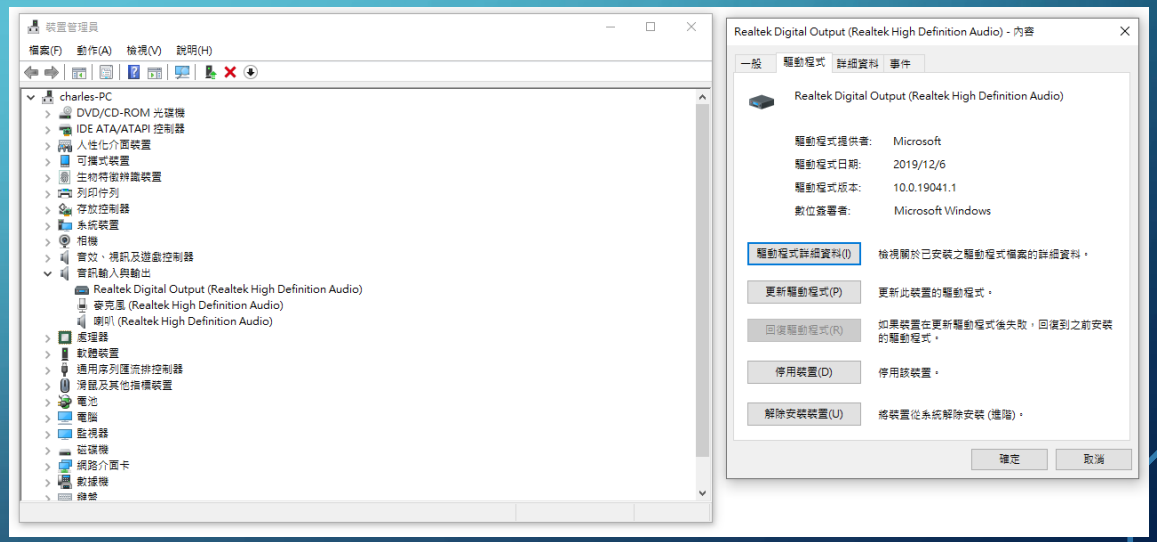
- 軟體更新：保持應用程式(如網路瀏覽器、辦公軟體、防毒軟體等)之更新至最新版本，以獲得更好的功能和安全性



個人電腦更新

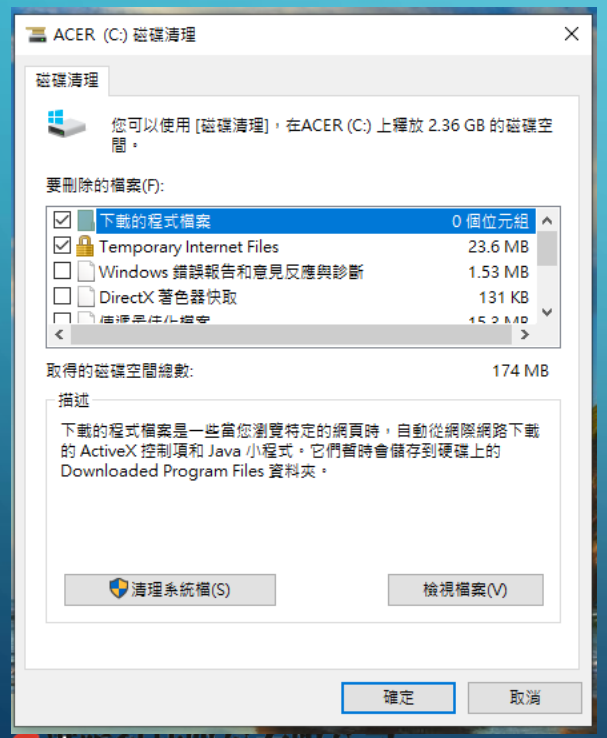
- 驅動程式(Drivers)更新：檢查並更新電腦中的硬體驅動程式，包括韌體、顯示卡、音效卡、網路卡等。可以從硬體製造商的官方網站或裝置管理員中獲取最新的驅動程式。

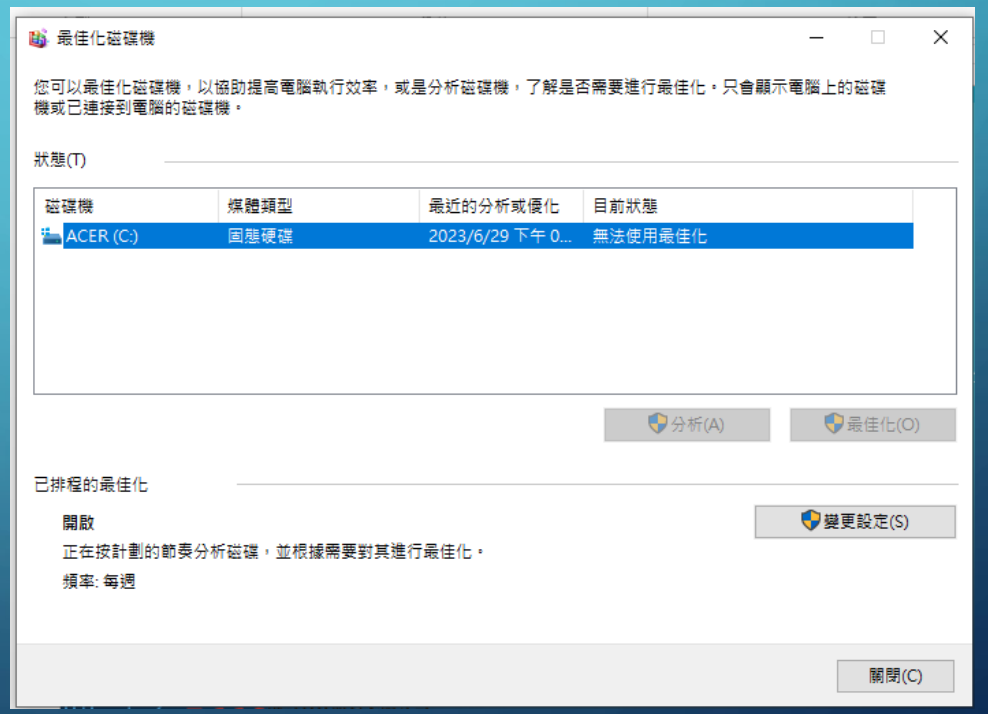




個人電腦更新

- 清理和優化：定期清理暫存檔、不需要的應用程式和檔案，以釋放硬碟空間。可以使用系統內建工具或第三方優化程式進行清理和優化操作。





伺服器更新的做法

- 伺服器更新的作法可以因不同的情況而有所不同，需要注意的是，可能因組織的需求和環境而有所不同。
- 在進行任何伺服器更新之前，建議先詳細閱讀相關的文件、指南或諮詢專業人士，以確保採取正確的步驟和順序進行更新作業。
- 以下是一般常見的伺服器更新流程：

伺服器更新的做法

備份資料：在進行任何伺服器更新之前，重要的第一步是備份所有的重要資料。這樣做可以確保在更新過程中出現任何問題時，可以復原到更新前的狀態。

測試環境：建立一個測試環境，在其中複製主要伺服器的配置和設定。在測試環境中進行更新，測試所有相關的應用程式、服務和功能是否正常運作。這可以幫助確保更新不會對主要伺服器造成任何問題。

伺服器更新的做法

計劃更新時間：確定一個適合的時間進行伺服器更新。這可能是在離峰時段，以減少對使用者的影響。同時，考量到更新可能需要一些時間，確保有足夠時間來完成更新過程。

通知使用者：提前通知使用者伺服器將進行更新，並說明更新可能導致暫時中斷服務或其他相關問題。可讓使用者有時間準備或計劃其工作。

伺服器更新的做法

關閉服務：在更新開始前，暫停伺服器上的所有相關服務。可避免在更新過程中，有用戶訪問或修改數據的情況發生，以防止資料損壞或其他問題。

執行更新：根據具體的更新內容和需求，執行伺服器更新。可能包括安裝更新的操作系統、應用程式程式碼的更新或配置變更等。

伺服器更新的做法

測試和驗證：在更新完成後，進行測試和驗證，以確保更新成功。測試各種功能、服務和相關應用程式，並確保它們正常運作。

重新啟動服務：完成測試後，重新啟動伺服器上的相關服務，使其恢復正常運作。確保服務恢復後，監視伺服器的運行狀態，以確保一切正常。

伺服器更新的做法

監視和維護：更新後，持續監視伺服器的運行狀態，確保沒有出現任何問題。同時，進行定期的維護工作，包括更新安全性修補檔、監視性能、備份資料等。

資訊與物聯網設備密碼設置原則


TVBS新聞台 HD
密碼太好記「1秒可破解」·最強組合曝
資料來源:ETtoday
網路安全專家凱特琳
駭客技術
日新月異
破解6字元密碼 最快只花1秒
破解7字元密碼 只需要1分鐘
8字元密碼 能在1小時內解開
9字元密碼 可以在3天內猜出
最強密碼
密碼最好11字元以上
同時含字母.字元.符號
未含已知單字或名字
可能需41年才能破解
1. Enter your email, first and last, name and password
善用工具檢查是否遇駭
Scanning for Data Leaks...
翻攝TikTok@cybersecuritygirl
TikTok
@cybersecuritygirl
記者 韋家齊
密碼別設太簡單 資安專家:駭客1秒就破解
掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道

