

日月光

資訊安全教育訓練講座



大綱

- 前言
- 詐騙訊息宣導
- 資安政策
- 資安與生活
 - 社交工程、變臉詐騙、工作詐騙
- WiFi與IoT設定
- 密碼與他們的未來
- 個資與隱私安全



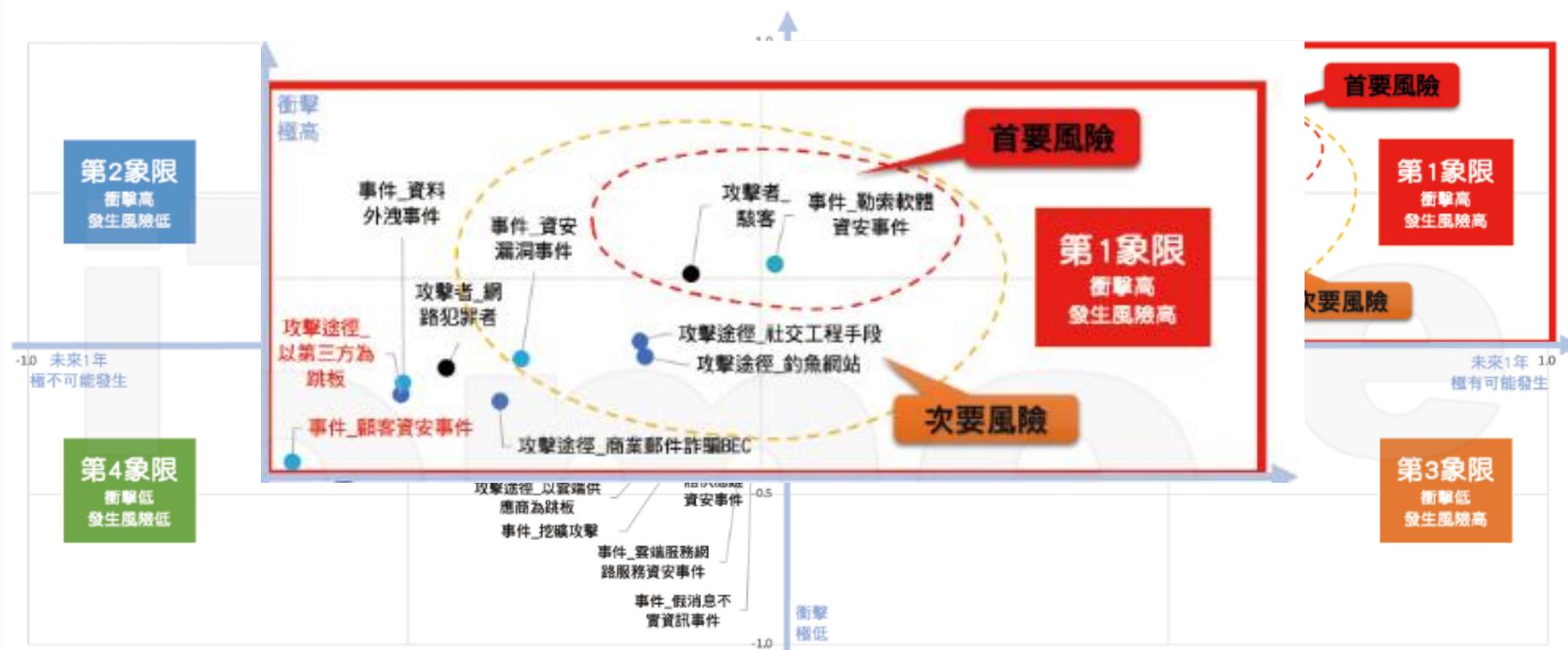
前言



預測整體產業資安風險

整體產業企業資安風險圖（未來一年）

勒索軟體資安事件和駭客是臺灣大型企業未來一年必須優先注意的首要風險，其次還得留意社交工程手段、釣魚網站、資安漏洞的風險。今年有兩項風險突然提高，以第三方為跳板的攻擊和顧客資安事件都進入了高衝擊、高發生率的第一象限



