中華民國
臺灣警察專科學校
Taiwan Police College

資安通識教育訓練

莊瑞倫 Allen Chuang

BCCS 漢昕科技

本次教育訓練的目的?

- 對資訊安全應有之認知
- 瞭解各項資訊安全攻擊態樣和預防
- 了解新型資安防護
- 瞭解資訊安全威脅與重要性，及其保護的方法

- 何謂資訊安全
- 近期資安事件案例分享
- 常見的攻擊手法
- 虛擬貨幣簡介
- 新型資安漏洞
- 行動裝置與電腦資安防護建議

何謂資訊安全？

何謂資訊安全？

攻擊者動機:

- 認知作戰
- 竊取情資、網路間諜
- 個人、商業利益
- 報復行動
- 新手練功

何謂資訊安全？使用者為什麼成為目標?

- 竊取機密檔案/文件
- 針對性機密資料蒐集
- 線上遊戲、網路購物及網路銀行等服務之有價財產
- 部落格或社群網站之帳號密碼
- 跳板(殭屍電腦)
- 監控使用者行為
- 智慧型手機富含使用者個資(通訊錄、E-Mail等)

何謂資訊安全？

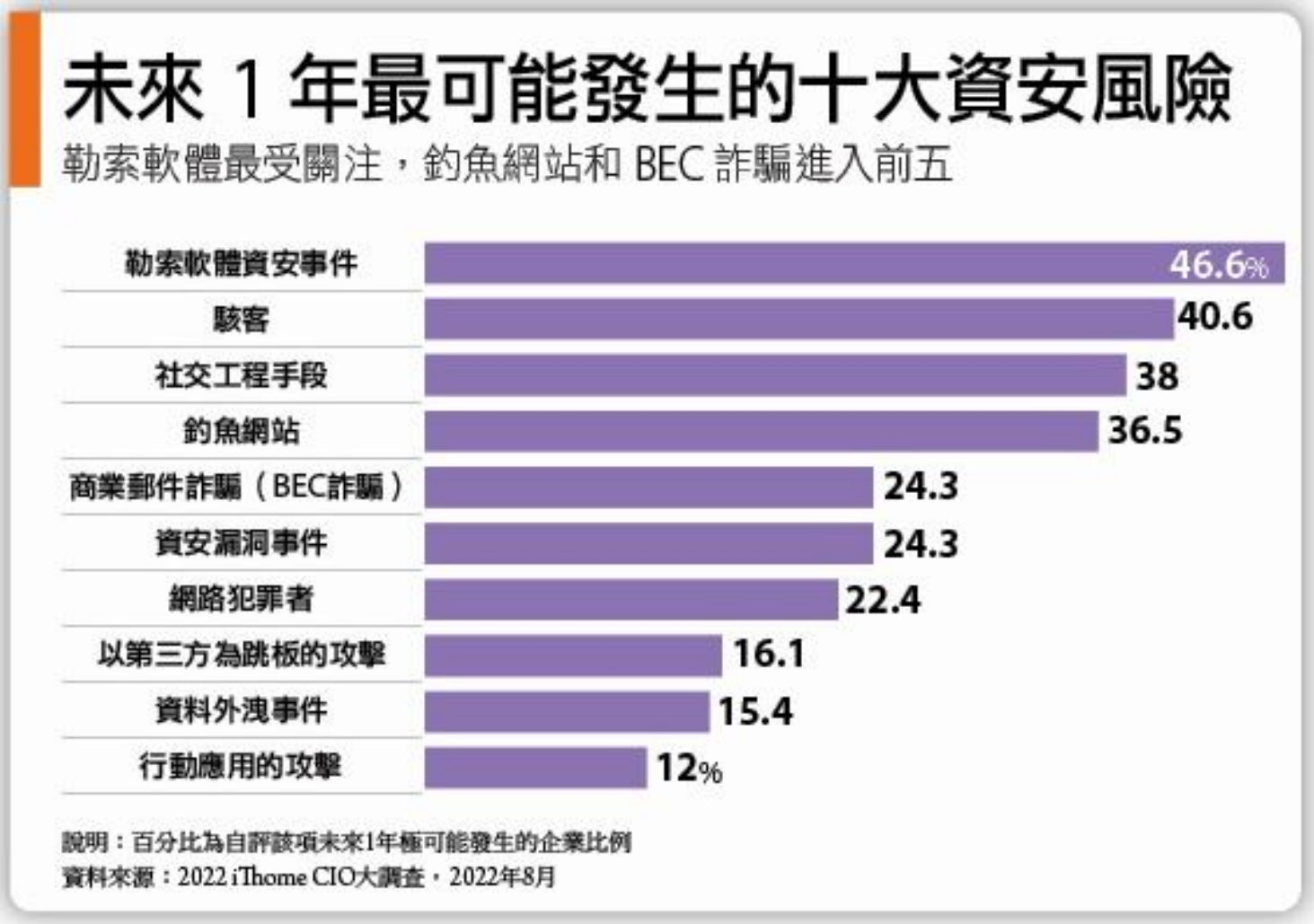
意為保護資訊及資訊系統免受未經授權的進入、使用、披露、破壞、修改、檢視、記錄及銷毀。

政府、軍隊、公司、金融機構、醫院、私人企業積累了大量與員工、顧客、產品、研究、金融資料有關的機密資訊，而絕大部分的資訊現在被收集、產生、儲存在電腦內，並通過網路傳送到別的電腦。

企業的顧客、財政狀況、新產品線的機密資訊落入了其競爭對手的掌握，這種資安性的喪失可能會導致經濟上的損失、法律訴訟甚至該企業的破產。保護機密的資訊是商業上的需求，而在許多情況中也是道德和法律上的需求。
對於個人來說，資訊安全對於個人隱私具有重大的影響，但這在不同的文化中的看法差異很大。

近期國內資安事件案例分享

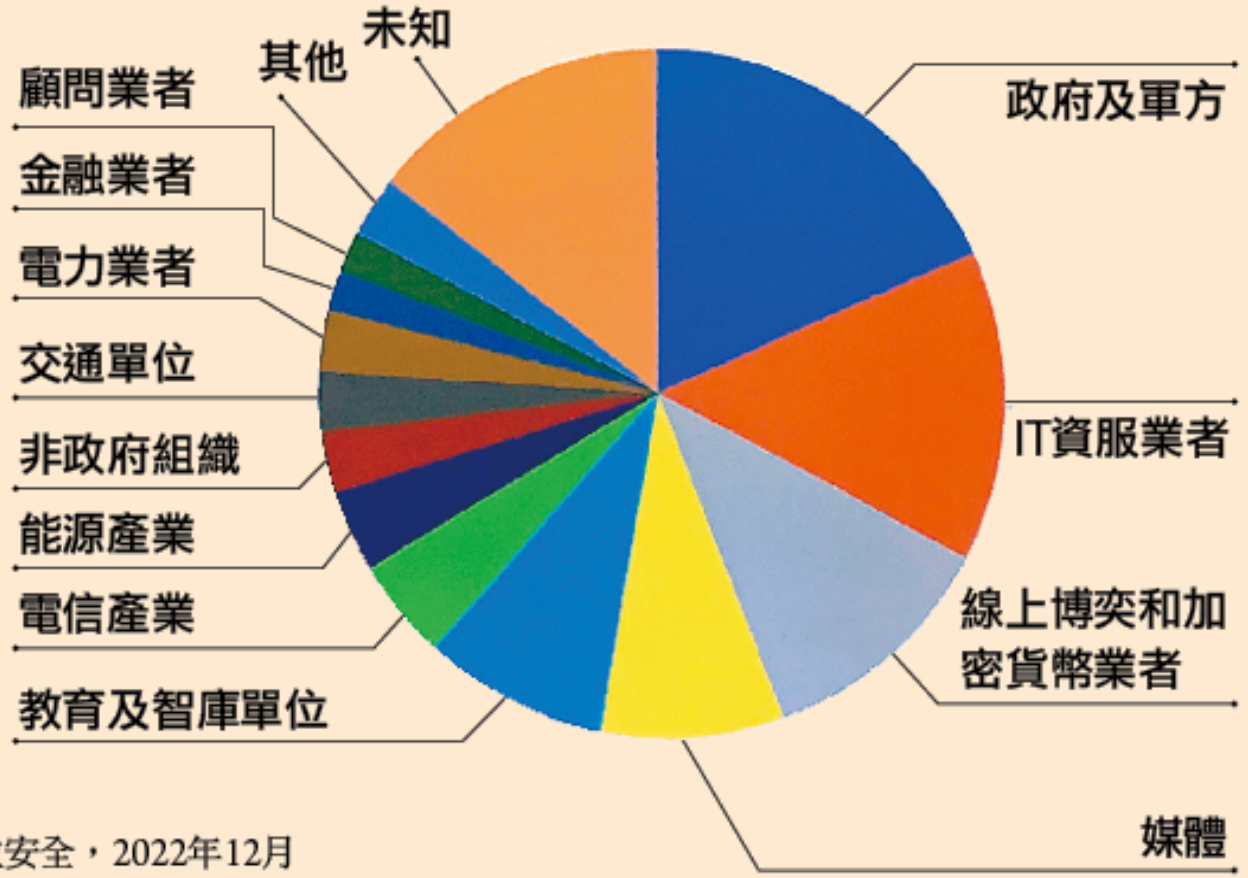
2022 資安危機


未來 1 年最可能發生的十大資安風險
勒索軟體最受關注，釣魚網站和 BEC 詐騙進入前五
勒索軟體資安事件 46.6%
駭客 40.6
社交工程手段 38
釣魚網站 36.5
商業郵件詐騙（BEC詐騙） 24.3
資安漏洞事件 24.3
網路犯罪者 22.4
以第三方為跳板的攻擊 16.1
資料外洩事件 15.4
行動應用的攻擊 12%
說明：百分比為自評該項未來1年極可能發生的企業比例
資料來源：2022 iThome CIO大調查，2022年8月