密碼設置的重要性

- 資訊及物聯網設備的密碼的重要在於，它們直接關係到你的資料及設備的安全性，可以避免未經授權的使用者操作運用，保護個人的隱私資料不被外洩，更重要的是，可以防止帳號被盜用，成為犯罪的工具，因此，資訊及物聯網設備密碼的設置，不可輕忽。
- 以下針對幾個密碼設置的原則，提供大家做為參考。

密碼設置的原則

- 使用高強度密碼：至少12個字元以上的高複雜度密碼，包括英文大小寫字母、數字和特殊符號。避免使用常見字詞、生日、姓名等容易猜測的密碼。
- 不使用重複密碼：確保在不同設備和帳戶中使用不同密碼。如果一個密碼被破解或洩漏，其他帳戶仍然保持安全。

密碼設置的原則

- 定期更換密碼：定期更改密碼是一種良好的安全習慣。根據需要，定期更換資訊和物聯網設備的密碼，例如每三到六個月更換一次。
- 使用多因素身份驗證：啟用多因素身份驗證（MFA）是增強安全性的有效方式。除了密碼之外，還需要提供其他驗證因素，例如生理辨識系統(如指紋、臉部辨識)、硬體安全金鑰等。

密碼設置的原則

- 不要共享密碼：避免將密碼共享給其他人，即使是信任的人也應該避免。如果需要授權其他人使用設備或帳戶，應考慮使用特定的權限管理功能。
- 定期檢查和更新設備韌體：定期檢查設備的韌體並安裝最新的安全更新。許多設備製造商會針對已知漏洞和安全問題發布更新。

密碼設置的原則

- 監控和記錄：監控設備和系統的活動，並記錄異常事件。這樣可以追蹤潛在的安全威脅並及時採取適當的對策。
- 教育用戶：教育和提高使用者對密碼安全和資訊安全的意識。使用者應該知道不要將密碼透露給他人，不要點擊不明來源的鏈接，以及適當管理和保護他們的設備和帳戶。

零信任與多因素身分認證是現今資安環境的治本關鍵

- 零信任和多因素身份認證有效地提高資訊安全性，防範各種威脅和攻擊手法。
  - **零信任原則**：即使攻擊者在內部網路，仍需通過多重階段驗證才可以讀取敏感資源，這能有效地降低內外部攻擊的成功率。
  - **多因素身份認證**：要求使用者提供多個獨立的驗證因素，如密碼、指紋辨識等，增加攻擊者入侵帳戶的難度。

- 這兩種安全措施的結合，使得資訊安全更加全面。它們能夠幫助單位保護敏感資料和資源，防止未經授權的存取，降低資訊洩露和入侵的風險。

零信任的原則與架構

- 零信任（Zero Trust）是一種資訊安全的原則與架構，基本理念是不信任內部或外部網路中的任何資源、用戶或裝置，而是持續地驗證、授權和監控它們的行為，並且基於需要的最小權限原則，只授予最小必要的訪問權限。
- 傳統的安全模型通常是建立在信任內部網路的前提下，當用戶一旦獲得網路內部的訪問權限，就可以自由訪問內部資源。但隨著日益複雜和隱蔽的攻擊手法的出現，這種信任模型變得容易受到攻擊，導致資訊安全漏洞。

零信任的原則與架構有以下重要特點

1. **不信任原則**（**Never Trust, Always Verify**）：不信任任何用戶、裝置或資源，無論是位於內部網路還是外部網路。每個訪問者都必須經過驗證和授權，無論是內部員工還是外部供應商。
2. **最小權限原則**（**Least Privilege**）：每個用戶或裝置只能獲得執行工作所需的最低權限，並且權限應該根據需要進行動態調整，以便及時應對不同風險場景。
3. **多重身份驗證**（**Multi-Factor Authentication**）：採用多種身份驗證方式，例如密碼、生物識別、硬體密鑰等，以確保使用者的身份真實可信。
4. **內、外部網路同等對待**：對於訪問內部網路和外部網路的要求應該同樣嚴格，不因為處於內部網路就授予更多權限。

零信任的原則與架構有以下重要特點

5. **運用加密技術保護數據**：將數據加密，無論是傳輸中還是靜態儲存，確保即使數據被竊取也無法被解讀。
6. **持續監控和分析**：實時監控用戶和裝置的活動，並分析異常行為，以及時發現並應對安全事件。
7. **明確政策的權限控制**：建立明確的安全政策，根據這些政策來控制資源的訪問權限。
8. **強調可見性**：使安全團隊能夠審核和監控資源訪問的細節，了解網路中發生的活動。

零信任的目標是建立一個更安全、更靈活且更有彈性的資訊安全環境，有效地保護敏感資訊和資源免受內、外部威脅。

多因素身分認證

- 多因素驗證（Multi-Factor Authentication, MFA）是一種資訊安全機制，用於確認使用者身份的有效性。MFA引入了多個獨立的驗證因素，提供了更強大的安全性，並有效地降低帳戶被盜用或不正當存取的風險。
- MFA已成為許多應用和網站的標準安全措施，尤其是當涉及到敏感資訊或重要資源時。它是一種簡單而強大的安全增強措施，有助於保護用戶帳戶免受盜用和未經授權的存取。

常見的多因素驗證方式

1.知識因素（Something You Know）：
密碼：輸入預先設定的密碼來驗證身份。
PIN碼：通常是較短的數字組合。
2.擁有因素（Something You Have）：
智慧型手機驗證器：使用者在智慧型手機上安裝驗證器應用程式，生成一次性驗證碼（TOTP，Time-Based One-Time Password）。
硬體金鑰：硬體USB裝置(如指紋碟)，生成一次性驗證碼或與網站進行加密通訊。
晶片卡：帶有智能晶片的身份證件或卡片，用於提供身份驗證。
3.生物特徵因素（Something You Are）：
指紋辨識：使用者的指紋用於驗證身份。
虹膜辨識：掃描使用者的虹膜來進行驗證。
臉部辨識：掃描使用者的臉部特徵用於驗證身份。