資料來源：<https://www.ithome.com.tw/article/153104>

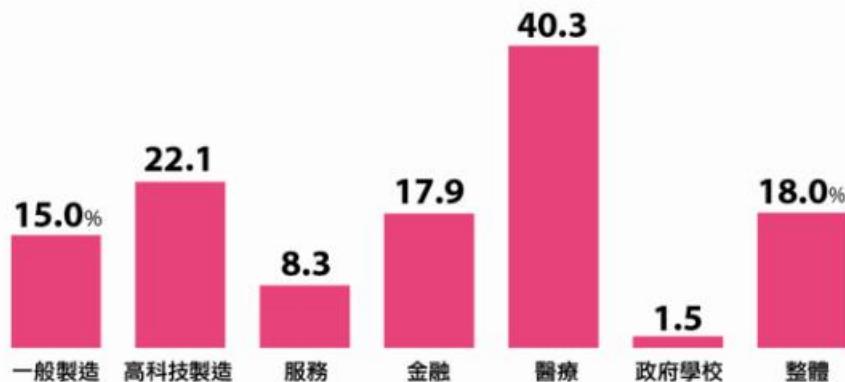


中華資安國際

資安重點投資

各產業 2023 年資安預算成長率

醫療業資安預算成長率最高，高科技製造業第二高

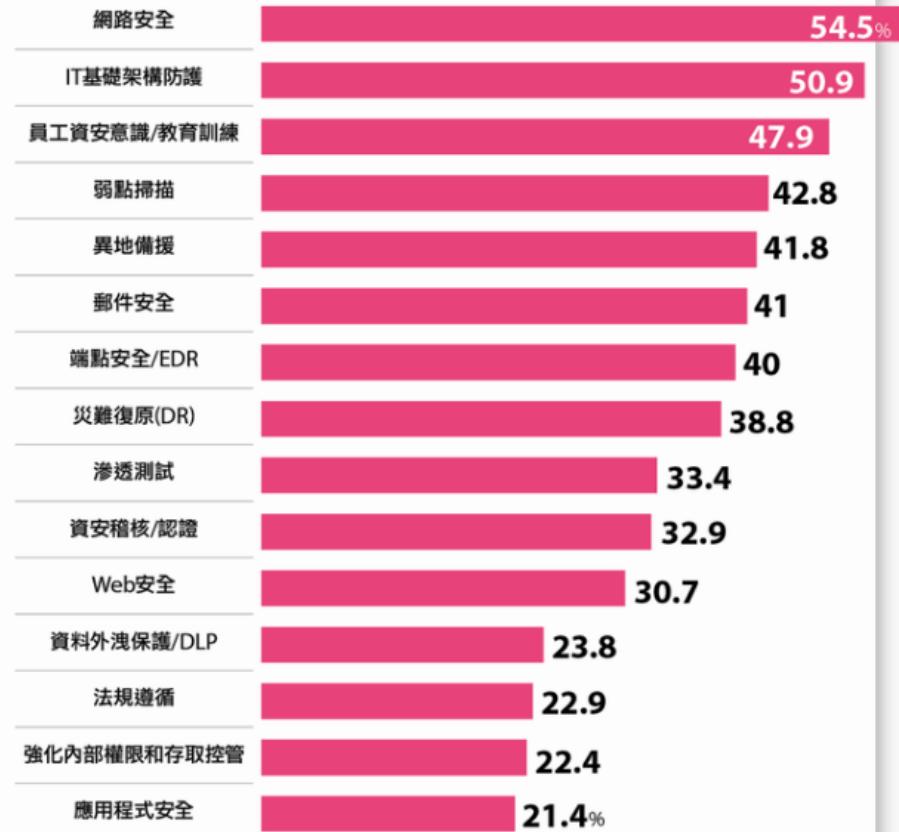


資料來源：2023 iThome CIO大調查，2023年5月

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



資料來源：2023 iThome CIO大調查，2023年5月

iThome

<https://www.ithome.com.tw/article/156845>

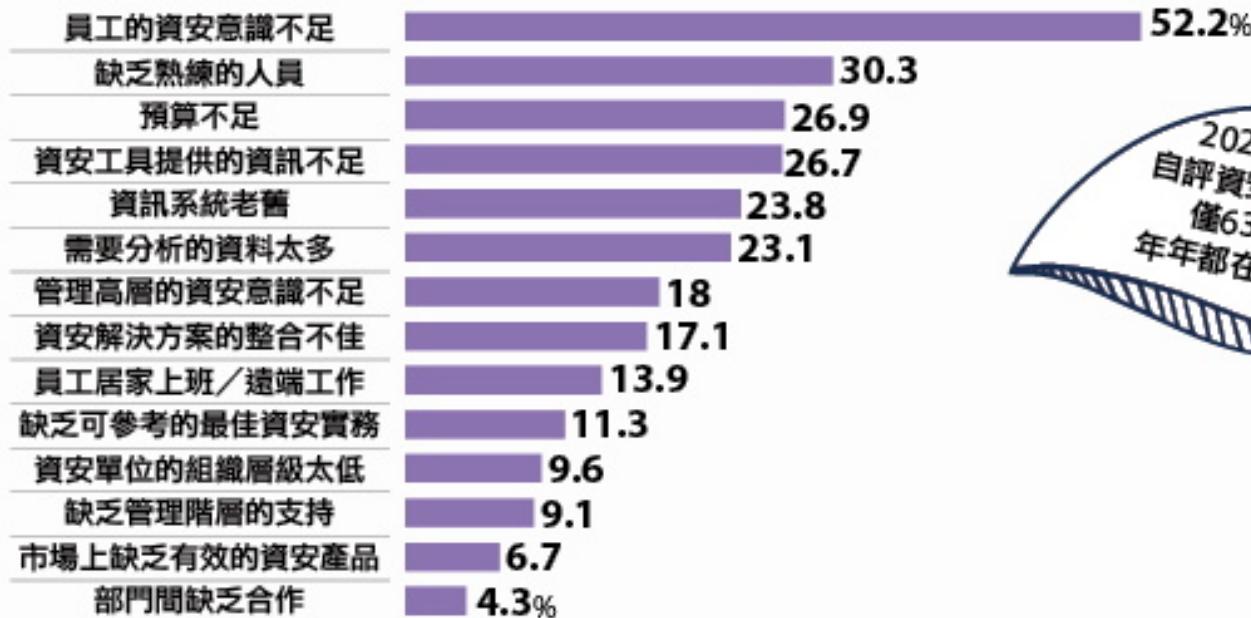


中華資安國際

強化員工資安意識

為何企業難以抵抗資安攻擊（資安弱點排名）

員工資安意識仍是主因，資安老手不足問題日益嚴重



說明：百分比為CISO自評遭遇該項弱點的企業比例

資料來源：2022 iThome CIO大調查，2022年8月

2022年企業
自評資安信心水準
僅63.7分，
年年都在及格邊緣

資料來源：<https://www.ithome.com.tw/article/153104>

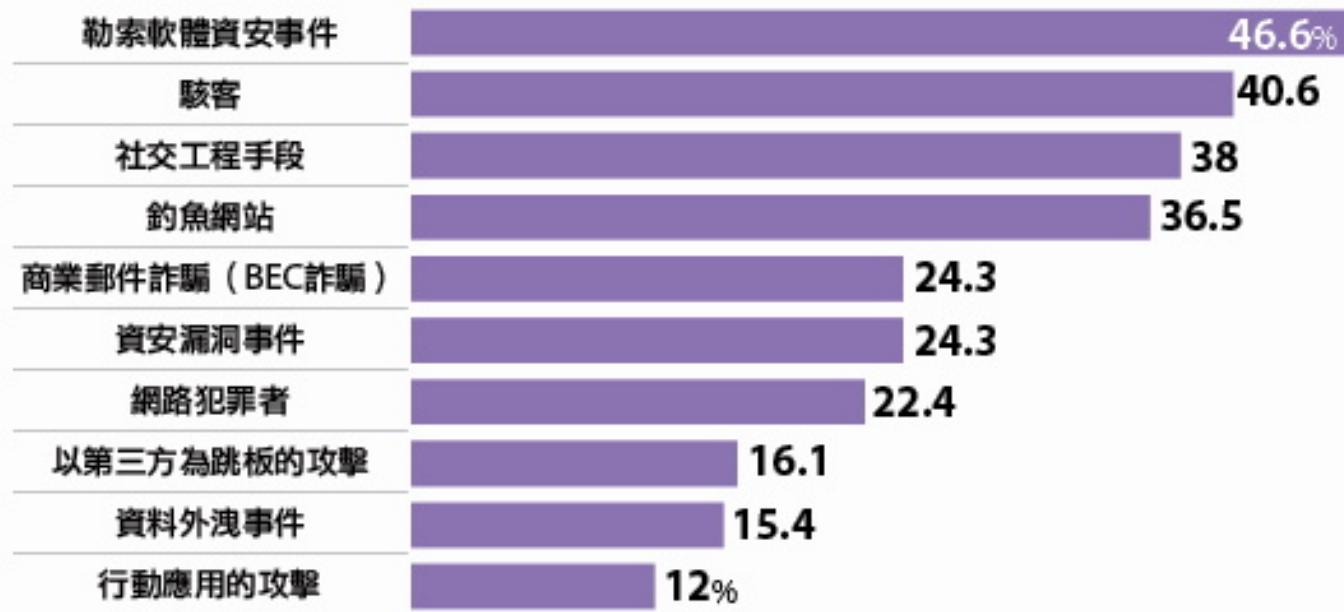


中華資安國際

強化員工資安意識

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