2022年臺灣APT攻擊研究分析

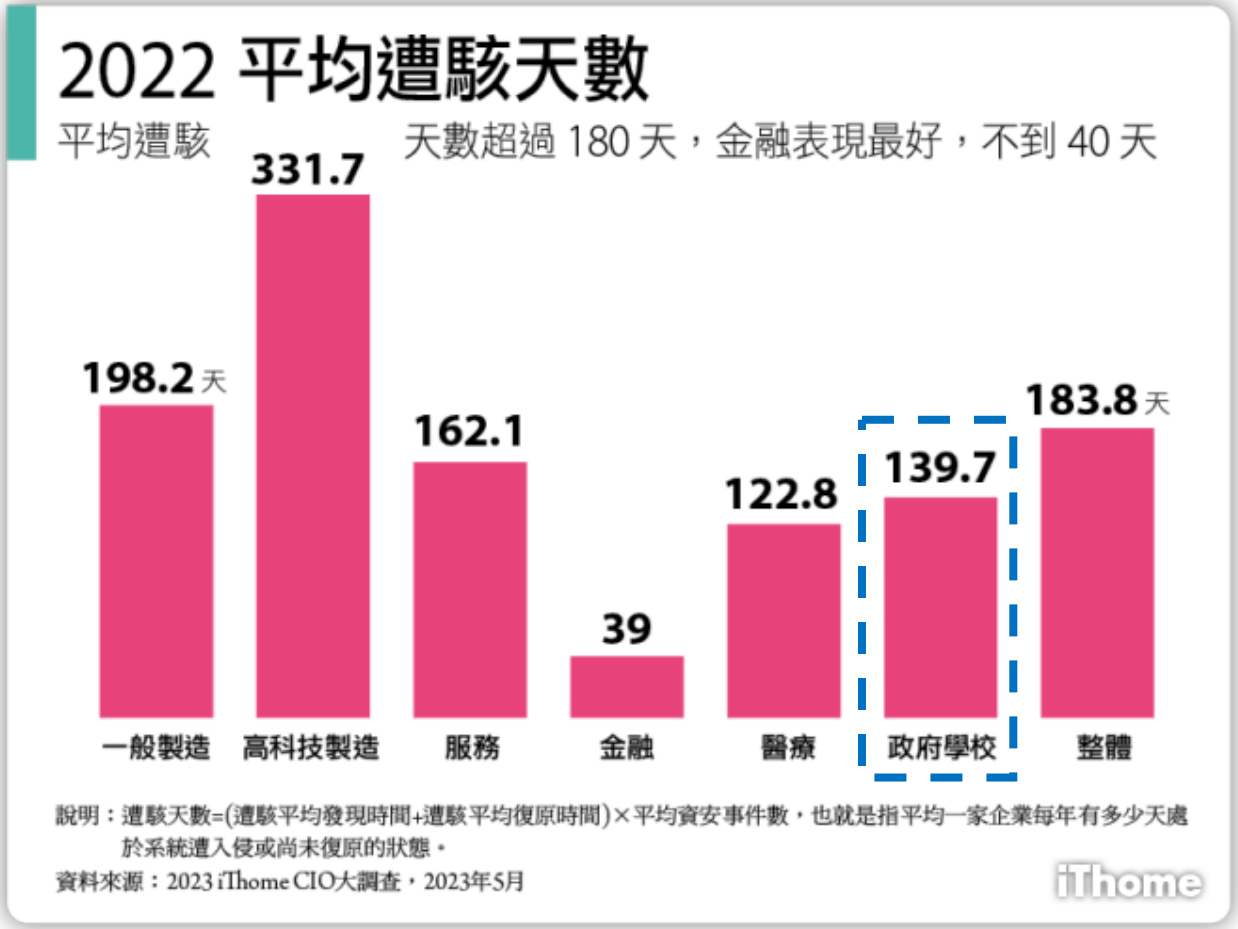
臺灣2022年政府軍方及資服業者受駭比例最高

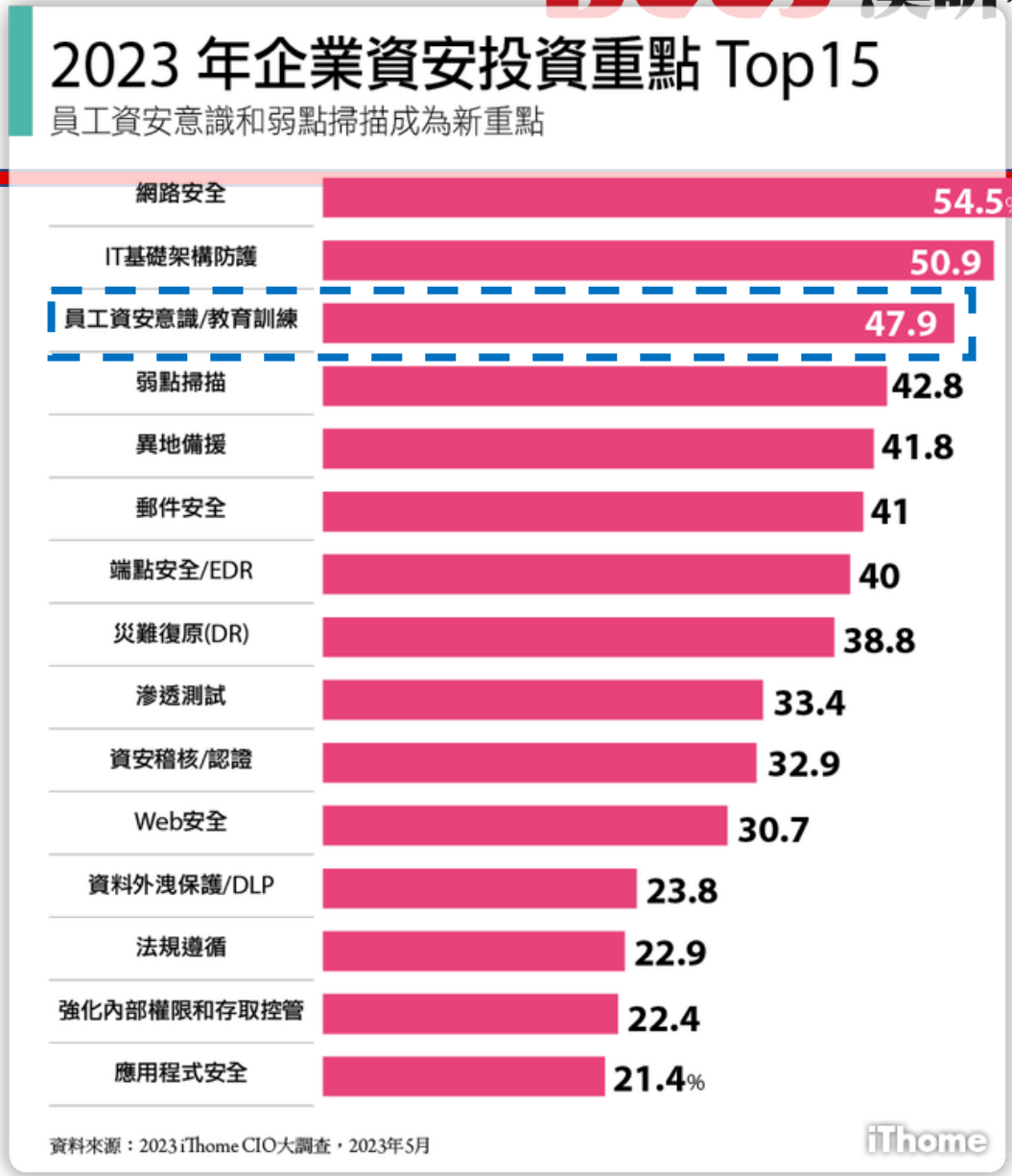
TeamT5杜浦數位安全技術長李庭閣表示，連續兩年來，政府和軍方是受攻擊主要對象，排名第二的資服業者，主要是被當作駭客攻擊的跳板，可以藉此發動供應鏈攻擊。



資料來源：TeamT5杜浦數位安全，2022年12月

近年資安危機


2022 平均遭駭天數
平均遭駭天數超過 180 天，金融表現最好，不到 40 天
198.2 天
331.7
162.1
39
122.8
139.7
183.8 天
一般製造
高科技製造
服務
金融
醫療
政府學校
整體
說明：遭駭天數=(遭駭平均發現時間+遭駭平均復原時間)×平均資安事件數，也就是指平均一家企業每年有多少天處於系統遭入侵或尚未復原的狀態。
資料來源：2023 iThome CIO大調查，2023年5月
iThome


2023 年企業資安投資重點 Top15
員工資安意識和弱點掃描成為新重點
網路安全 54.5%
IT基礎架構防護 50.9
員工資安意識/教育訓練 47.9
弱點掃描 42.8
異地備援 41.8
郵件安全 41
端點安全/EDR 40
災難復原(DR) 38.8
滲透測試 33.4
資安稽核/認證 32.9
Web安全 30.7
資料外洩保護/DLP 23.8
法規遵循 22.9
強化內部權限和存取控管 22.4
應用程式安全 21.4%
資料來源：2023 iThome CIO大調查，2023年5月
iThome

國內資安事件案例分享

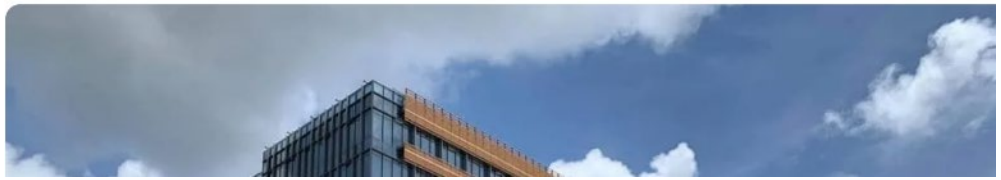
- 資料來源
https://tw.nextapple.com/finance/20221129/ED0F90B7619B481454A69B4521516792

驚傳遭駭客攻擊詐騙消費者！雄獅：已向調查局通報

財經 2022/11/29 16:05

加好友

【記者陳慦蔚／台北報導】雄獅（2731）網路驚傳遭駭客攻擊！公司今表示，駭客惡意攻擊電腦作業系統，並進而向近半年曾於雄獅購買相關旅遊產品的消費者進行詐騙，除已向法務部調查局通報協助外，也以同步委請外部資安公司技術專家共同處理，持續加強資訊安全管理。



雄獅說明，目前從不法人士詐騙手法研判，其不法利用的資料可能包括近半年購買訂房、機票、票券、證照等訂單資料，涵蓋訂單聯絡人姓名、聯絡電話及購買商品內容，但不包括旅客信用卡交易訊息。

雄獅強調，於發現遭駭客攻擊後隨即啟動內部資安相關防禦機制與應變作業，除已向法務部調查局通報協助外，並同步委請外部資安公司技術專家共同處理，並持續加強資訊安全管理。

國內資安事件案例分享

- 資料來源
https://udn.com/news/story/7315/6519354

刑事局公布詐騙高風險賣場 博客來、迪卡儂、誠品上榜

2022-08-07 15:40 聯合報／記者蕭雅娟／台北即時報導

讚 223 分享 分享

刑事局今公布今年第二季受理「解除分期付款」高風險賣場，包含博客來網路書店、迪卡儂、誠品網路書店等。警方指出，歹徒先竊取電商的消費者個資，再陸續假冒客服、金融機構人員，詐騙消費者，前五名民眾通報的高風險賣場均已宣導反詐騙，呼籲民眾慎防詐騙。

詐騙集團使用的話術為「工作人員操作錯誤，導致誤設分期付款、重複扣款或升級成VIP會員，要求客戶前往操作ATM、購買遊戲點數或使用網路銀行、App來解除設定」

警方分析詐騙手法，歹徒首先「駭入」電商或電商委託系統商資料庫，取得消費者個資，包含姓名、電話、消費資料及付款方式；緊接著「偽冒電商業者」客服人員，撥打客服電話給民眾，要求民眾提供消費時的信用卡、金融卡上的金融機構電話號碼。