三貪小豬

禁用大陸廠牌之識別

依據

- 資通安全管理法
- 數位部民國111年11月28日數授資綜字第1111000056號函「各機關對危害國家資通安全產品限制使用原則」

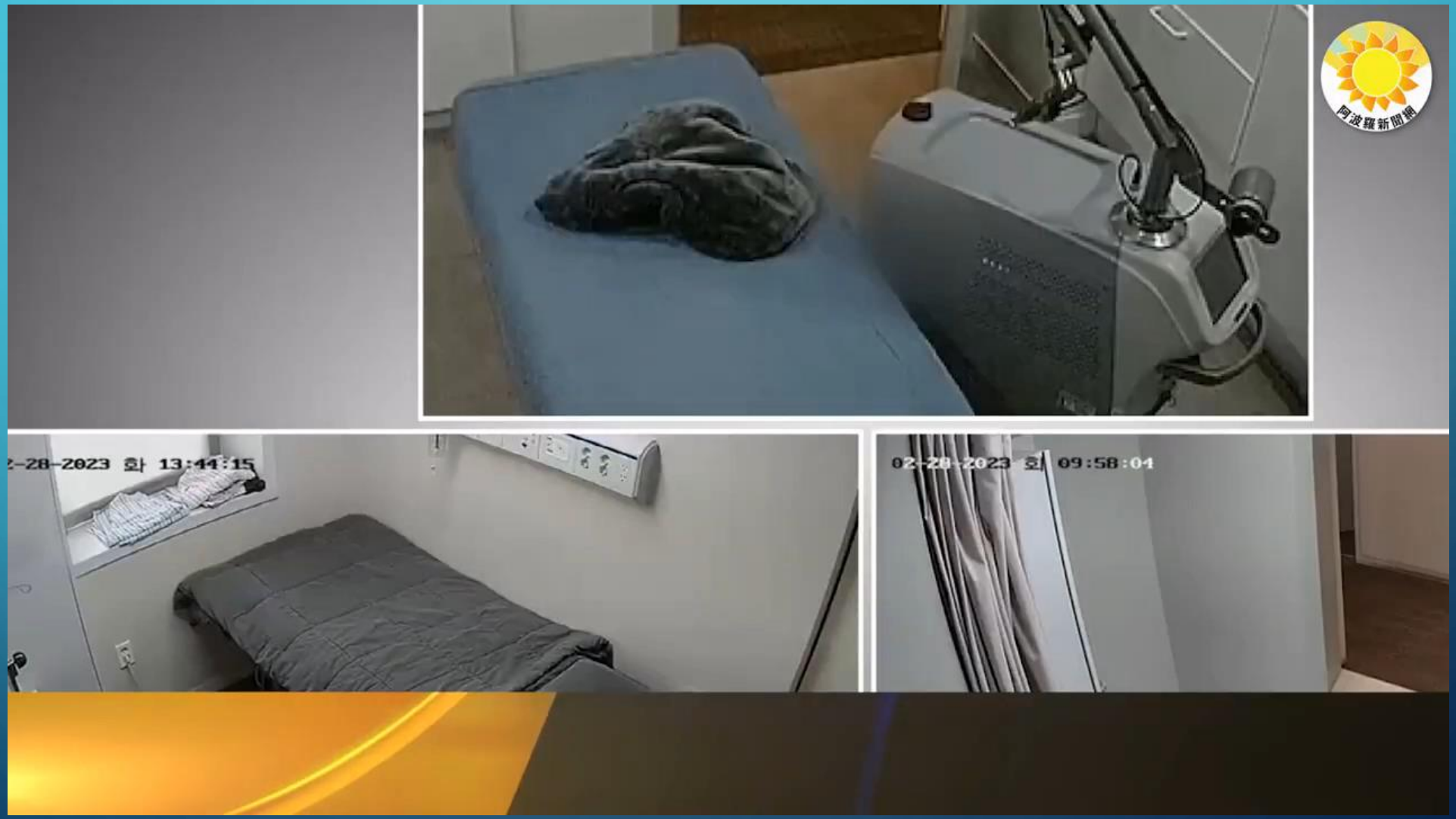
華為首席安全官：中共能在所有產品裝後門

2019/11/15

資料來源：https://www.youtube.com/watch?v=6F3DPhf1594

韓30名藝人裸身外流 遭駭攝影機是海康威視

2023/03/08



資料來源：https://www.youtube.com/watch?v=6Rn4gs0S3Uc&t=398s

陸製資通訊產品大學禁用！

2022/11/23

資料來源：https://www.youtube.com/watch?v=pasQjH89gc0

"大陸製資通訊產品"校園全禁? 立委籲:分級處理

2021/01/09

資料來源： https://www.youtube.com/watch?v=6gSfgyuAEis&t=20s

中國購物App"拼多多"資安危機

2023/04/04

資料來源： https://www.youtube.com/watch?v=1n7gVLkixyA

資通訊產品定義(資通安全管理法第3條)

資通訊產品定義

- 軟體：資通軟體或系統，如應用軟體、系統軟體、開發工具、客製化套裝軟體、APP及電腦作業系統等。
- 硬體：具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備，如個人電腦、伺服器、無人機、印表機、網路通訊設備、可攜式設備及物聯網設備等。
- 服務：資通服務，如客服服務及軟硬體資產維護服務等。

別貪便宜在中國大陸買安卓手機 到別國老大哥仍看著你

2023/02/08

三名研究人員在一篇名為「**放大鏡下的安卓作業系統隱私 - 來自東方的寓言**」文章，分析**小米、一加（OnePlus）、Realme**三個品牌的手機，發現這些手機的中國大陸用戶面臨嚴重的個資外洩風險。

這項研究指出，每支受測、安裝中國大陸韌體的安卓手機，都**預先安裝超過30個第三方軟體套件**，包含安卓的AOSP、供應商程式碼、第三方軟體，例如小米旗下Redmi Note 11的百度輸入法。在OnePlus 9R 和Realme Q3 Pro有做為導航用途的百度地圖以及在後台持續運作的高德地圖等App，已綑綁在這些手機的韌體。

研究發現，這三個品牌的裝置會向原廠或百度、大陸電信商等業者，**發送個人可識別資訊**（PII），例如GPS座標、電話號碼、App使用模式等。即使沒插SIM卡或插別家電信營運商的SIM卡，也都還會發送。」

另一個發現是，在中國大陸發行的安卓系統，**其預先安裝的第三方App數量是其他國家的三到四倍。這些App的權限要求更達到八到十倍**。

資料來源：https://money.udn.com/money/story/5599/6958010

大陸廠牌資通訊產品禁令擴大至對外出租場域

行政院111年8月資安警戒專案相關會議指示：

- 針對**傳播影像或聲音**，供**不特定人士**直接收視或收聽之情形，皆不可使用危害國家資安產品(如大陸廠牌軟體、硬體及服務)。
- 非屬前述傳播類型之危害國家資安產品，亦須列冊管理，控管資安風險，請各機關透過**委外契約**及**場地租借使用規定**來推動辦理。

陸資通產品禁令擴大 納公務場所

2022-08-07 04:06 聯合報／記者侯俐安、邱瓊玉、葉冠妤、盧逸峰、許維寧／台北報導

+ 台鐵

台鐵新左營站電視牆日前遭駭，稱美國眾議院議長裴洛西是「老巫婆」，行政院全面要求公務場所不得使用大陸資通產品。圖為新左營站被駭的電視牆目前停用。記者劉學聖／攝影

資料來源: 聯合新聞網111/8/7報導，
https://udn.com/news/story/122988/6518330

教育部要求應辦事項(對外出租場域)

限制出租場域使用大陸廠牌資通訊產品

- 於學校**委外契約**或**場地租借使用規定**，**明訂**不得使用危害國家資安之產品（**如大陸廠牌軟體、硬體及服務**）。
- 針對現有委外契約，協調廠商配合辦理或**修正契約規定**。
- 備妥應變機制，如遇駭入侵，能緊急斷電下架。

資料來源: 教育部111年資安長會議，
https://net.nthu.edu.tw/netsys/_media/mailing:announcement:a09000000e_1112703805_senddoc1_attach1.pdf

協助識別大陸資訊產品

產品標籤

- 許多資訊產品外包裝或產品本身上貼有標籤。
- 標籤可能包含產品的品牌名稱、型號、序列編號和製造日期等基本資訊。
- 標籤通常以文字和圖標的形式呈現。

國家或地區標示

- 產品上可能會標明其製造國家或地區。
- 常見的標示包括Made in China或具體的大陸品牌名稱。
- 標示通常位於產品外包裝的標籤上，並與製造商的商標或標誌一起呈現

協助識別大陸資訊產品(續)

產品說明書和包裝

- 產品說明書通常提供有關產品特性、功能和使用方法的詳細資訊。
- 包裝上可能會包含相關的商標、製造商資訊和其他識別標誌。

認證和標準

- 大陸資訊產品通常需要符合特定的國際標準和認證，例如中國強制性產品認證（China Compulsory Certification, CCC）。
- 標準認證可能會在產品標示上或相關文件中顯示。
- 常見的認證標誌包括CE標識（歐洲符合性）和FCC認證（美國聯邦通信委員會），這些標誌可能與製造商的國家或地區相關聯。

協助識別大陸資訊產品

製造商名稱

- 對於大陸資訊產品，製造商通常是中國的企業或品牌。
- 藉以提供關於產品製造來源的重要資訊。

常見大陸資通訊產品廠牌清單

軟體

- 瀏覽器：360瀏覽器
- APP：抖音/Tiktok、微信、支付寶、剪映、淘寶、騰訊QQ、小紅書、愛奇藝、知乎
- 防毒軟體：360安全衛士、金山毒霸、瑞星防毒、騰訊電腦管家、百度殺毒

常見大陸資通訊產品廠牌清單

硬體

- 監控攝影機：海康威視(Hikvision)、大華技術(aJhua)、中興通訊
- 網路通訊設備：TOTOLink、普聯（TP-Link）、Tenda
- 無人機：大疆(DJI)
- 手機：華為(Huawei)、歐家控股(OPPO)、小米(MI)、海信、VIVO、魅族、努比亞、SUGAR、REALME