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

資料來源：<https://www.ithome.com.tw/article/153104>



中華資安國際

不同時事、不同詐騙

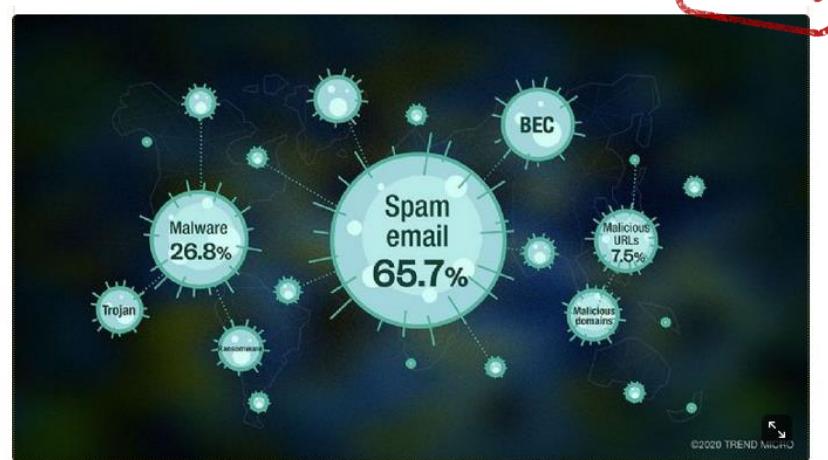
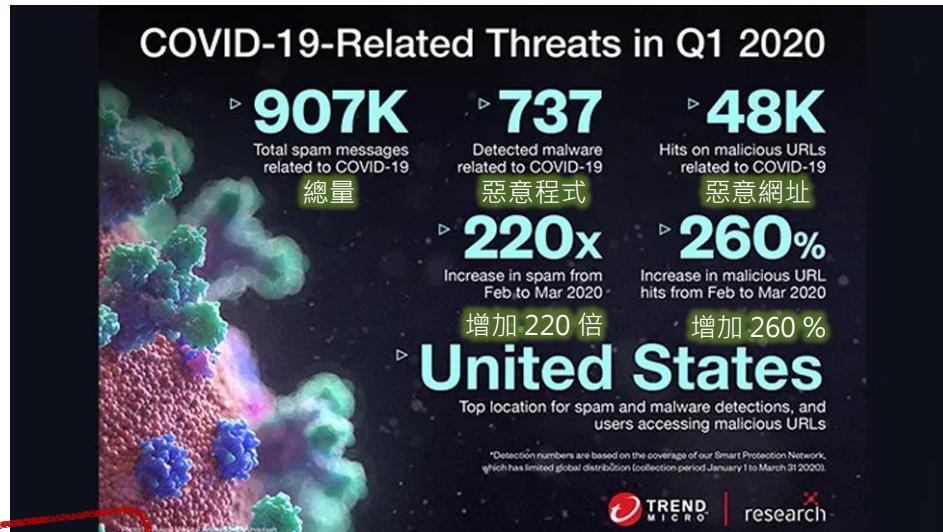
- 臺灣因政治關係，中國對臺灣的網路攻擊態度並不友善

臺灣政府網站 8 成來自中國網軍的攻擊



不同時事、不同詐騙

- 駭客根據**不同時事**，創造**不同的議題**進行社交工程
- 以近幾年來看，**COVID-19** 所創造的社交工程信件數量驟增



趨勢科技近日針對全球以假冒「COVID-19(新冠肺炎)」為主的資安威脅狀況進行深入調查，全球前三大資安風險分別是垃圾郵件、惡意軟體與惡意連結。

聯合報標題：全民遇駭紀實

- 資訊安全是個嚴肅也沉重的議題

這是無聲的國安危機。

2022年，台灣有四項資安威脅，被偵測到的數量高居全球前五，包括：勒索攻擊、惡意連結、手機資安事件、智慧家庭連網的內外部攻擊。

資安不再是企業議題

2023年，航空公司華航、汽機車服務公司iRent、百貨公司微風，再到隸屬行政院中央二級單位的故宮博物院，陸續爆發資安漏洞，上百萬個資外洩、上萬張國寶圖檔外流。

攻擊會針對各種產業

如今台灣每月遭受多達2000萬至4000萬次境外網攻，各組織平均每周遭3118次攻擊。台灣逾2300萬筆戶政資料被放上暗網兜售、全台65%手機外洩致至少1040萬人個資暴露於風險中。據刑事局統計，詐騙財損金額5年增長75%。

你所保護的個資，輕易的外洩