國內資安事件案例分享

- 資料來源
https://news.ltn.com.tw/news/life/breakingnews/4147163

竊取個資、竄改給藥資料 衛福部桃園醫院遭中國駭客攻陷

桃園醫院被爆採用中國系統，導致資安後門大開。（資料照，本報合成）

2022/12/07 19:10

〔記者鄭淑婷／桃園報導〕衛福部桃園醫院資訊系統被爆採用中國系統，從2020年8月起陸續發生遭駭客入侵，竊取病患個資、醫護資料，植入惡意程式等，更出現醫療錯誤資訊，危害到病患安全，桃園醫院早於2020年2月即與系統商昱誠智能服務股份有限公司結束合約，但目前仍採用這套系統，只是改由自行維管，全案已報請警方、調查局偵辦中；桃園醫院今天發布聲明指出，前年確實有發現駭客入侵事件，但僅有1台主機遭受影響，主機內無個資，並無病人個資外洩疑慮，至今也無任何個資外洩情事，非如爆料內容所言。

國內資安事件案例分享

• 資料來源
https://news.ltn.com.tw/news/society/breakingnews/4180017

健保署3人被控查洩個資13年 疑涉國家情報工作

衛生福利部中央健康保險署傳出健保被保險人個資外洩案，檢調兵分多路搜索及約談，9日晚間將已退休的健保署前主秘葉逢明移送台北地檢署複訊後，以被告身分晉獲諭回。（記者羅沛德攝）

2023/01/10 06:51

〔記者錢利忠／台北報導〕衛生福利部中央健康保險署驚傳有「內鬼」外洩民眾個資！已退休的健保署前主秘葉逢明、在職的健保署承保組科長謝玉蓮、承保組職員李仁輝等3人，被健保署內部職員檢舉，涉嫌從內部系統偷查民眾的健保個資；台北地檢署指揮調查局新北市調查處兵分5路搜索健保署及3被告住處，原依可處3年以下徒刑之刑法洩漏或交付國防以外機密罪偵辦；不過，謝女於今凌晨4時許訊後，被改依違反「國家情報工作法」諭令10萬元交保，案情急速升溫。

據了解，謝女被檢調查出，她偷查的健保個資被害人中，疑似包含了警察、調查官、移民署官員等可能涉及國家情報工作法所規範的「情報機關人員」，因而涉及「刺探或收集」國家情報資訊等罪嫌，不過尚缺乏洩漏或交付給包括中國在內等敵對勢力的事證，暫時僅止於「偷查」，才諭令她10萬元交保。

國內資安事件案例分享

- 資料來源
https://www.businesstoday.com.tw/article/category/183027/post/202302150040/

從華航到iRent都被「駭」 資安危機事件一演再演.....
40天四起個資外洩 中小企業資安拉警報

成立邁入第9年、已奪下台灣共享租車龍頭的iRent，日前意外爆出40萬消費者個資遭洩，公路總局依《個資法》開罰20萬元。

月底，和泰集團旗下共享汽車品牌iRent，被爆出四十萬名消費者的個資遭外洩，舉凡消費者的姓名、手機號碼、身分證、住家地址、駕照照片，通通被駭客揭露。iRent後續聲明表示，由於暫存資料庫沒有完整阻擋外部連線，導致被駭客使用特定工具及技巧進入。

然而，這已是今年僅過不到兩個月以來，第四起個資外洩。一月中，掌握台灣兩千三百萬人健康資料的健保署，爆發官員盜賣民眾個資；同一個禮拜，華航也被踢爆會員資料外流，包括副總統賴清德、名模林志玲的個資都外洩，二月上旬，格上租車也發生訂單資料流出。

國內資安事件案例分享 • 資料來源https://udn.com/news/story/123309/6989196

udn / 產經 / 強化資安

微風遭駭 90萬用戶個資外洩

2023-02-23 00:48 經濟日報／記者林淑、馬瑞璿、何秀玲／台北報導 + 資安

日前有人在駭客論壇聲稱竊得微風百貨的內部資料，微風表示，近日收到匿名網路勒索信件，第一時間立即啟動損害機制，目前內部資安團隊已完成軟體及作業系統安全性更新。記者曾學仁／攝影

微風集團遭駭概況

事發經過	有人在駭客論壇BreachForums聲稱，竊得微風百貨內部資料
微風因應措施	1.近日收到匿名網路勒索信件，第一時間啓動損害機制 2.目前內部資安團隊已完成軟體以及作業系統安全性更新，同時提高資安防護層 3.經內部清查確認，外流個資與公司資料庫有所落差，因此駭客未必是從微風駭入

資料來源：採訪整理　何秀玲／製表

圖／經濟日報提供

國內資安事件案例分享

2022年10月21日，以「OKE」為代號的匿名使用者，在駭客論壇BreachForums兜售號稱全台2300萬筆戶役政資料。為了吸引顧客買單，OKE更直接公開20萬筆設籍在宜蘭的個資當作商品樣本。

其中包含39個欄位，從個人生日、性別、身分證號等資訊外，戶號、戶長，甚至是生父生母、養父養母都有單獨欄位和對應的身分證號。

[影片欣賞]

國內資安事件案例分享

威秀影城個資外洩！詐騙集團對資料「一字不漏」

投訴人是威秀影城會員，今（2023）年2月25日上網訂購電影票，後續卻接到自稱「威秀影城會計」的女子來電，稱該筆消費誤刷20筆，公司會將重複扣款的款項為款給會員，並要求投訴者提供銀行存簿帳號，甚至會補償500元補助金作為會員點數，可消費折抵。

投訴人與對方核對個人資料，包括姓名、生日、電話、身分證字號、16碼信用卡卡號、有效年月皆正確，但他仍覺得有異，因此未將存簿帳號提供給對方；事後他向銀行確認，信用卡正常並無重複扣款情形，當下打給看電影的威秀影城，接電話的主管表示「公司訂票系統遭到入侵，導致50萬名會員個資外洩，公司已在官網公告」。

國內資安事件案例分享

誠品書店個資外洩

誠品書店近日陷入個資外洩爭議，「台灣佇遮計畫」副祕書長楊欣慈於誠品網購書籍《阿共打來怎麼辦》，沒想到竟接到自稱是誠品回訪的詐騙電話，甚至對其屢出統戰言論，稱「您買的這本書很敏感」「統一台灣勢必發生」等。對此，5/16 數位部數位產業署也會同資安院與警方前往誠品生活實地行政調查

國內資安事件案例分享

疑個資外洩！統聯旅客遭詐騙

統聯客運資料庫疑遭駭，傳出部分旅客接獲詐騙，甚至有學生存款因此消失只剩下92元，統聯緊急關閉官網與App，進行資安調查，迄今仍未開放，統聯客運表示，資安調查尚未出爐，本周末前訂票系統仍將預防性關閉，車站和超商可購票取票。公路總局則表示，統聯訂票系統開放暫無時程表。

日前有民眾接獲假藉統聯客運名義的詐騙電話，告知系統出錯重複刷20張票，且還有消費者手機號碼和真實訂單資訊；另還有學生在統聯臉書上留言，指他省吃儉用存下4萬元，一個小時全不見，只剩92元存款。

國內資安事件案例分享

BCCS 漢昕科技

當日重大訊息

中華

公司當日重大訊息之詳細內容

本資料由 (上市公司) 2204 中華 公司提供

序號	2	發言日期	112/07/24	發言時間	06:47:59
發言人	錢經武	發言人職稱	副總經理	發言人電話	03-4783191
主旨	本公司發生網路資安事件				
符合條款	第 26款			事實發生日	112/07/23
說明	1.事實發生日:112/07/23 2.發生緣由:部分資訊系統遭到惡意攻擊 3.處理過程:自偵測到部分資訊系統遭到惡意攻擊，資訊部門已全面啟動相關防禦機制與復原作業，並與外部資安專家協同處理。 4.預計可能損失或影響:目前正積極進行復原，對公司營運影響尚在釐清中，後續視情況更新訊息。 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:本公司於查知網路異常狀態後，立即啟動資安相關防禦機制與應變作業，並進行復原工作，本公司將持續提升網路與資訊架構之安全管控，以確保資料安全。				

7月24日中華汽車於股市公開觀測站發布重大訊息，表示部分資訊系統遭到惡意攻擊，該公司資訊部門啟動防禦機制，並進行復原作業，協同外部資安專家後續處理，而對於營運帶來的影響，該公司表示尚在釐清。根據民視新聞的報導，有資安專家認為，此起事故很有可能是駭客勒索事件，並指出中華汽車已出現部分產線停工的情況，現正全面針對相關系統及設備進行檢修。

而對於本次事故發生的原因，有資安專家推測，可能是因為資訊部門在系統整修或更新期間，為便於遠端連線操作，短暫關閉防火牆而釀禍，駭客趁機入侵並取得控制權，並索討高額解鎖費用。截至目前為止，該公司尚未出現個資外洩的跡象。

個資法修法

2023年到現在，台灣已經發生至少15起資安事件，像是：華航的電商平台發生異常後傳出會員資料遭竊、微風廣場收到匿名勒贖信件後客戶資料外洩、威秀影城發生顧客個資外洩、宏碁資訊委外權限遭竊導致產品資料外洩.....。立法院在5月16日三讀通過《個人資料保護法》部分條文修正案，針對近期多家企業發生的個資外洩事件提出舉措。

1. 修正個資法第48條非公務機關違反安全維護義務之裁罰方式及額度，改為逕行處罰同時命改正，並提高罰鍰上限，**處新臺幣（下同）2萬元以上200萬元以下罰鍰，若是情節重大者，處15萬元以上1,500萬元以下罰鍰。屆期未改正者，按次處15萬元以上1,500萬元以下罰鍰**。
2. 第二，增訂個資法第1條之1規定，由個人資料保護委員會擔任個資法主管機關。行政院將積極推動設置個資保護獨立監督機關，以呼應去年8月12日憲法法庭第13號判決，要求3年內完成個資保護獨立監督機制之意旨，解決目前個資法分散式管理下之實務監管問題，並與國際趨勢接軌。

台灣已成國際資安攻防熱區

台灣因地緣政治與區域鄰近性，經常遭受各種新式資安攻擊，已是國際資安攻防熱區，據統計，台灣政府機關每月平均受到3000萬次以上的境外網路攻擊、各組織去年每周遭攻擊3118次。