常見大陸資通訊產品廠牌清單

服務

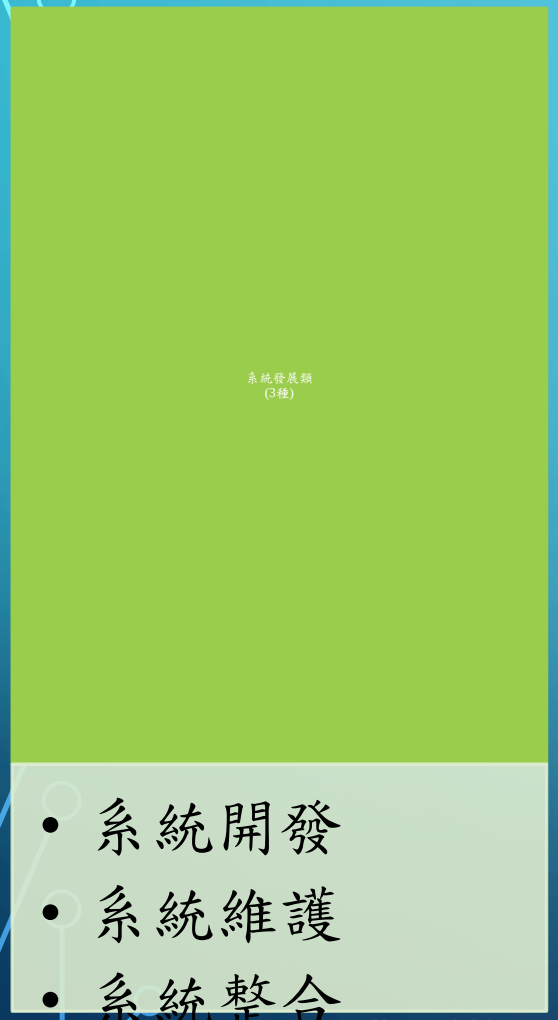
- 搜尋引擎：百度
- 電子郵件：網易郵箱
- 地圖和導航：高德地圖
- 線上購物：淘寶網
- 社交平台：新浪微博
- 視頻網站：優酷、bilibili
- 即時通訊：騰訊QQ、微信
- 電子支付平台：支付寶
- 雲端服務：阿里雲

資訊委外合約訂定與人員資格

依據

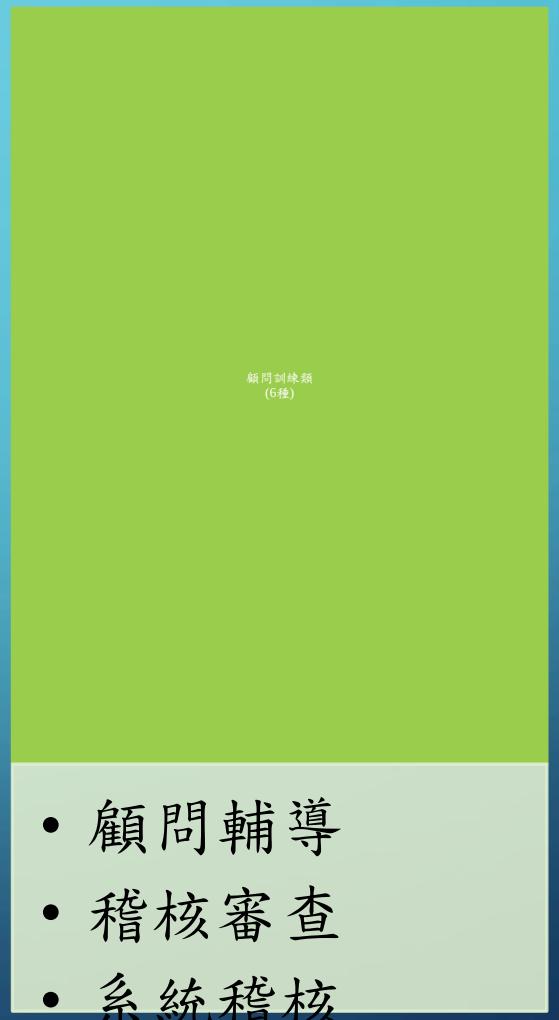
- 資通安全管理法
- 個人資料保護法
- 教育部民國110年06月18日臺教資(四)字第1100068264B號令頒「教育部委外辦理或補助建置維運伺服主機及應用系統網站資通安全及個人資料保護管理要點」
- 教育部國民及學前教育署 111 年度校園資通安全專責人員知能研習「委外合約的訂定與管理」

資訊委外類別與形態-4類22種型態

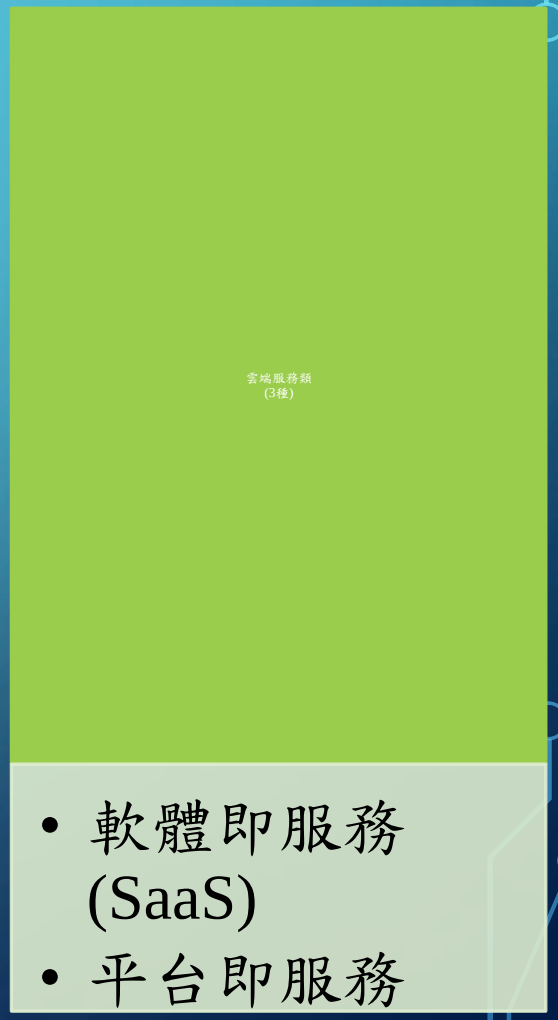


- 系統開發
- 系統維護
- 系統整合

- 設備操作、硬體維護、機房設施管理、備份與備援服務、



- 顧問輔導
- 稽核審查
- 系統稽核
- 軟體驗證



- 軟體即服務(SaaS)
- 平台即服務(PaaS)

系統發展類

系統開發

- 依機關規格需求，開發一套應用系統程式，並於開發完成後，進行測試、訓練、製作技術文件及上線之專案。
- 其作業範圍包括：新系統開發設計、舊系統汰舊換新、舊系統架構更改、系統移轉訓練及系統保固等工作 。

系統維護

- 應用軟體之維護服務與功能增修，包括軟體版本更新、應用程式錯誤與漏洞之排除及更正性服務等。

系統整合

- 提供一套完整解決方案(Total Solution)之資通系統，涵蓋範圍包含整合網路、通訊及硬體設備，加上訂製軟體(Tailormade Software)或套裝軟體，及新資通系統教育訓練等項目。

維運管理類(1/5)

設備操作

- 委由廠商派員操作其資源設備，並依一定程序處理產出報告。

硬體維護

- 購買硬體設備(如系統主機、終端機、工作站、個人電腦、印表機、繪圖機及連線設備等)於保固期限內，應由原供應廠商依購買時契約約定，提供各項售後服務，非屬硬體維護範圍。
- 在設備保固期滿後，為維持原硬體功能與正常運作，提供之定期維護合約工作。
- 惟部分機關考量經常門預算編列不易，將設備維護費用一併納入採購案中，保固期限由1年延長3~5年不等

維運管理類(2/5)

機房設施管理

- 指電腦設備、機房設施及機房相關業務，運用外界提供之專業技術，協助執行設施管理任務。
- 包含管理制度之規劃與執行，提供運作環境與軟硬體設備之規劃或管理等。

備份與備援服務

- 備援指機關透過本地端備用之儲存空間與設備、遠端備用儲存空間、設備與網路，保存重要資訊資產與恢復系統正常作業。
- 資訊委外之備援服務指廠商提供儲存空間、主機運算能力、網路頻寬及備援場所(含辦公場所)等方式，協助機關保存重要資產與恢復正常作業，有效降低資通系統無法運作之風險與成本及災害復原所投資成本，減低因人員操作疏失造成資料遺失，或系統遭受攻擊致系統網路無法運作等風險，並可縮短系統回復作業時間。

維運管理類(3/5)

網路與資安服務

- 網路服務包含提供機關外部網路連線服務、私有網路服務、其他網路加值服務(含系統與應用)。
- 資安服務包含「資安健診服務」、「資安監控服務」、「弱點掃描服務」、「滲透測試服務」、「社交工程郵件測試服務」、「行動應用App檢測」及「應用程式原始碼安全檢測」等服務。

網路管理

- 監控機關內部網路活動，含路由器、交換集線器、防火牆管理與網路流量分析及網路蠕蟲與病毒攻擊防護等服務，並提供問題診斷與產生各類網路活動統計資料，以協助機關之網路管理者維持網路正常運作。

維運管理類(4/5)

資料處理

- 協助電腦系統線上與批次作業之運作，將需要以電腦處理之工作，全部或部分由委外廠商以其自有設備，代為規劃、設計及處理，或派員前來操作機關之設備，按一定程序與程式處理產出資料者。