總統蔡英文2016年喊出「資安即國安」口號，兩任任期結束在即，實績卻是：政府失能、企業失責、民眾無感，數位國土防線全面潰堤。

《聯合報》數位版，獨家揭露台灣這一連串荒謬「遇駭」紀實，揭櫫台灣為何難以承擔「世界大戰3.0」的複合式攻擊。

新聞來源：聯合報 (https://topic.udn.com/event/newmedia_hacker?from=udn_ch2_menu_v2_main_index)



中華資安國際

逐年成長的商務郵件詐騙(BEC)

- 全球著名市調中心分析：商務郵件詐騙(Business Email Compromise, BEC) 在2021年市場價值達 0.97 億美元
- 並對市場進行預測，全球商務郵件將以 19.32% 的成長率_(年)速度增加
- 這意味著越來越多的駭客將投入此商務郵件詐騙市場



中華資安國際

詐騙訊息宣導



詐騙訊息爆發

你把聯絡方line有

7/14 週四
強勢漲停
買入價位
綜合營收
恭喜有跟
抱等待，

沒有買入的
一檔明牌
領取到
領取賴:x7

添加即可
預計營收

台股精準預測大師
贊助 · 0
『全球唯一！公開預測股市指數 精準20次紀錄
保持人』
千萬人追蹤的精準預測術，
國寶級投資大師一次解答！
🏆 綿造20次精準預測世界紀錄的一史托克老師
2018唯一一場講座！

限額30名，你即將學會：..... 繼續閱讀

台股精準預測大師 史托克
你看那股票就會漲
戶籍知識管理學院

facebook.com

極限哥教你用期貨賺大錢
贊助 · 0
玩期貨你想梭哈家當？😱😱😱
不行！！！你的極限就是.....
出書作者『極限哥』為你財務健診
小資族靠10萬也能挑戰200萬
學員千萬見證👉 http://bit.ly/limit-csh