問題一，企業缺乏資安意識及社會責任，不願投注更多經費，組建專職資安團隊、更新設備、加強防禦。
美國最大金融服務機構摩根大通，2019年就宣布，未來每年斥資6億美元添購設備、更新軟硬體、招募資安人才，以因應駭客威脅。
據IThome統計，台灣大型企業2022年資安投資，平均每家企業預算僅新台幣715萬元，即使政府機關和金融業的預算稍高，平均亦僅約兩千多萬元。即使如台積電、玉山金、聯發科等「優等生」，去年宣布斥資上億台幣強化資安，亦難達一呼百應之效。
與國外企業相較有巨大懸殊，證明許多台灣企業未將防駭視為己任。
雖然數位部積極幫助政府機關導入T-Road資料傳輸機制，但公部門人員未改變習慣採用T-Road機制，老是採用傳統的USB、燒光碟傳輸資料，導致有心人士從中攔截資料甚至外洩；政府在完善政府機制、立法、資安人才培養、要求企業當責上，皆未採取積極行動。

台灣已成駭客天堂

問題二：政府無鐵腕 個資外洩企業未受懲處
台灣也未曾有企業因個資外洩遭受嚴峻懲處。
例如iRent此次個資外洩，導致40萬人的手機、電郵暴露於風險中，儘管該公司已致歉並以時數折抵券慰問用戶，但政府僅要求限期改正，否則依個資保護法處新台幣2萬元以上、20萬元以下罰鍰。

相較之下，2019年，英國航空曾因個資外洩，遭英國官方判處年營收1.5%、高達1.83億英鎊、約新台幣64億元罰金。當時英國資訊委員會（ICO）主席Elizabeth Denham公開指出，企業未保障個資免於損失、 毀損或被竊，法律必須明確要求企業克盡職責，失職者將面臨嚴格審度。
安永管理顧問公司總經理萬幼筠指出，歐美是依營收按比例懲處，讓廠商心生警惕，「台灣個資外洩罰個20萬，購買一個功能最簡易的企業資安防護軟體要50萬，難怪企業不會把錢花在資安上。」
萬幼筠說，個資到處外洩，勢必引爆經濟市場大災難，政府之責就是該指導、防護、管理並責成企業。
未來戰爭主打「混合戰」（融合傳統、政治、網路和不對稱作戰），當美國、中國大陸、歐洲、烏、俄都在拚「資安軍備競賽」，台灣資安還得補破網，個資外洩後的一連串惡性循環與外溢衝擊，正要發酵。

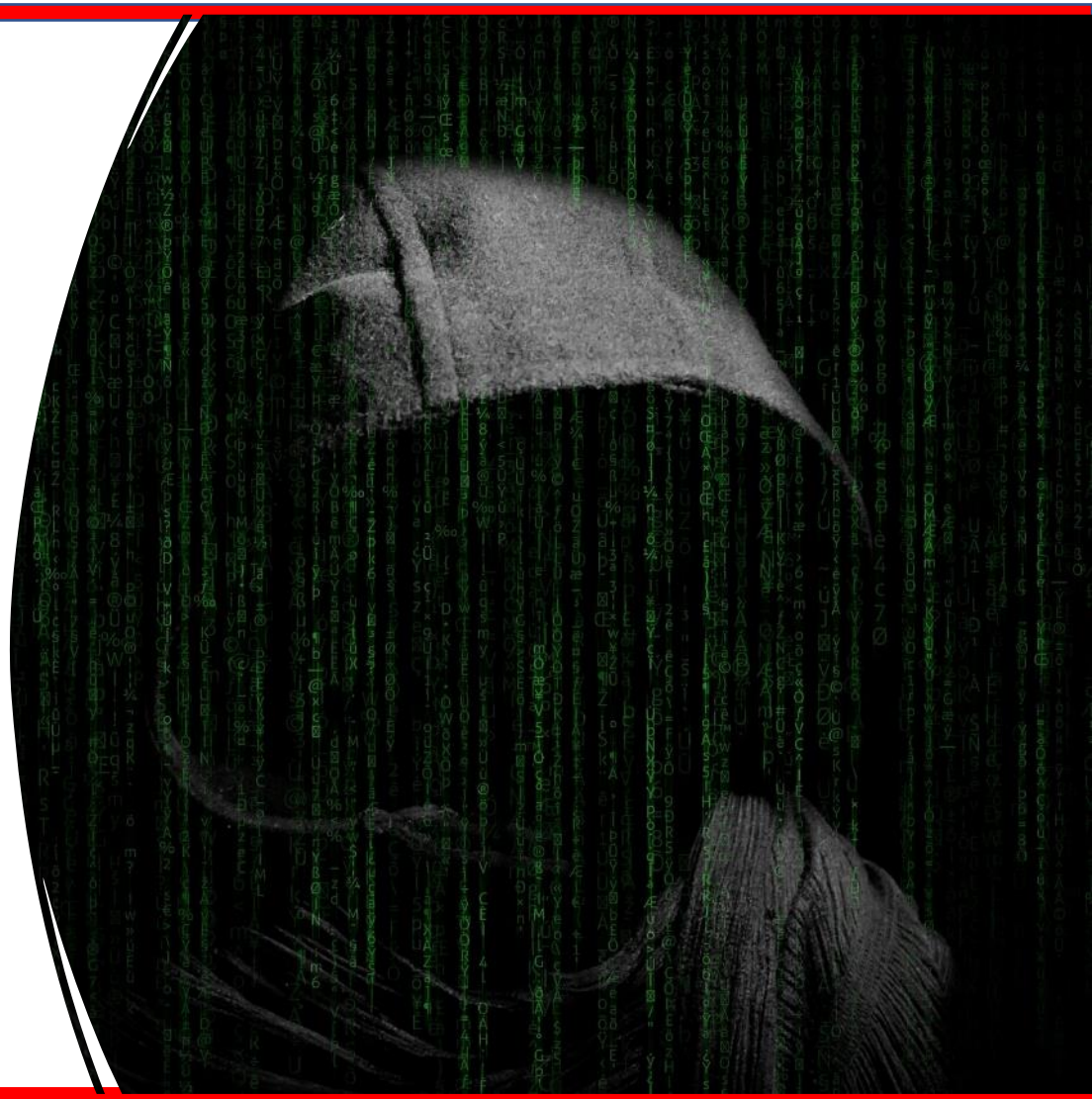
影片欣賞

常見的攻擊手法

駭客常見的攻擊手法

實際上駭客常用手法:

- 文件中夾帶惡意巨集病毒
- Cookie竊取
- 物聯網攻擊
- 分散式阻斷服務攻擊（DDoS）
- 網路釣魚（Phishing）
- 點擊劫持（Clickjacking）/ 介面偽裝（UI redress）
- 中間人攻擊（Man-in-the-middle attack）
- 跨網站指令碼攻擊（Cross-site scripting，XSS）
- DNS 欺騙（DNS spoofing）
- 水坑攻擊（Watering hole）
- 鍵盤側錄器攻擊（Keylogging）
- 暴力攻擊（Brute force）/字典攻擊
- 社交工程
- 進階持續性滲透攻擊（Advanced Persistent Threat, APT）



常見的攻擊？

文件中夾帶惡意巨集病毒:

- 文件中隱藏的惡意巨集是一般人不會特別注意的惡意軟體，但其實這種惡意病毒很容易察覺。Excel 或 Word 等文件都能製作巨集，打開文件後能執行巨集中的指令碼，但通常打開文件時，會提示需要用戶授權才能使用巨集功能。如果您允許文件執行巨集，巨集中的指令碼可以在系統中打開許多漏洞，讓駭客上傳更嚴重的惡意軟體來控制您的電腦。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

Cookie竊取:

Cookie是當你瀏覽網路時會儲存在你裝置上的小型文件檔案。它們被用來儲存你的偏好、登錄資訊及其他敏感資料等資訊。Cookie就像是瀏覽器在你瀏覽網站時所作的小筆記，用來提供流暢的瀏覽體驗。

儘管cookie可能很有用，但就和會儲存你個人資訊的其他東西一樣，cookie也可能帶來一些問題，例如：

1.隱私問題：Cookie中儲存了登錄資訊或個人資料等敏感資訊，如果遭到駭客攔截就可能導致隱私洩露。這會帶來如身份盜用或金融詐騙等嚴重的後果。

2.安全漏洞：Cookie可能會遭受漏洞攻擊，進而危及使用者資料安全。

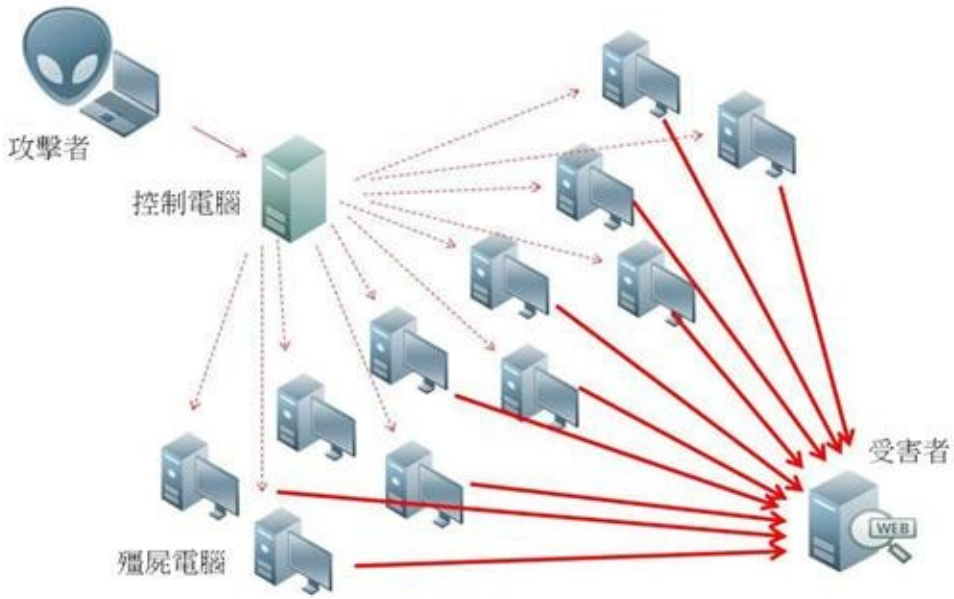
3.過時資料：隨著時間推移，cookie可能會過時或無效，這可能會導致瀏覽器出現非預期行為或在存取資訊時出現錯誤。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

分散式阻斷服務攻擊（DDoS）:

- 分散式阻斷服務攻擊又稱DDoS攻擊，這是一種常見的網路攻擊手法。執行這些攻擊的惡意程式不會傷害受感染的設備，而是將這些設備組成殭屍網路，在短時間內發動大規模的攻擊，藉此耗盡資源和頻寬，造成服務癱瘓。駭客可以透過惡意程式或網站感染許多設備，並控制這些設備向目標網站發送大量請求，導致目標網站不堪負荷而中斷服務。