資料登錄

- 將機關之書面或微縮影片等原始文件，委外以人工作業方式輸入、校對、彙整及轉換，產出電腦可處理之電子媒體檔案者。

維運管理類(5/5)

整體委外

- 將全部或部分資通系統之整體運作，包含人員、環境設備、機器設施、作業程序、管理制度及其他相關或延伸之資訊委外管理。
- 系統管理服務之方式可以是機關自備設備，委外廠商提供管理服務；或設備與管理服務皆由委外廠商提供，機關擁有使用權等不同之方式。
- 工作內容含整體資訊管理制度規劃與建置，擬定資通系統運作方式與執行，由機關訂定服務水準指標，做為執行之要求與改善依據等工作。

人力支援

- 依機關所需技術能力採人力派遣或業務承攬方式供機關使用。

顧問訓練類(1/2)

顧問輔導

- 在特定主題範圍內，進行需求調查、相關資訊法規制度研擬、新技術導入可行性、資訊技術服務及訂定專案相關採購案件之規格研擬等，如ISMS導入。

稽核審查

- 為驗證管理程序或資通系統符合特定規範或標準而進行之專案，如政府機關之資訊安全管理系統(ISMS)第三方驗證。

系統稽核

- 為確保資訊單位內部作業資安控制機制，能有效建立並長期維持一定品質，協助評估並稽核資訊單位資安作業管制標準。

顧問訓練類(2/2)

軟體驗證

- 透過一連串具稽核功能之特殊程式，驗證資通系統運用與功能是否正確與符合原始需求，通常由公正第三方來執行。

教育訓練

- 協助機關於業務資訊化過程中，有關各階層人員常態性或專案性資訊教育訓練之規劃與執行。
- 訓練範圍可包含電腦軟、硬體技術、資訊管理技術、行政管理技術及資安等專業領域技術等。

整體規劃

- 在政府整體業務、跨機關業務或機關業務範圍內，進行政府整體、跨機關業務或機關整體資通服務需求彙整、網路與資訊技術架構規劃、訂定相關系統間資訊交換規格及相關配套措施之規劃等。

雲端服務類

軟體即服務(Cloud Software as a Service, SaaS)

- 透過網際網路提供軟體的一種服務模式，廠商將應用軟體統一部署在雲端伺服器上，客戶可透過瀏覽器使用服務，無須再購買軟體及更新維護。例如：Google DOCS、Microsoft Office Live等。部分政府機關或企業使用Google Gmail即為SaaS的一種服務模式。

平台即服務(Platform as a Service, PaaS)

- 廠商透過網際網路將雲端服務平台，如儲存設備、資料庫等開放給使用者，使用者可自行透過服務平台來部署應用程式及使用程式語言，無須管理或控制雲端設備，包含網路設備及伺服器。
- 例如：Google App Engine及Windows等。

基礎設施即服務(Infrastructure as a Service, IaaS)

- 廠商透過網際網路，以虛擬主機方式提供完整作業系統及資料庫存取，如AWS (Amazon Web Services)等 。

資訊委外原則(1/5)

- 委外辦理資通系統之建置、維運或資通服務之提供，應考量**廠商之專業能力與經驗**、委外項目之性質及資通安全需求，選任適當之廠商，並**監督其資通安全維護情形**。
- **涉及國家機密業務不宜委外**，惟若經評估仍須委外辦理，則執行廠商之相關人員應接受**適任性查核**，並依**國家機密保護法**之規定，管制其出境。
- 限制使用**危害國家資通安全產品**。
- 委外廠商辦理受託業務之相關程序及環境，應具備完善之**資通安全管理措施或通過第三方驗證**。
- 委外廠商應配置**充足且經適當訓練**、擁有**資通安全專業證照**或具有**類似業務經驗**之資通安全專業人員。

資通安全專業證照請參閱數位部資通安全署官網之**資通安全專業證照清單**
https://moda.gov.tw/ACS/laws/certificates/676

資訊委外原則(2/5)

- 委外廠商辦理受託業務時，得複委託之範圍與對象，及複委託之受託者**應具備之資通安全維護措施**，且應要求委外廠商對其進行管理，**包含一致性的資安與個資保護目標、執行風險評鑑等**。機關甚至可與委外廠商協商，出具監控管理報告。
- 受託業務包括**客製化資通系統開發者**，委外廠商應提供該資通系統之**第三方安全性檢測證明**。
- 該資通系統屬機關之**核心資通系統**，或**委託金額達新臺幣一千萬**元以上者，機關應自行或另行委託**第三方進行安全性檢測**。
- 涉及利用非自行開發之系統或資源者，並應**標示**非自行開發之內容與其**來源及提供授權證明**。

資訊委外原則(3/5)

- 委託關係**終止或解除時**，應確認委外廠商**返還、移交、刪除或銷毀履行契約所持有之資料**(含委外廠商交付複委託之資料)。
- 委託機關應**定期(或於知悉委外廠商發生可能影響受託業務之資安事件**時)，以**稽核或其他適當方式**確認受託業務之執行情形。
- 具**敏感性或國安(含資安)疑慮**之業務範疇，於**招標文件載明**不允許**投審會公告之陸資資通服務業者**參與。
- 應建立資安管理之**事前規劃、事中招標及事後執行**維運機制。

資訊委外原則(4/5)

- 視需要以顧問導入(如重要資訊專案)，考量資安需求，並經由**顧問標**、**規劃標**、**建置標**及**監督審驗標**等程序辦理。
- 擴大委外重要資訊專案經濟規模效益，各機關得整合其他相關需求一次委外，朝最適合之標案規模辦理。
- 應**透過公開徵求資訊**(Request For Information，RFI) **或徵求修正意見**(Request For Comments，RFC)等方式，廣納各界意見，據以訂定合宜的**徵求建議書文件**(Request For Proposal，RFP)**規格**。

資訊委外原則(5/5)

- **應用軟體宜與硬體分開招標**，並**先行辦理應用軟體招標建置**，如需合併於同一標案辦理，應由各機關視個案性質訂定應用軟體與硬體經費比例上下限，列入計價，納入評選計分，遴選出能提供最佳整體解決方案之廠商。
- 應將**應用軟體品質保證計畫**列為委外必要工作項目，並要求廠商依照**主管機關訂定之標準或規範發展系統**，確保軟體品質與政府資訊的流通互用。
- 廠商或團隊人員**通過軟體相關資格評鑑或管理能力認證**者，得列入評選加分項目
- 為確保委外服務績效，各機關應**落實監督、稽核及管控服務水準**，協助廠商溝通協調事宜，確保服務績效

資訊委外策略(1/2)

以政府機關採購招標觀點而言：

- **自行建構**、採購硬體或訂製軟體轉為**購買資通服務**
- 從**開立軟硬體規格**轉為**設定服務水準**(Service Level)
- 從短期與一次性購買關係轉為**中長期夥伴關係**
- 從重視**價格**轉為重視**價值**
- 從**解決個別問題**轉為**購買整體解決方案**

資訊委外策略(2/2)

- 視委外個案性質決定，將**資通安全需求所需費用**列入成本分析計價項目
  - 例如：Web資安檢測服務與報告
- 規劃過程
  - 將機關的**資安規範與對廠商**(含複委託廠商)**資安要求**納入【契約書或RFP】
  - 將【資通安全需求】納入RFP中，列為委外需求與評比必要工作項目
- 執行過程
  - 要求廠商**遵循主管機關訂定之標準或規範**執行，並提供可行建議方案，確保委外作業安全
- 因應【個資法/施行細則】之施行
  - 廠商(被委託機關)**增加多項義務與賠償責任**，建議機關在估算成本時應一併考量
  - 委託機關必須負起「監督」職責

資訊委外合約人員僱用(1/2)

人員篩選

- **委外人員背景查證檢核**：
  查證檢核時考量所有隱私權與個人資料保護等相關法令，參酌下列控制措施：
  - 是否有**合格的品格推薦信**或可諮詢的人員
  - 進用**人員的學經歷檢核**
  - 確認應徵人員**學歷與專業資格**
  - 獨立**身分檢核**，例如：護照或類似文件
  - 更詳細的核對，例如：**信用核對**或**犯罪紀錄**檢核(良民證)
- **定義查證檢核準則與限制程序**
  - 宜定義查證檢核準則與限制程序，例如：誰有資格篩選人員，如何、何時及為何執行查證檢核

資訊委外合約人員僱用(2/2)