✓ 第一次創業，企業每年總營收就上億..... 繼
續閱讀

我說你的極限

【小資族】靠10萬挑戰200萬的故事

澳豐事件：你知道天上不會掉餡餅，為什麼會相信8%獲利？



澳豐承諾給與投資人8%以上的年化收益，與銀行定存利息相差甚遠，究竟澳豐在十餘年內吸金1千多億的手法為何？

圖片來源：giggsy25/Shutterstock

2023年5月27日，號稱資產有1千億元規模的澳豐金融集團宣告倒閉清算，成為台灣史上最大金融詐騙案。國內受害者多達1.3萬人，其中不乏政商名流，甚至有十餘家上市櫃公司也被捲入其中。

<https://opinion.cw.com.tw/blog/profile/552/article/13708>

投資詐騙百百種，特色大公開！

詐騙投資案的10個特色

報酬率過高 不用付出努力 不用銷售 商業模式複雜 高人頭獎金



專找窮人加入



強調無風險



炫富裝闊



公司很新



急著成交



資料整理：Mr.Market市場先生

資料來源：<https://www.softnext.com.tw/focus/BEC/qa.html>



中華資安國際
15

支付資格暫時被封鎖  



雷神講堂

...

您的 Apple ID 帳戶有一筆交易目前受到限制

您好：

您的 Apple ID 已於2023年8月7日18:13:16 GMT+8 購買了以下內容：

檢測到異常行為：第三方登錄您的 Apple ID-web 服務並進行消費活動。

Apple支援想確認該卡是否為本人使用，因此很遺憾地通知您，我們已經部分延緩了該筆訂單的進度，時間為24小時。

賬單

分享

APPLE ID

日期
2023年8月7日

訂單號
SLX7MDZ

文橫編號
1759888543

付款信息
Apple Pay
桃園市
大內區
廣西路86號6B2座030室
桃園市, 74564
TW



中華資安國際
16

天上不會掉餡餅—請時刻注意網路釣魚訊息



LINE認證連結

LINE

LINE 官方宣導
2022.8.11

在聊天室裡傳給你的
LINE 認證連結都是假的！



#LINE 簡訊認證碼不要給任何人

注意！這是假的！ 注意！這是假的！ 注意！這是假的！ 注意！這是假的！



中華資安國際
18

ios用戶單則簡訊封鎖、刪除與回報



iOS用戶過濾未知的寄件人



資料來源：警政署官網

iOS用戶設定不使用電子信箱接收iMessage



iOS用戶關閉 iMessage



Android 手機「垃圾訊息阻擋」功能

開啟【垃圾訊息阻擋】



【垃圾訊息阻擋】



【啟用】垃圾訊息阻
擋功能



中華資安國際
23

資安政策



零信任網路政策

- 依據

- 第六期「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，將發展零信任網路資安防護環境，推動政府機關導入零信任網路，完善政府網際服務網防禦深廣度

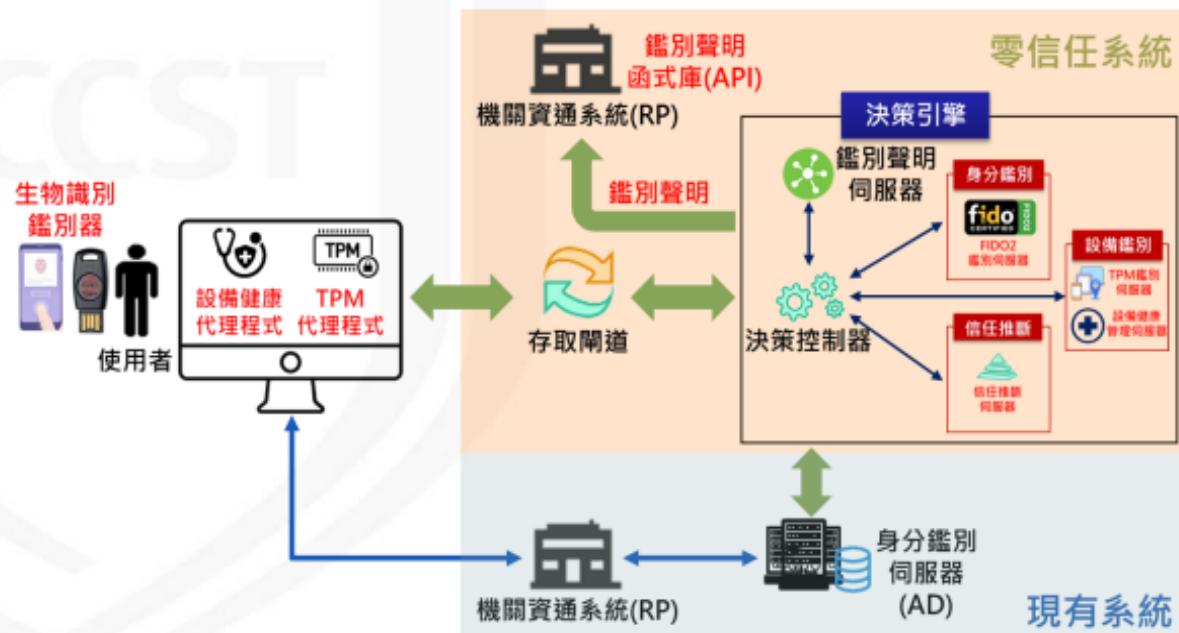
- 推動規劃

- 數位發展部資通安全署規劃投入經費，優先推動A級公務機關導入零信任網路



政府零信任網路架構

- 參考NIST零信任架構，結合向上集中防護需求，政府零信任網路採存取門戶部署方式，具備身分鑑別、設備鑑別及信任推斷3大核心機制
 - 身分鑑別：FIDO2身分鑑別與鑑別聲明
 - 設備鑑別：TPM設備鑑別與設備健康管理
 - 信任推斷：基於分數與情境之信任推斷機制