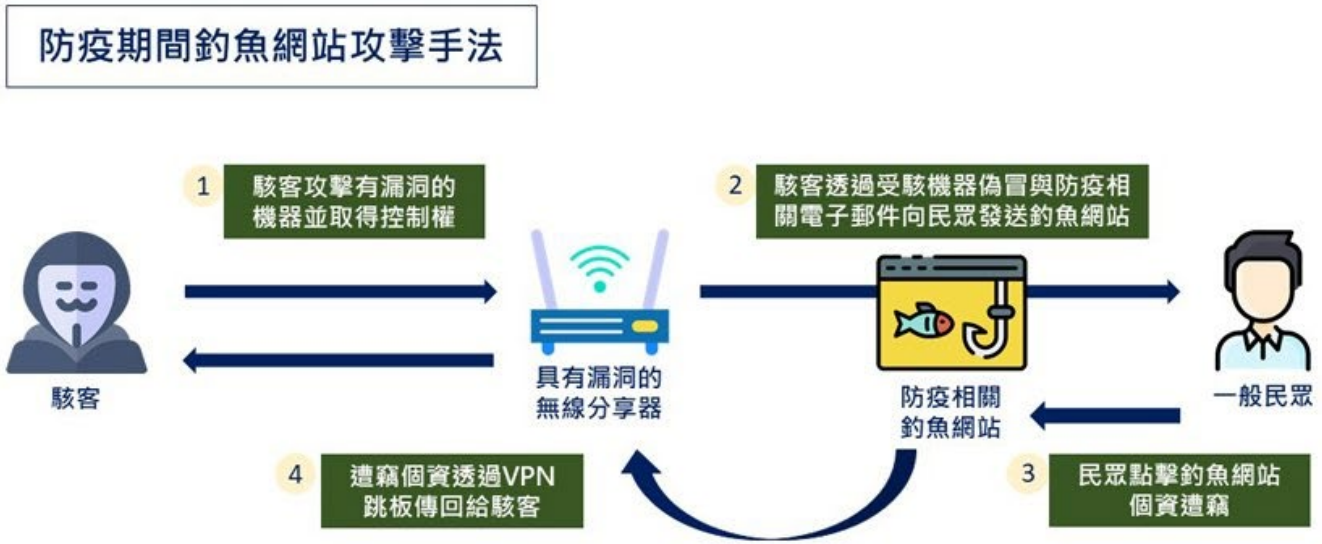


圖片來源:凌群電子報

常見的攻擊？

網路釣魚（Phishing）：

- 與大多數駭客攻擊不同，網路釣魚的目標是設備的用戶，而不是設備本身。這種攻擊經由一封精心設計的電子郵件來欺騙受害者，誘導受害者打開郵件上的惡意網站連結或郵件上的附件，讓受害者的設備受到感染，進而竊取設備上的機密資訊。

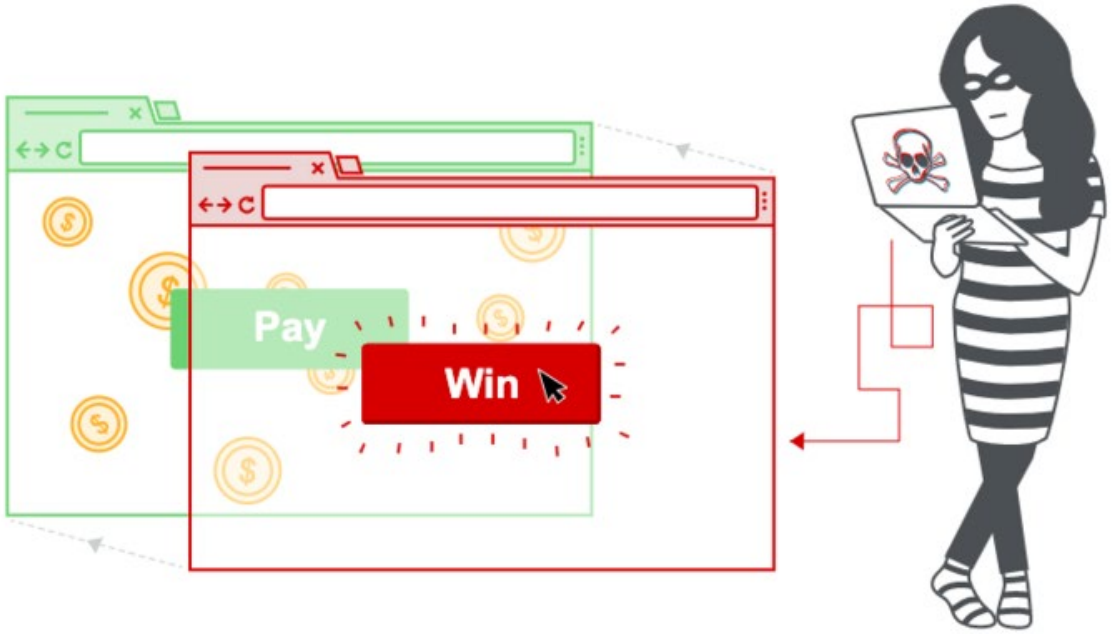


圖片來源:刑事警察局

常見的攻擊？

點擊劫持（Clickjacking）/ 介面偽裝（UI redress ）:

- 許多用戶可能在瀏覽網站時，沒有注意到它其實是惡意網站，或者是合法網站被入侵後成為惡意網站。這些網站看似正常的網頁上，隱藏著看不見的框架或按鈕，引誘用戶點擊或誤觸，有些攻擊甚至可以追蹤用戶的滑鼠和鍵盤行為。用戶執行的任何一次點擊都是在執行某種他們不知道的動作。



資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

中間人攻擊（Man-in-the-middle attack ）：

- 中間人攻擊（ MITM）又稱為竊聽攻擊，攻擊者在用戶和網站之間，將自己作為一個隱形的中間人。一但攻擊者攔截流量，就能監控並竊取資料，甚至可以在不被察覺的情況下竄改內容。

- 中間人攻擊有很多不同的手法，最常見的方法是引誘受害者連上駭客自己的 Wi-Fi 熱點或入侵公用 Wi-Fi 熱點（假冒無線熱點攻擊），就能輕鬆扮演中間人角色，竊取受害者的機密資料。

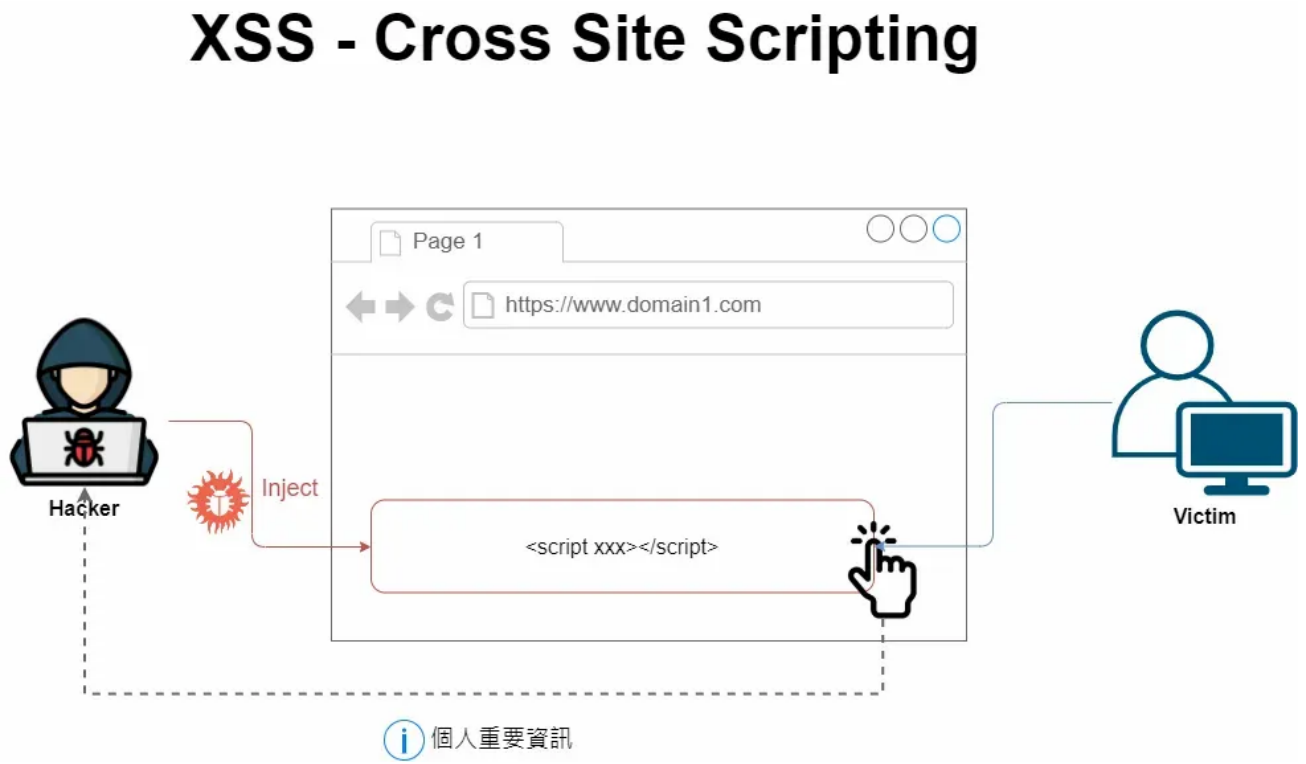
影片欣賞

常見的攻擊？

跨網站指令碼攻擊（XSS）：

- 網站通常會連結不同的服務以強化各種功能。例如不必每次交換資料時都要重新進行身份驗證。這些連結可能包括廣告服務或特殊插件。

- 如果網站中的某個連結被駭客入侵，攻擊者可以將惡意程式碼直接注入到網頁上，進而讓瀏覽網站的用戶受到影響。這些程式碼可以竊取用戶登入網站的資訊，或者執行不同類型的攻擊，例如點擊挾持。