- **保密切結書**
  - 為保障委外作業安全，宜針對參與廠商之作業員工，經由個人同意並簽署**僱用同意書**。該同意書陳述其與機關對資通安全的責任
- **僱用同意書**，反映機關**資安政策**
  - 被賦予敏感資訊存取權之委外人員，在被允許存取資訊處理設備前，先簽署**機密性或保密協議**
  - 委外人員**法定責任與權利**，例如：著作權法或個資法規定
  - 委外人員所**處置資通系統與服務**相關資訊分類及機關**資產管理之責任**
  - 委外人員**處理來自其他公司或外部團體資訊**之責任
  - 延伸至**機關外與正常工作時間外之責任**，例如：在家工作
  - 委外人員**違犯**機關**資安要求**時，所採取之行動
- 確保委外人員**同意機關資通安全條款與條件**，及其將會取得資通系統與服務之**存取權限範圍與限制**。

Solarwinds供應鏈攻擊事件

2023.04.14 資安相談室

引用網站： https://www.youtube.com/watch?v=UuYIc6vRyJM

個人資料使用與保護注意事項

依據

- 個人資料保護法
- 個人資料使用與保護注意事項

政府近5年資料外洩，最便宜只賣10歐元

天下雜誌 CommonWealth Magazine

政府重大個資外洩紀錄

外洩時間	2018/4	2019/6	2020	2022/10/21	2022/10/25
資料時間	2012年	駭客聲稱2019年	未知	2018/4	未知
事件	台北市政府衛生局市民個資外洩	銓敘部公務人員個資外洩	戶役政個資外洩	戶役政個資外洩	役政個資外洩
筆數	298萬	59萬	2000萬	2357萬	887萬
影響或後續	調查局**半年後**發布調查報告，同一天，**北市府發出公衛系統個資外洩公告。**	近7成公務人員個資在此次外洩，**爆發兩天內，銓敘部在網站上公告個資外洩，並向24萬餘人聯繫告知。**	行政院資安處在**爆發兩天內**發布兩次新聞稿，**表示外洩資料是由多個資料庫整併而成。**	事發4個多月，截至出刊前，**內政部尚未發布完整調查報告。調查局則證實，外洩資料為2018年4月以前的戶役政資料。**	截至出刊前，**政府未有回應。**
販售金額	29.8萬美元	10歐元	2500美元	5000美元	未知

研究整理：史書華
資料來源：行政院、內政部、調查局、銓敘部、台北市政府、BreachForums、RaidForums、Toogod

《天下》查證立委，證實被洩個資為真

天下雜誌 CommonWealth Magazine

2022年10月遭洩戶役政資料39欄位

姓名	**曾銘宗**（國民黨黨團總召）		
生日	1/22	**相關親屬**	本人、配偶、兒女
姓名	**謝衣鳳**（國民黨黨團書記長）		
生日	7/12	**相關親屬**	本人、父母、兄弟姊妹
姓名	**林思銘**（國民黨黨團首席副書記長）		
生日	3/16	**相關親屬**	本人、配偶、兒女
姓名	**賴香伶**（民眾黨黨團副總召）		
生日	1/5	**相關親屬**	本人、配偶、兒女
姓名	**邱顯智**（時代力量黨團總召）		
生日	4/29	**相關親屬**	本人、父母、配偶、兄弟姊妹、兒女

其他欄位

個人資訊： 身分證字號、性別、出生年、出生地、教育程度

特殊身分別： 原住民身分、原住民族別、役別

婚姻： 婚姻狀況、配偶名、配偶身分證字號

戶籍相關： 戶號、戶長姓名、戶長身分證字號、與戶長關係代碼、戶之區分

父母相關： 父名與身分證字號、母名與身分證字號、養父名與身分證字號、養母名與身分證字號

戶籍地址相關： 縣市、縣市代碼、地區、地區代碼、鄉鎮區、村里、鄰、地址、遷入日期

其他（無特殊含意）： id、SEREAL、SOURCENO

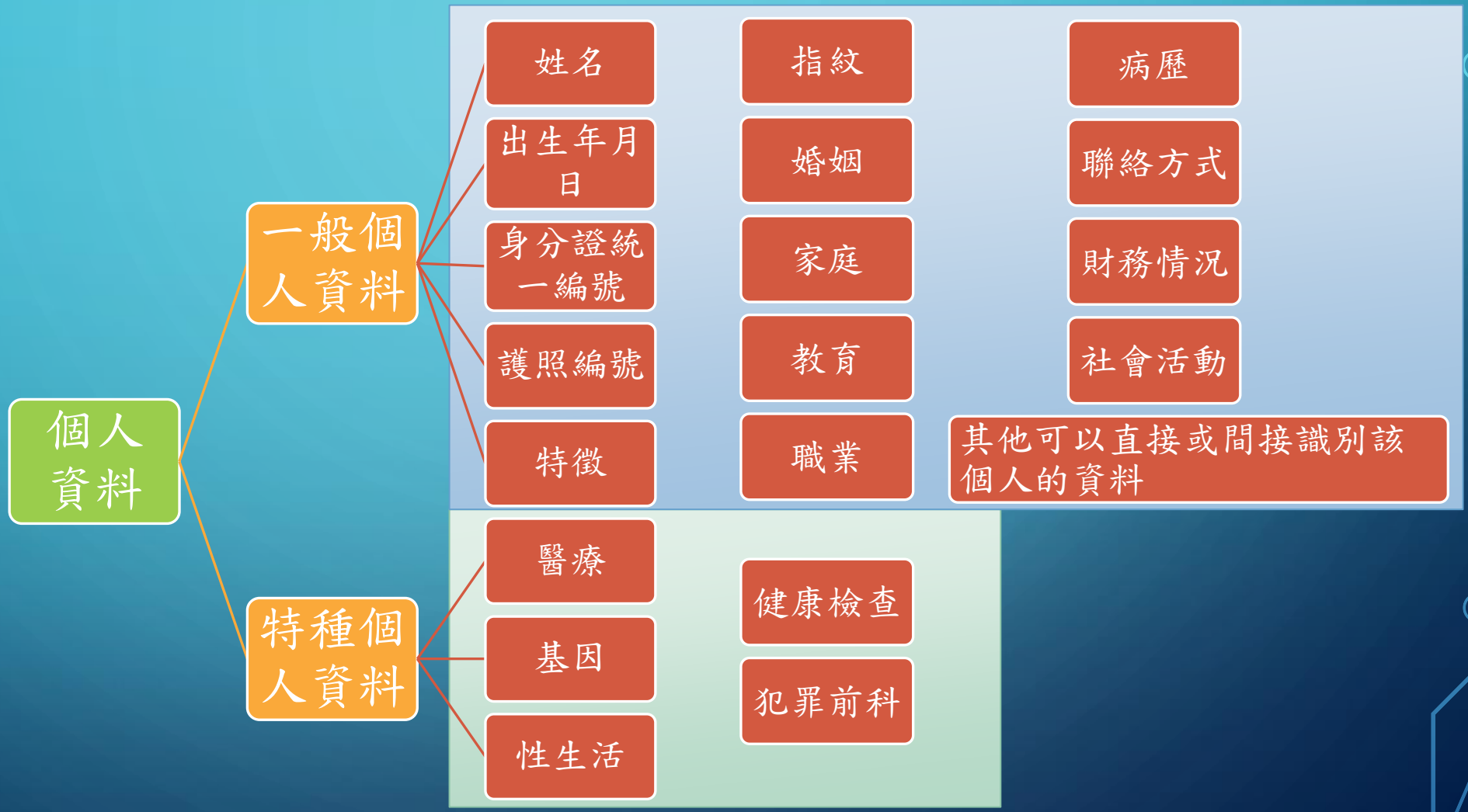
註：《天下》徵詢立法院民進黨團、國民黨團三長，以及民眾黨團、時代力量黨團兩名幹部共十名立委，是否願意以不涉隱私個資，協助證實資料真偽，表內刊出資訊皆獲本人同意。柯建銘、鄭運鵬、吳琪銘、張其祿、王婉諭截稿前未回覆或拒絕揭露。
研究整理：史書華、鄭閔聲　資料來源：BreachForums

華府2015年最嚴重個資外洩 關鍵100天危機處理

2023/3/8

資料來源：https://www.youtube.com/watch?v=mG0ev48u4QQ

個人資料



BCCS 漢昕科技股份有限公司
Business Continuity Computing System Inc.