推動進程

● 政府機關

- 111年起遴選機關逐年導入零信任網路之身分鑑別、設備鑑別及信任推斷3大核心機制
- 後續於資通安全責任等級A級公務機關推動導入

● 商用產品

- 配合111~113年之機關導入，推動廠商開發符合政府零信任網路部署架構、部署原則及核心機制之商用產品，以因應後續A級公務機關之導入

111

112

113

資通安全責任等級
A級公務機關

•身分鑑別

以生物識別鑑別器進行無密碼雙因子身分鑑別

•設備鑑別

基於信任平台模組(TPM)之設備鑑別，並進行設備健康管理

•信任推斷

依設備健康狀態、資安威脅情資及使用者情境等資訊，動態支援存取決策

資安與生活



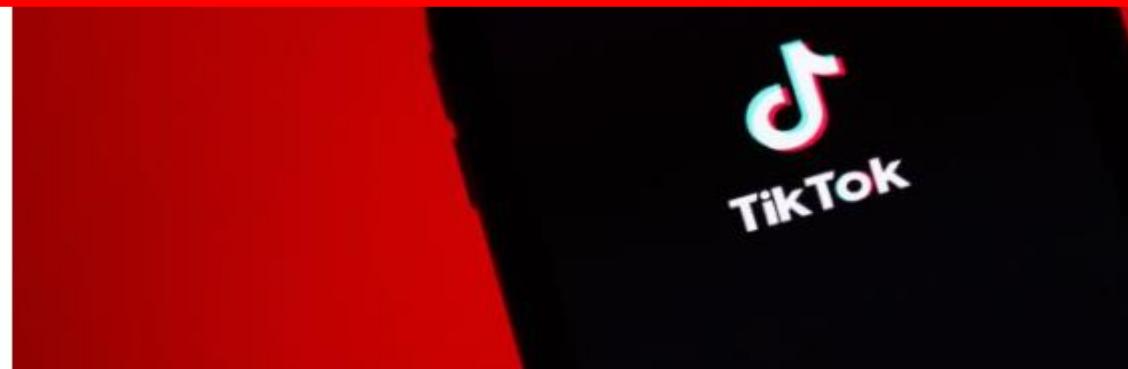
中國要求科技業必須披露應用程式演算法

北京掌握演算法！阿里巴巴、抖音等 30 間中企首次提供細節

作者 林好柔 | 發布日期 2022 年 08 月 16 日 14:51 | 分類 中國觀察, 數位內容, 網路 [分享](#) [分享](#) [Follow](#) [讚 85](#) [分享](#)

中國國家互聯網信息辦公室（網信辦）12 日表示，騰訊、阿里巴巴、美團等 30 間科技巨頭提交部分應用程式演算法詳細資訊，包括如何收集個人數據、客製個人推薦和提供內容。企業名單包括鳳凰網、微博、美團、優酷、快手、百度、新浪、抖音、小米、微信、騰訊，以及阿里巴巴旗下天貓和淘寶等。

彭博社稱這舉措可說前所未有的，雖然清單沒透露實際編碼，但不清楚這些公司提供政府多少程式和軟體。



臺灣8月初因裴洛西訪臺而遭到網路攻擊

在美國聯邦眾議院議長裴洛西訪問臺灣的前後，駭客不斷發動攻擊長達超過一週，我們彙整了這段時間發生的資安事故

【8月】 【8月4日】

內容置 DDoS攻擊桃園機場網站疑遭到網路攻擊陸續出現服務中斷的情形

內容置 假訊息網路流傳解放軍擊落我國戰機的消息，遭國防部駁斥

DDoS 網頁內容置換高雄市環保局飲用水網站被置換五星旗

假訊息 DDoS攻擊行政院政務委員唐鳳表示，8月3日攻擊流量逾15 TB、最高流量為過往的23倍

假訊息 DDoS攻擊臺灣網路資訊中心指出8月2日至3日的攻擊流量占整體75%

假訊息 DDoS攻擊台電公布8月3日遭到網路攻擊的次數達490萬次，已超過6月及7月總和



Avast：28款Chrome/Edge擴充程式含有惡意程式碼

1. 這些惡意的擴充程式多半與熱門服務有關

- 例如有12款具備Instagram的直接傳訊、下載、上傳或Stories功能，7款提供影片下載功能。這28款程式的下載量總計超過300萬次。

2. 這28款擴充程式都是以Javascript撰寫，還可下載其它的惡意程式

- 安裝了這類的擴充程式之後，使用者只要隨便點選一個連結，擴充程式就會通知C&C伺服器並接收命令，其中一個命令可將使用者先導至另一個網站，之後再導回使用者準備造訪的網站。