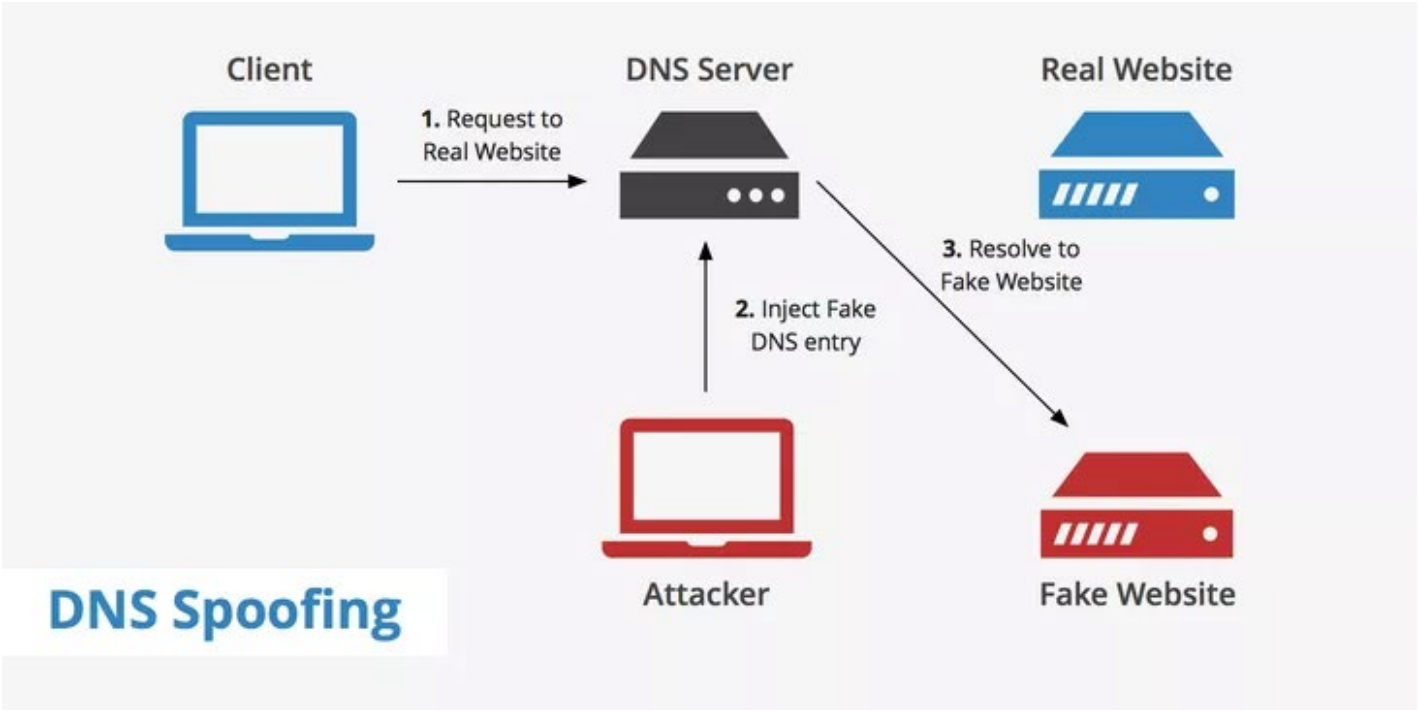


資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

DNS 欺騙（DNS spoofing）：

- DNS欺騙是指攻擊者冒充功能變數名稱伺服器的一種欺騙行為。攻擊者通過入侵DNS伺服器、控制路由器等方法把受害者要訪問的目標機器功能變數名稱對應的IP解析為攻擊者所控制的機器，這樣受害者原本要發送給目標機器的數據就發到了攻擊者的機器上，這時攻擊者就可以監聽甚至修改數據，從而收集到大量的信息。
- 例如讓DNS伺服器解析銀行網站的IP為自己機器IP，同時在自己機器上偽造銀行登錄頁面，那麼受害者的真實賬號和密碼就暴露給入侵者了。



圖片來源:iT邦幫忙

資料來源https://wiki.mbalib.com/zh-tw/DNS%E6%AC%BA%E9%AA%97

常見的攻擊？

水坑攻擊（Watering hole ）：

什麼是水坑式攻擊呢？水坑式攻擊是一種網路攻擊的策略。當攻擊者想要攻擊特定族群（組織、公司、地區）時，攻擊的流程會分成三個階段。
1. 先觀察或猜測特定族群使用的網站。
2. 利用惡意程式嘗試入侵這些網站。
3. 最後當特定群組的成員來瀏覽這些被入侵的網站時就會被感染。

就像非洲的大草原上，獅子在水池附近等待來喝水的動物一樣。駭客會先觀察攻擊目標習慣瀏覽那些網站，鎖定這些網站後開始入侵並植入惡意程式。等攻擊目標瀏覽該網站就有可能被感染。

資料來源https://scitechvista.nat.gov.tw/Article/c000003/detail?ID=1ff276c2-e39b-4f31-a2f8-a5d1872c95bb

常見的攻擊？

鍵盤側錄器攻擊（Keylogging）：

- 鍵盤側錄器會秘密擷取鍵盤上敲擊的按鍵，受害者不會察覺打字內容被側錄。窺探者透過鍵盤側錄器、軟體或硬體記錄用戶輸入的數據來完成這項工作。然後，就可以輕易竊取密碼和其他機密資料。

- 雖然鍵盤側錄器本身並不違法，但駭客卻能將其用於非法目的。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

暴力攻擊（Brute force）：

- 在暴力攻擊中，駭客嘗試猜測密碼、PIN 碼或加密金鑰。駭客透過這種攻擊手法，可以存取受保護的服務和資料庫，或者解密資料。

- 駭客使用的軟體每秒會嘗試大量密碼組合，直到猜測正確密碼為止。因此，如果您的密碼規則很簡單，這類軟體只要幾秒就能破解密碼。然而，破解複雜密碼則需要幾年的時間。

2022

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	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

GIF

› Learn about our methodology at hivesystems.io/password

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

字典攻擊:

- 字典攻擊是一種暴力攻擊手法。不同之處在於字典攻擊，駭客使用預定義的密碼清單。字典中有時包含常用的密碼短語，有時可能包含所有字典條目。

- 駭客在編輯詞典時通常會進行敏銳的研究。他們可以分析用戶的社群媒體檔案和其他公開可用的資料，找出寵物、親戚和興趣的名字，讓字典更準確。基本上，字典攻擊是暴力攻擊更具自訂性和針對性的變體。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

社交工程(1/3):

- 社交工程 (Social Engineering) 係利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破個人、企業或政府機關的資通安全防護，遂行其非法的存取、破壞行為。

常見的攻擊？

社交工程(2/3):

- 社交工程 (Social Engineering) 係**利用人性弱點**，應用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破個人、企業或政府機關的資通安全防護，遂行其非法的存取、破壞行為。

- 社交工程攻擊(Social Engineer)過程重現

影片觀賞

常見的攻擊？

社交工程(3/3):

- 常見的社交工程攻擊方式如下：
  1.利用電話佯裝資訊人員，騙取帳號及通行碼。
  2.偽裝委外廠商之維護人員或上級單位人員，乘機騙取帳號及通行碼。
  3.利用電子郵件誘騙使用者登入偽裝之網站以騙取帳號及通行碼，如網路釣魚。
  4.利用電子郵件誘騙使用者開啟檔案、圖片，以植入惡意程式、暗中收集機敏性資料。
  5.利用提供工具、檔案、圖片為幌子，誘騙使用者下載，如偽裝的修補程式、p2p 下載軟體、工具軟體等，乘機植入惡意程式、暗中收集機敏性資料。
  6.利用通訊軟體，偽裝親友來訊，誘騙點選來訊中之連結後中毒。

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

常見的攻擊？

APT攻擊:

- 簡單的說就是針對特定組織所作的複雜且多方位的網路攻擊。APT 進階持續性滲透攻擊(Advanced Persistent Threat, APT)可能持續幾天，幾週，幾個月，甚至更長的時間。APT攻擊可以從蒐集情報開始，這可能會持續一段時間。它可能包含技術和人員情報蒐集。情報收集工作可以塑造出後期的攻擊，這可能很快速或持續一段時間

- (APT攻擊:一場沒有中立國的戰爭(真實案例模擬))

影片觀賞

資料來源https://nordvpn.com/zh-tw/blog/heike-gongji/

BCCS 漢昕科技

虛擬貨幣簡介

虛擬貨幣

1. 虛擬貨幣是什麼？
2. 加密貨幣有哪些？
3. 加密貨幣種類、特色、風險？

虛擬貨幣是什麼？

- 虛擬貨幣（英文：Virtual currency），又稱「數位貨幣」，是一種數字貨幣，也就是沒有實體的貨幣。它適用於互聯網，且多數以「中心化」交易的形式，由中央政府或是大型機構發行、管理與控制。

虛擬貨幣有哪些種類？

- 虛擬貨幣大致上可以分為以下三種。其中都有些微的差別，但卻都屬於虛擬貨幣的一種。

1. **由政府發行的虛擬貨幣**：它大多是以法定貨幣的電子形式呈現，像是：網路銀行帳戶裡所顯示的數字 / 金額。
2. **由大型企業、機構所發行的虛擬貨幣**：像是：蝦幣、P幣、街口幣、LINE POINTS、OPEN POINTS...等，能在網路世界中所使用的虛擬貨幣（多數為機構的平台幣）。
3. **「去中心化」的加密貨幣**：雖然多數虛擬貨幣，是以中心化的形式，被政府、機構所控制。但像是：比特幣、以太幣、狗狗幣...等，進行過加密的虛擬貨幣，都不同於一般虛擬貨幣，它們擁有去中心化的特性。

BCCS 漢昕科技

加密貨幣是什麼？

加密貨幣（英文：Cryptocurrency），又稱「密碼學貨幣」、「密碼貨幣」，是一種利用區塊鏈密碼學技術，進行過**「加密」**的虛擬貨幣。而最早期的加密貨幣為「比特幣」，它是由一個叫「中本聰」的人 / 團體（因為這是一個筆名，所以我們無從得知他是一個人，還是一個團體。）在 2008 年所提出的概念。

快速理解公式：

加密貨幣 = 密碼學 + 虛擬貨幣

加密貨幣原理

✓由於加密貨幣是去中心化的，沒有第 3 方的協助，**因此需要透過「挖礦」的過程，來進行計算並維持運行**。這裡分成 3 個部分解釋：

- **提出交易**：當 A 要將加密貨幣轉帳給 B 時，一筆交易被提出。
- **進行計算**：礦工（指挖礦的人，通常是電腦設備）這時候發現有新區塊，並開始交易進行計算與驗證。
- **交易完成**：交易驗證完成後，礦工會將交易紀錄添加到區塊鏈，並更新交易記錄；同時，礦工也會獲得加密貨幣，作為挖礦的獎勵。

由此可知，加密貨幣原理是一種互惠的過程：提出交易的人，無須第 3 方即可完成交易；礦工則是透過驗證交易，而獲得獎勵。

加密貨幣特性

- **加密貨幣特性：**

✓底層技術為區塊鏈

區塊鏈技術的形成，一開始是為了比特幣（第一個加密貨幣）而製造出來的。而現在所有的加密貨幣基本上都需要依靠區塊鏈技術才能運作。

✓去中心化

區塊鏈技術中，有著去「中心化」的特質。而這使加密貨幣無需中央銀行或政府等第三方協助，就可以完成交易。

加密貨幣特性

✓無法篡改、更改

區塊鏈是一種共享數據庫。它允許數據庫中的數據分佈在不同位置的多個網路節點之間（ 如果駭客要入侵，就必須駭每個節點，這幾乎不可能達成 ）。而幾乎所有的加密貨幣，包括比特幣、 以太坊 ...等，都通過區塊鏈網路獲得「保護」和「驗證」。