校務行政相關的個人資料

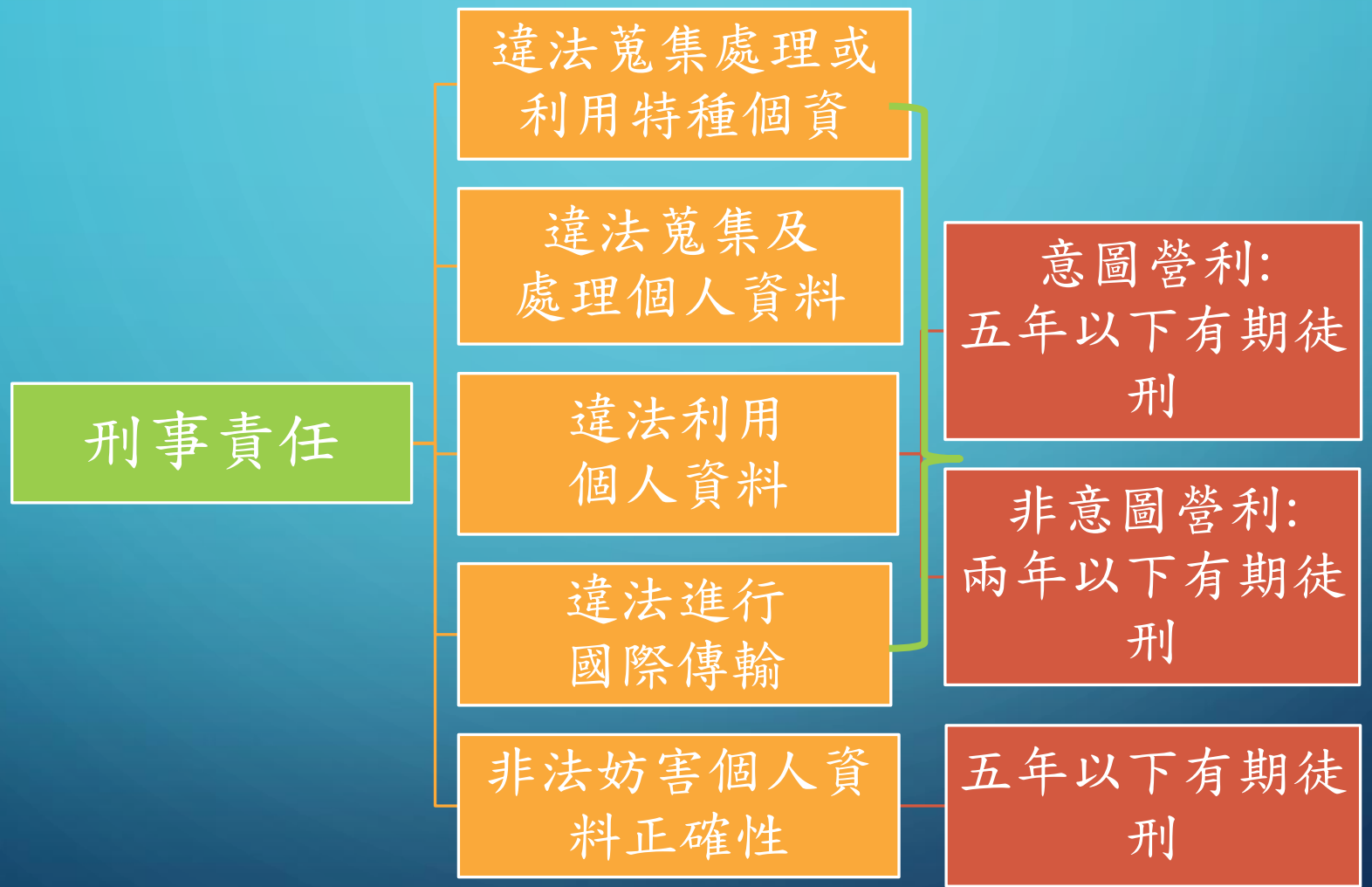
學生申請補助　教職員人事資料　獎懲及違規紀錄

家長聯絡方式　教職員出缺勤紀錄　學生基本資料

家庭狀況　病歷紀錄　健康檢查　清寒家庭身分

學生輔導紀錄表之AB卡資料　學生學業與操行成績資料

公務機關之法律責任



BCCS 漢昕科技股份有限公司
Business Continuity Computing System Inc.

公務機關之法律責任

公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(第44條)

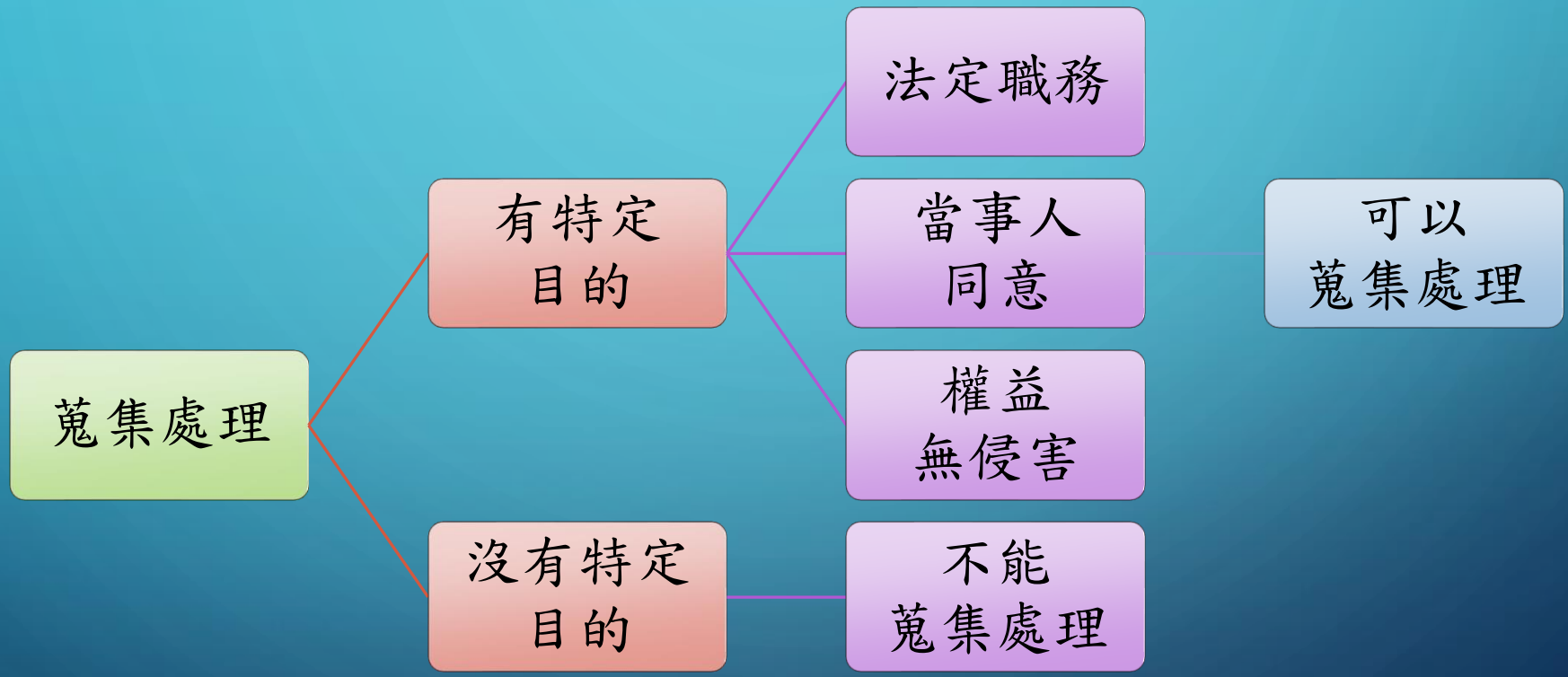
BCCS 漢昕科技股份有限公司
Business Continuity Computing System Inc.

個資法規範行為

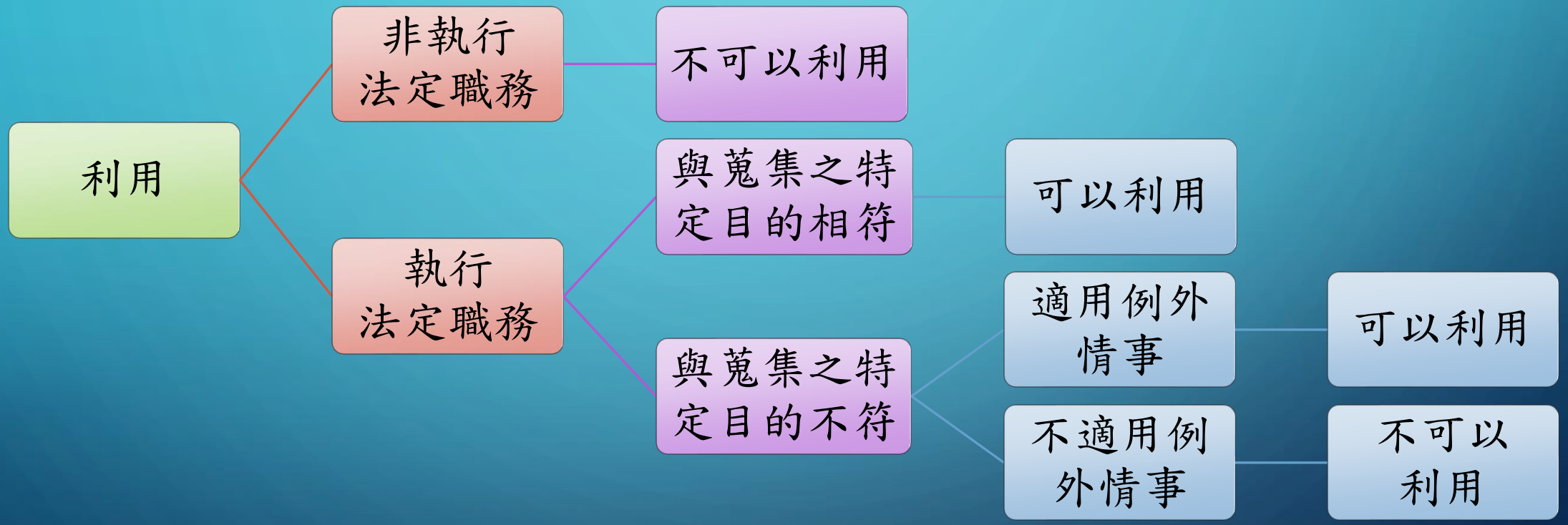
蒐集	• 以任何方式取得個人資料。
處理	• 為建立或利用個人資料檔案所為資料的紀錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
利用	• 將蒐集的個人資料為處理以外的運用。

BCCS 漢昕科技股份有限公司
Business Continuity Computing System Inc.