3. 所有點擊的紀錄都會被傳送到該第三方網站

- 使用者的隱私曝光，亦允許駭客蒐集使用者的生日、電子郵件、裝置資訊，甚至是IP位址。

4. 擴充程式作者在培養了大量的使用者之後，把它賣給了駭客

- 駭客再藉由程式更新植入惡意程式。由於這些擴充程式把後門藏得很好，而且還在使用者安裝了好幾天之後才開始活動，才使得它們能夠逃過安全檢查。

<https://www.ithome.com.tw/news/141737>

SharePoint Online遭勒索軟體攻擊，不經電腦也可以感染

Obsidian研究人員觀測到針對某家SharePoint Online用戶的勒索軟體攻擊事件，攻擊者不從用戶電腦終端進行感染，而是從入侵缺乏2FA等防護的微軟全域管理員服務憑證著手

讚 137

分享

文/ 林妍溱 | 2023-06-12 發表

<https://www.ithome.com.tw/news/157280>



中華資安國際
32

駭客打造專門用於網路犯罪的AI語言模型

WormGPT

WormGPT – The Generative AI Tool
Cybercriminals Are Using to Launch
Business Email Compromise Attacks

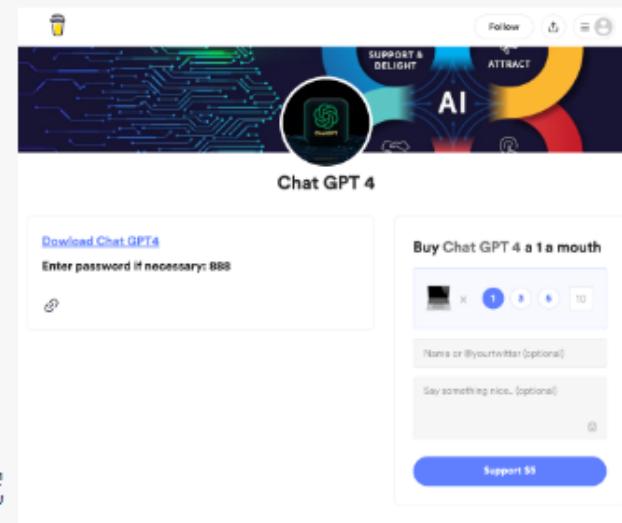


偽裝成ChatGPT的擴充套件

偽裝ChatGPT或類似AI工具的網路攻擊頻傳，Meta發現3月就有10個惡意軟體以此作為誘餌

駭客利用時下熱門的ChatGPT話題來散布惡意軟體，近期有越來越頻繁的現象，但這樣的情況有多嚴重？

Meta的資安團隊指出，他們光是在2023年3月，就發現約有10個惡意軟體家族打著這類名號來發動攻擊，在其中1起事故當中，研究人員看到駭客建立了惡意瀏覽器擴充套件並上架於官方市集，聲稱提供ChatGPT打造的工具，然後透過社群網站及搜尋引擎的廣告引誘使用者上當。



面對社交工程攻擊，你準備好了嗎

臺灣民眾網路詐騙抵抗力有待加強，透過錯誤資訊來確認資訊真偽的比例高達8成

金融服務業者Visa針對全球18個市場、6千個成年人進行詐騙話術（Fraudulese）有關的調查，結果發現，一般人大多會擔心親友受騙，但忽略自己也是歹徒行騙的目標，再者，有81%受訪者透過錯誤資訊來確認資訊真偽——有46%主要依據公司名稱與標誌來判斷。此外，對於釣魚郵件橫行的現象，他們發現僅有6成受訪者會檢查是否來自寄件者的電子郵件信箱，且只有47%會確認郵件是否有錯字。

而針對臺灣的部分，該公司表示，我國消費者最容易受到「限定期間回應」、「免費贈禮」等關鍵字的引誘。



資訊安全人人有責



社交工程



密碼強度



個人資料



中華資安國際
36

社交工程



複習一下...

- 社交工程是?



社交工程

操控人類心理的藝術

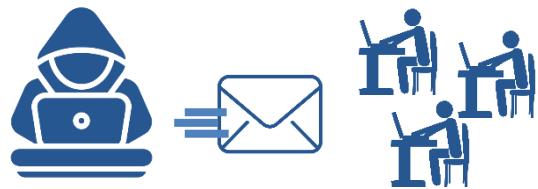
- 利用**人性弱點**、運用**溝通技巧**所發展出來的一種的**詐騙技術**
- 透過電子郵件、電話、手機簡訊、即時通訊...等方式，誘騙受害者提供機敏資訊或入侵
- **非完全技術的攻擊手法**，資安設備也無法完全阻擋