> 如果有人試圖在數據庫上更改交易記錄，也毫無用處。因為其他節點並不會被篡改、更改。

加密貨幣特性

✓透明化

由於區塊鏈的 去中心化 特質，加密貨幣網路上的每一筆交易，都是以區塊鏈的形式公開發布。也就是說，「只要你想要，你可以隨時隨地都可以查看任何一筆交易」。

使交易變的相當透明化，防範了許多我們時常監督不到的行為（ ex. 貪污、 詐騙 ..等 ）。

虛擬貨幣、加密貨幣差別

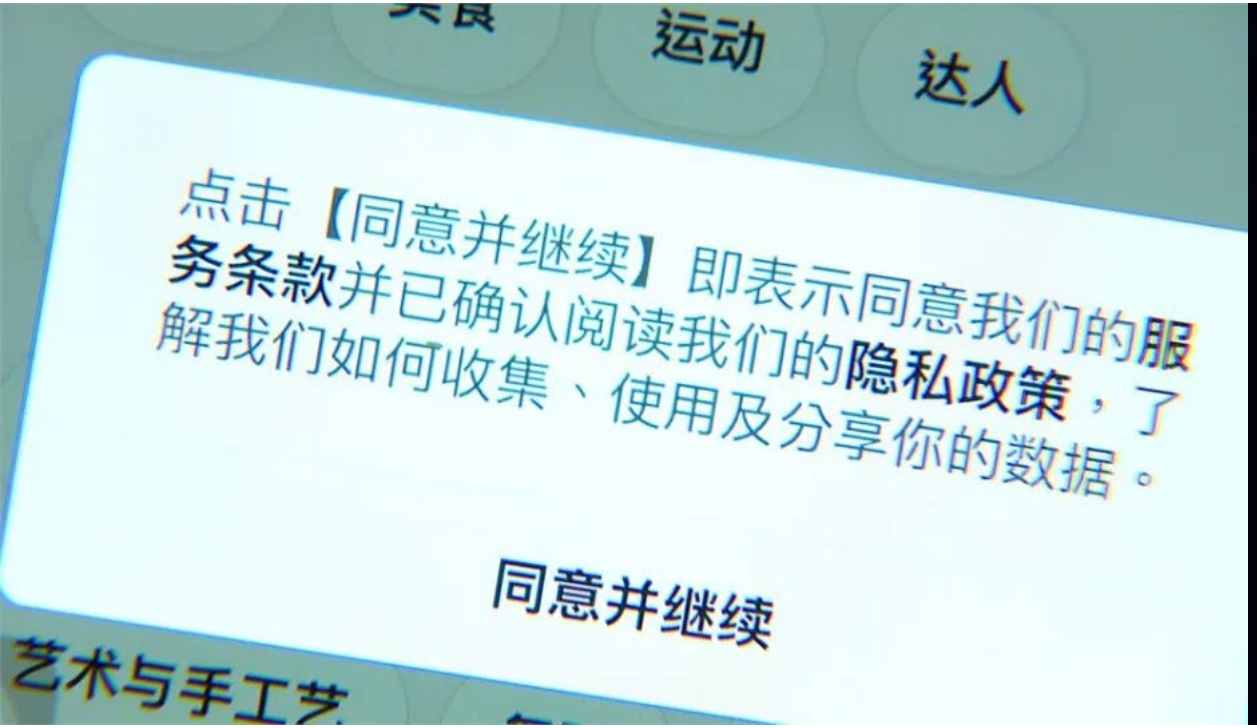
	虛擬貨幣	加密貨幣
管理模式	中心化（受第 3 方監管、控制）	去中心化（不受任何監管、控制）
保護方式	強密碼、生物識別驗證（指紋、臉部等）	密碼學加密
使用場景	多為法定貨幣的電子形式	多為交易、投資與價值儲存
發行數量	無限量發行（由政府、機構決定與控制）	有限量發行（少部分沒有）
存放方式	銀行機構、個人持有	區塊鏈
數據儲存	非透明化（可能被人為竄改）	透明化（無法被竄改）
價格取決	符合政府或法規價格（穩定）	取決於市場價格（波動較大）

影片欣賞

BCCS 漢昕科技

新型資安漏洞

新型資安漏洞？(以抖音為例)



當你點選同意，就等同你可能把所有的數據讓APP取用

新型資安漏洞？(以抖音為例)

- ✓在3月23日美國舉辦了國會聽證會，TikTok的首席執行官周受資面歷經超過四個半小時長的問訊。
- ✓聽證會舉辦緣由，2022年底眾多記者遭到不當監控，包含金融時報記者克里多（Cristina Criddle），以及曾服務於網路媒體BuzzFeed、現為富比世記者的貝克懷特（Emily Baker-White）、舒瓦布（Katharine Schwab）、尼瓦（Richard Nieva）等人。
- ✓金融時報的克里多，則自2022年6月起持續追蹤抖音倫敦辦公室的勞動問題與離職潮。她的報導指出，有員工一天工時高達12個小時，有人因為請育嬰假而遭降職，還有人透露抖音高層有一份「死亡清單」，希望逼退名單上的員工。

- TikTok2020年全球的下載量約為八億次。那麼現在呢？根據應用分析公司Sensor Tower稱，目前它的下載量為35億次。

新型資安漏洞？(以抖音為例)

1. TikTok 收集「過多」的數據？

其中包含收集使用者資料的應用程式，包括擊鍵模式和節奏、IP位址、移動運營商、時區設置、設備型號和作業系統以及臉部辨識等生物識別以及聲紋。

相關的應用程式還收集使用者的年齡、用戶名、電子郵寄地址、密碼、電話號碼和位置。它還收集消息的內容、消息的發送、接收和閱讀時間以及發送者。它還收集支付資訊，包括支付卡號、帳單和送貨位址以及檔案名和類型，以及其它資料。

新型資安漏洞？ (以抖音為例)

2. TikTok可能被中國政府用來監視用戶

- <中華人民共和國國家情報法> 第七條

「任何組織和公民都應當依法支持、協助和配合國家情報工作，保守所知悉的國家情報工作秘密。 國家對支持、協助和配合國家情報工作的個人和組織給予保護。」

- 正如對華為所做的那樣，中共軍隊引入了偽裝成無害編碼缺陷的惡意軟體代碼。當檢測到時，華為可以簡單地回應，「哦，抱歉，我們會糾正的」。但是，如果沒檢測到，此類代碼可用於針對個人或更大數據集的高效間諜活動。
- TikTok目前也面臨一樣的問題，將偽裝成無害編碼缺陷的惡意軟體代碼寫入軟體中

新型資安漏洞？(以抖音為例)

3. TikTok可能被用作「洗腦」或「同儕霸凌」工具

- 除了數據安全問題，TikTok本身還包含與心理健康問題、兒童色情、暴力和吸毒有關的內容。甚至，其所推薦的多項挑戰視頻導致多名青少年死亡，美國國會委員會的成員施壓抖音要承擔責任。
- 為了博人眼球，有些TikTok用戶於是發起自虐式的危險挑戰，像是傷痕挑戰、龍之吐息挑戰、昏迷挑戰、瞌睡雞肉挑戰、鎮定劑挑戰等，輕則嗜睡、噁心想吐，重則食物中毒、身體灼傷，還有人因此昏迷死亡、窒息慘死。

- TikTok首席執行官周受資的孩子不使用TikTok

新型資安漏洞_拼多多

- TikTok資安爭議還未落幕，中國電商「拼多多」的App也爆出暗藏惡意程式，3月已遭Google商店下架。《CNN》報導指出，拼多多的App不但會竊取安卓手機用戶個資，還會擅自更改設定，相當於享受低價購物的代價，卻是出賣自己的個資，國際資安專家直呼「非常可惡」。
- 芬蘭資安業者首席研究官赫佩根直言，拼多多應用程式利用安卓作業系統漏洞，惡意軟體可以繞過安全系統監控其他App，查看通知、閱讀私人訊息，甚至擅自更改手機設定，而且安裝後很難完全移除，例如從私人相簿中竊取照片。赫佩根表示，團隊能證實拼多多App確實試圖在安卓手機上提高權限，讀取其他應用程式無法讀取的項目。

新型資安漏洞？

語音生物辨識（voice biometrics）已不再安全！無論是語音線上購物，或要通過銀行的電話語音驗證，當 AI 工具越來越聰明，前所未見的資安風險正在產生。加拿大跨國媒體 VICE 記者實測，成功透過 AI 合成虛擬聲音「駭」進自己的銀行帳戶，使用的還是市面上現有的免費 AI 工具；而同樣在加拿大，一對夫妻被騙走 2.1 萬美元——他們以為電話裡找金援的是親生兒子，殊不知是 AI 合成語音詐騙。

參考資料：Insider、VICE

新型資安漏洞_Deepfake

利用人工智慧和機器學習(Machine learning,ML)（AI/ML）合成的媒體資訊（圖片、聲音、影像等），將無辜明星、政客等知名人物的臉孔和聲音合成進成人影片和宣傳訊息內。
這種「影片換臉」的技術，不知情的人乍看之下就像以為被惡搞的受害者,真的參與了演出。這些假影片就稱為Deepfake（深偽技術）。

TREND MICRO 趨勢科技

Deepfake 影片演變成一項很不容易辨識的社交工程（social engineering）詐騙工具，讓受害者更容易上當。透過換臉、控制嘴唇,植入假造的音源檔,在網路上流傳著上萬個用 Deepfake (深偽技術) 製造的造假影片。如果你的老闆在 Youtube 上有很多影音,得當心被詐騙集團利用向員工詐騙,從事變臉詐騙攻擊或稱為商務電子郵件入侵 (Business Email Compromise”，簡稱 BEC)。已出現的案例是模仿大老闆的聲音，語調、斷句及腔調,進行語音網路釣魚,騙走 24.3 萬美金。

新型資安漏洞_Deepfake

辨識 Deepfake 假影片的四個方法:

變造媒體資訊的情況如此嚴重，人們該如何辨識deekfake作品？對於影片，Wired.com採訪了白金漢大學數學與電腦教授Sabah Jassim及Spectre聯合創辦人Bill Posters，他們建議要注意以下事項：

1. **眨眼率；Deepfake製作對象的眨眼率少於正常人**
2. **語音和嘴唇運動的同步狀況**
3. **情緒不符合**
4. **模糊的痕跡、畫面停頓或變色**

新型資安漏洞_Deepfake

製作深度偽造影片，這項技術會分別學習如何對兩張不同的臉進行編碼和解碼。舉例來說，一位著名人士舉行了公開演說，而另一個人談的卻是完全不同的爭議性內容，這項技術卻能破解並重建人臉，最終將影片與第二張臉合併。這樣一來，原本那位著名人士的臉看起來就像第二張臉。這項技術也可以用來把另一張臉疊加在特定人物臉上，就能創造深度偽造影片。

這項技術能針對聲音做出細微變化，進而改變整個影片的核心訊息。這項技術的確有正面的用途，像是用在電影產業，透過深度偽造技術省下重拍某些片段的麻煩。但它也已經被用在負面的情形，例如在未經許可的情況下，用名人的臉來製作成人色情內容。有鑑於此，人們憂心這項技術經常被用來影響選舉、衝擊市場、毀掉職業生涯，甚至產生更可怕的犯罪。

影片分析

新型資安漏洞_Deepfake

Deepfake（深偽技術） 對一般人有何影響?