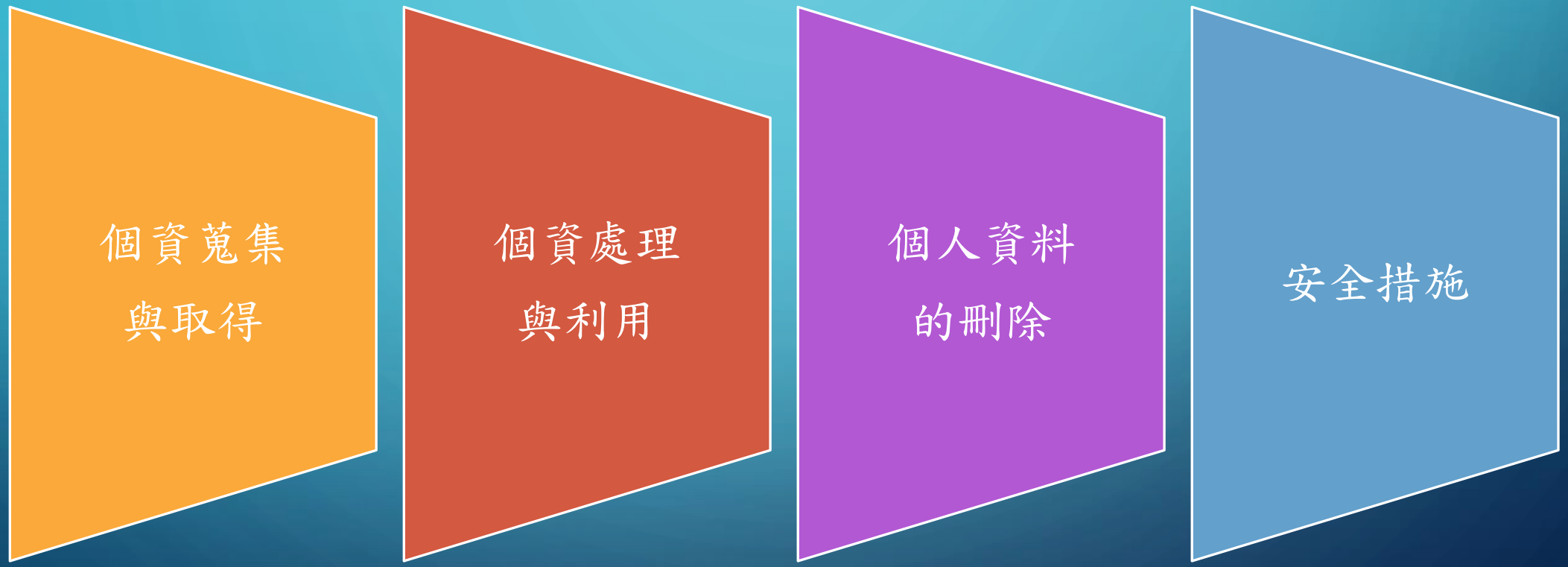
個人資料蒐集處理流程



個人資料利用流程


利用
非執行
法定職務
不可以利用
執行
法定職務
與蒐集之特
定目的相符
可以利用
與蒐集之特
定目的不符
適用例外
情事
可以利用
不適用例
外情事
不可以
利用

個人資料使用與保護注意事項



個資蒐集與取得

向個資之本人告知單位名稱、蒐集目的、資料類別、當事人權利、利用時間、地區、對象與方式、不告知的影響等。(依法令蒐集不再此限)

蒐集之個人資料時，單位承辦人員是否填具「D006-個人資料檔案複製、轉檔申請單」，經單位主管簽章同意，並檢附資料保密同意書。

個資處理與利用(1/2)

各單位保存之紙本個資文件妥須善收置可上鎖的櫃子內、檔案室或資料倉儲，勿放置個人辦公桌面或容易被取得之地點。

電子檔之個人資料須設定存取保護措施或限制存取人員，並對檔案進行加密保存或實施防拷貝機制，且定期盤點。

個資處理與利用(2/2)

內部傳遞或與其他機關交換個人資料時，應選擇可靠且具備保密機制之傳遞方式，如於實體文件封袋加上彌封、或對資料檔案壓縮加密，並對轉交或傳輸行為登記於「個人資料檔案文件遞送登記簿」，加以記錄流向備查。

因業務需要或應主管機關、產學合作或計畫等需揭露、轉移個資，除法律另有規定外，應將個人資料進行去識別化，如遮蔽部分姓名、部分身分證字號，或部分地址，以無法直接識別當事人為原則，如陳OO。

個人資料的刪除

資料已超過保存期限，或經由當事人主張，保存資料單位應主動銷毀。

當個資蒐集之特定目的消失、業務終止、保存期限屆滿，且無保存之正當性，應立即將個資檔案之刪除(電子檔案或資料庫型態個資)或銷毀（紙本、媒體）。

個資處理過程中因錯誤或其他原因(如暫存之檔案、印出之參考文件)，於事後需進行刪除或銷毀之個資檔案，應由資料保有及業務負責單位進行刪除或銷毀。

當事人權利行使

當事人如行使查詢等權利，各單位應要求其填具「個人資料權利行使申請表」或依學校相關業務申請辦法辦理申請。

如為代理人申請，則另需檢附委託書及出示相關身分證明文件。

查詢或請求閱覽、製給複製本(15日內准駁決定)、補充或更正、停止蒐集、處理或利用(30日內准駁決定)。

安全措施(1/3)

儲存個人資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。

儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。

處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，交接人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。

安全措施(2/3)

禁止人員使用即時通訊軟體傳輸個人資料檔案。
公用群組，傳輸資料應加密。

禁止人員使用外部網頁式電子郵件傳輸個人資料檔案。

應隨時清理個人電腦的資源回收筒，以確保已經刪除的個資不會因為遺留在資源回收筒未清理，而遭未經授權之使用。

可攜式電腦使用應以密碼保護，於使用完畢後應刪除電腦中暫存之個資。

安全措施(3/3)

外部團體在場、個人資料更新或維修電腦設備時，應指派專人在場，確保個人資料之安全及防止個人資料外洩。

禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。

儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。

教師網路上公告成績?

1. 資料範圍: 學號, 姓名 , 其他資料?
2. 公開, 需要帳號密碼?
3. 例子:
   ① 在學校的Moodle系統中(需帳號密碼), 公告修課學生成績(僅包含學號, 成績). 不違反個資.

   ② 在公開網路中(公開的Blog網站, 任何人皆可看見), 公告修課學生成績(學號, 姓名, 電話, 成績), 有違反個資法之嫌疑.

善盡個資保管之義務

- 教師對個資法應有的作為：
  - 辦公室電腦請設定密碼，非必要勿讓學生使用。
  - 學生資料系統及校務行政系統使用後，請記得登出，也勿將帳號、密碼記錄在電腦內。
  - 電腦安裝防毒軟體，並定期更新。
  - 學生的機敏資料使用後，非必要勿存放於公用電腦內，也不要上傳至網路上，避免造成麻煩。
  - 紙本資料(如：通訊錄)請妥為保管，勿流出。
  - 已過期的資料請確實銷毀(用碎紙機或撕碎後分段式丟棄)。

結論

- 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法執行，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。
- 在個資蒐集、處理、利用、儲存、傳輸、廢除過程中，建立適當保護措施，防範非法竊取、遺失和誤用等情事。
- 個資保護是組織全體人員應有的共識，需共同遵守。

簡報完畢

THANK YOU FOR YOUR ATTENTION