雖然一般市井小民,影像被盜用的機率比較低,但仍需注意以下可能的風險：

✓詐騙

盜用名人的照片做廣告已經不是新聞但若這些名人真的說起話來推薦呢？

俄羅斯某家銀行的創辦人就被盜用,運用深偽技術製作影片推薦投資工具,並附上釣魚連結來進行詐騙。

✓某些交友軟題上甚至也出現明星藝人,還不只照片，能跟你視訊對答如流,有些人就因此受騙，匯款非常多錢給對方

✓假新聞

一個造假的惡意攻擊影片,會不會改變一場選舉結果?日前歐巴馬造假事件,讓人擔心 Deepfake 被有心人士惡意運用。

BCCS 漢昕科技

新型資安漏洞_網路釣魚進化成 AI 語音釣魚

語音釣魚是***網路釣魚***（Phishing）的電話版，Vishing 這個詞是從 voice (語音) 加 phishing (網路釣魚) 這二個字組合而來。受害者可能直接接到歹徒的電話，或者可能收到一封邀請函 (透過電子郵件或語音郵件)，請受害者打電話到假的客服中心來解決某個問題。一旦受害者撥打電話，自動語音系統就會請受害者在電話上輸入自己的帳號、PIN 碼或密碼

對歹徒來說，語音釣魚的流程共有三個步驟。第一步驟是「挑選」對象。歹徒會撰寫一些程式來自動撥號給許多人，就像許多大量散布的網路釣魚（Phishing）一樣布下天羅地網，期望能夠抓到幾個不夠警覺的銀行客戶。攻擊者可能下載一些軟體，讓他們在受害者的來電顯示某個號碼，這樣他們就能輕易假冒某銀行的來電。第二步驟是從「被挑中」的受害者套出個人資料。歹徒會向受害者詢問信用卡卡號以及其他相關帳號資訊。最後一個步驟是想辦法利用被害者的資訊來竊取受害者的錢。

新型資安漏洞_AI 語音複製詐騙（Voice Cloning）

詐騙者現在會利用AI語音複製技術來冒充他人欺騙受害者給出金錢或敏感資訊。詐騙者利用社群媒體短片裡的聲音就能夠輕易地加以複製，然後冒用身分來打電話給其家人/朋友/同事。

詐騙者最近會用AI語音生成技術來製造假的兒童綁架案，向心緒大亂的父母那要求高額的贖金。根據報導，有詐騙者複製了一名美國亞利桑那州15歲女孩的聲音，冒充她打電話給她的媽媽並威脅會傷害她，然後要求100萬美元的贖金。還好這位母親可以確認她的女兒是安全的，但這案例也顯示出詐騙者可以利用AI技術做到什麼程度。

另一種常見的AI語音詐騙是長輩騙術（grandparent scam），詐騙者複製孫兒的聲音來向會因擔心而上當的祖父母那騙取金錢和個人帳密。美國聯邦貿易委員會（FTC）已經對語音複製詐騙發出了警告。

BCCS 漢昕科技

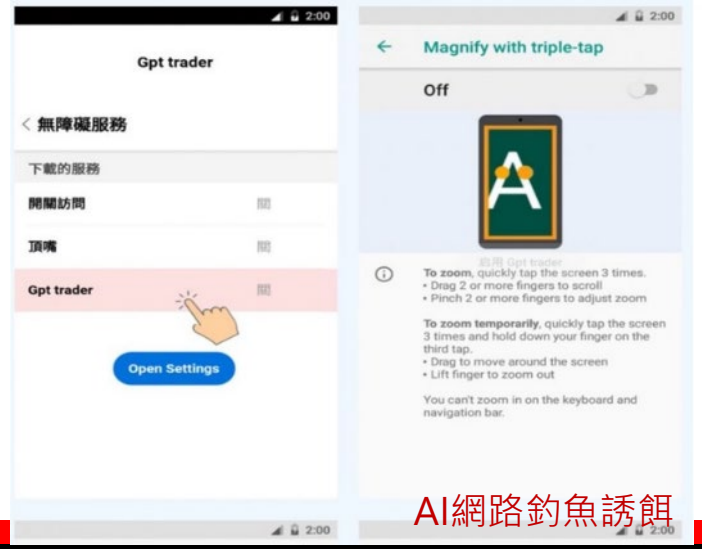
新型資安漏洞_AI 語音複製詐騙（Voice Cloning）

- **保護自己免於AI 語音詐騙**

- 📌 1.冷靜判斷：先掛斷電話並直接聯絡「被綁架」的親友,如果聯絡不上,致電可以確認其行蹤的老師/同事/朋友。
  📌 2.反問「被綁架」的親友:請對方回答只有家人知道的「通關密碼」（＊前提是：你們必須曾經共同設定過）。
  📌 3.發文前三思：不要在社群媒體過度分享，免得讓詐騙者的謊言可信度大增。
  📌 4.做好社群隱私設定：不要在社群網站公開自己或親友的電話號碼,如果一定要發布有自己聲音的影片,請做好隱私設定。
  尤其不要公開自己或親友的電話號碼,若要發布有自己聲音的影片請做好隱私設定

新型資安漏洞_假AI軟體/工具的網路釣魚廣告

可疑的ChatGPT Facebook網頁



AI網路釣魚誘餌

假的ChatGPT應用程式和釣魚網站。詐騙者會在社群媒體和搜尋引擎投放關於ChatGPT和其他AI工具或軟體的廣告。如果你點入這些惡意連結，就可能會被帶到會讓你的裝置下載惡意軟體的網站。有些廣告甚至會將你帶往真正的軟體/網站，但會利用漏洞攻擊或後門下載惡意軟體，讓你甚至無法察覺。一旦發生這些情況，你可能會成為勒索病毒的受害者或遭受身份盜用或金錢詐騙等攻擊。

防止AI 網路釣魚的重要建議：

1.永遠不要點開未知的軟體廣告。
2.直接透過搜尋引擎來訪問網站。
3.如果你不知道網站地址，請搜尋它。

新型資安漏洞_ AI 生成圖片詐騙

利用AI編輯過的敘利亞內戰時 Afrin 地區受害兒童照片 資料來源：TikTok

有可惡的詐騙份子使用AI生成圖片來利用土耳其-敘利亞地震賺錢。他們會貼出假的受害兒童照片來吸引人們的同情和捐款 – 然後將錢放進自己的口袋，可能還包括了受害者的帳密。

如何保護自己不受AI 詐騙所害？

- 在網路上看到圖片或內容時要保持懷疑態度。做好功課！
- 收到非預期的電話或訊息時要小心。
- 如果覺得電話可疑，請掛斷並直接聯絡你的朋友/家人/同事或打電話給能夠確認狀況的其他人。
- 當被要求透過加密貨幣、禮品卡等方式收錢時，要保持懷疑。
- 不要在社群媒體上過度分享，這讓詐騙者能夠去增加他們騙局的可信度。
- 如果你懷疑自己被騙了，請立即回報給防詐騙機構。

新型資安漏洞_惡意軟體利用 OCR 竊取敏感資料


惡意程式CherryBlos利用OCR技術竊取帳號密碼

Android用戶正面臨著一場新的威脅，一款名為CherryBlos的惡意軟體正在迅速蔓延。這種惡意軟體利用了光學字元辨識（Optical Character Recognition，OCR）技術，用於收集儲存在用戶裝置上的圖片中的敏感資料，其通過社交媒體平台上的虛假文章進行傳播，特別是針對使用加密貨幣錢包的用戶。

趨勢科技研究人員指出，CherryBlos攻擊方式相當狡猾，一旦用戶安裝惡意軟體，它會竊取加密貨幣錢包相關憑證，當受害者複製特定格式的字串到剪貼簿時，CherryBlos會偷偷替換錢包位址，將交易引導至駭客的位址。更嚴重的是，它還運用OCR技術來辨識圖片中的助憶詞組（Mnemonic Phrase），而這些助憶詞組對用戶在恢復錢包時扮演著關鍵的角色。

BCCS 漢昕科技

行動裝置與電腦資安防護建議

即時通訊軟體注意事項(1/2)

- 不得於公務個人電腦安裝
- 以傳送溝通訊息為主
- 傳遞訊息，內容不得涉及機密性、安全性、隱私性或洩漏個人資料
- 機關聯絡群組，指定管理人員
- 管理人員應建立群組名冊並定期清查群組成員，每月將群組訊息內容備份為檔案

即時通訊軟體注意事項(2/2)

- 機關交付正式文書，應循現有行政程序辦理(例如:公文、E-mail)
- 管理員應適時向群組成員宣達使用注意事項，發現問題應立即處理。成立群組目的消失，應即時刪除。
- 群組成員發現誤傳或內容不當者，應即時主動通報管理員處置

電腦安全

- 長時間離開辦公室，記得將電腦關機
  - 杜絕來自網路破壞
  - 防止帳號或密碼被盜用
  - 防止重要資料遭竊
- 應用程式不用時，登出應用程式及作業系統
- 離開座位，電腦應該設定螢幕保護程式
- 辦公室電腦不得任意加裝與工作無關之軟體

機密資料保護

- 紙本
  - 機密及敏感文件不可遺留於桌面上，必須存放於安全場所並加以上鎖
  - 作廢、敏感文件不得回收再利用
- 電子資料
  - 重要或敏感檔案要分開存放
  - 設定密碼或以加密軟體保護
  - 建議避免共用資料夾

重要資料備份

- 備份的重要性
  - 預防重要資料或設備損壞遺失
  - 確保可用性
  - 防範勒索病毒
- 可藉由以下方式達到備份目的
  - 不同的儲存媒體
  - 各式各樣的工具軟體
  - Windows本身所提供的程式
  - 網路存放及備份(加密上傳)

結論

結論

防疫 V.S. 防駭

防疫措施		防駭措施
配戴口罩並定期更換		安裝防毒軟體並更新病毒碼
在外不碰觸眼口鼻		勿點擊不明來源的網址及安裝程式
以正確洗手方式勤洗手	V.S.	定期依照密碼複雜度規則更新密碼
公共場所保持社交距離		企業及機關應落實內外網區隔及防護
機場、港口入出境管制		資安人員應阻絕釣魚網站並禁止電腦連結
感染者應接受隔離治療		受駭電腦應阻斷網路避免病毒橫向擴散

資安實務是一種取捨分析((Trade-off Analysis，TOA)，資安做的越嚴謹大家越不方便且可能影響工作流程；反之越鬆散則越不安全、危險但大家都很方便開心。因此，合理的資安政策要適時的、因地制宜的做取捨分析，或是安排配套措施，取其兼顧營運和風險的平衡點。

BCCS 漢昕科技

Q & A

BCCS 漢昕科技

感謝各位參與！！