社交工程-情緒詐騙攻擊手法

- 用主旨來達到人類情緒的改變，或與公務相關及使用感興趣的內容吸引

Step1



Step2



Step3



• 駭客發送吸引使用者的電子郵件

• 主旨通常會有讓使用者心情巨大的改變

• 誘使使用者點擊



中華資安國際

情緒起伏類-主旨吸引

公務類

(寄件者：廠商)
更改銀行收款帳戶

(收件者：人事)
我的履歷表

(收件者：業務)
客訴信件

(收件者：員工)
KPI 考核

情緒類

(恐慌)
你的私密照片流出

(緊張)
你有一筆刑事案件

(開心)
恭喜你獲得手機

(好奇)
最新危樓名單出爐

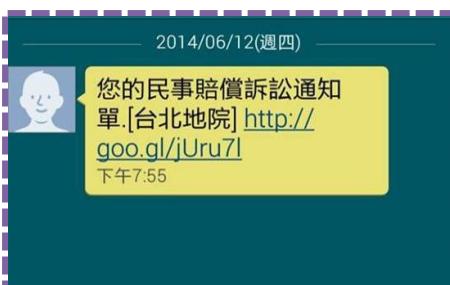
興趣類

(旅遊類)
冬季溫泉之旅清單

(時事類)
Covid-19解藥出爐

(保健類)
維他命怎麼吃才好

(影劇類)
鐵達尼號刪除片段



中華資安國際

偽裝官方類型(1/3)

檔案 郵件 Adobe PDF

此郵件已轉換為純文字。

寄件者: 台北富邦銀行 <service@bhu.taitpeifubon.com.tw>

收件者: 楊 [REDACTED]

副本:

主旨: 台北富邦銀行信託所得通知單

訊息 台北富邦銀行信託所得通知單.PDF (90 KB)

親愛的客戶 您好：

為達到資訊安全高度要求，以及提昇保護您個人信託所得通知單的瀏覽隱私權，自即日起本行提供安全性更高之「數位簽署」寄送機制，確保資料之完整性及隱私性，讓您接收憑單更放心！

請您開啟附件檔案並輸入您的個人資料或與本行約定之密碼以開啟信託所得通知單；

開啟信託所得通知單操作步驟及注意事項說明如下：

1. 開啟此封信件附加檔案。
2. 輸入您的個人資料(身分證字號)或與本行約定之密碼以開啟信託所得通知單，查看您的交易明細內容。
備註：另提醒您，已加密帳單開啟密碼之英文字母皆需輸入大寫。
3. 可開始閱讀您的信託所得通知單。
4. 若您仍無法順利閱讀帳單內容，請下載 Adobe Reader <<http://get.adobe.com/tw/reader/>> 。

※若您希望使用更安全的機制，可與本行約定開啟信託所得通知單之密碼；

偽裝官方類型(2/3)

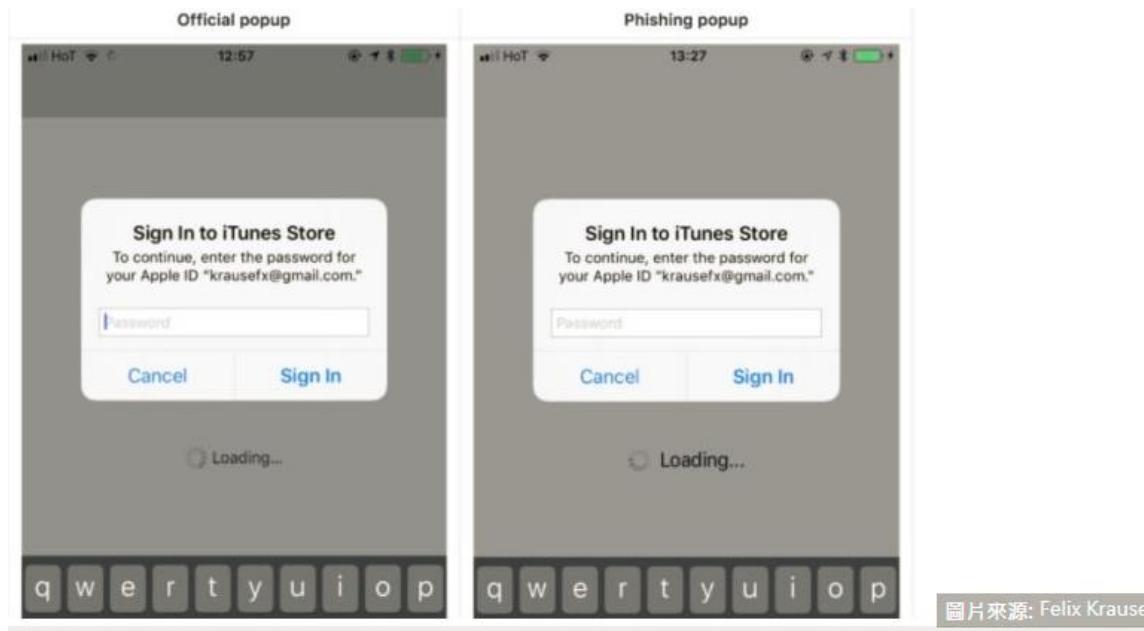
The image displays three side-by-side screenshots of Mozilla Thunderbird email clients, each showing a different type of phishing attempt:

- Screenshot 1 (Left):** Shows an alert titled "Sign - in attempt prevented". It informs the user that someone tried to sign in to their Google Account from an IP address in the United States. It includes a "REVIEW YOUR DEVICES NOW" button.
- Screenshot 2 (Middle):** Shows an email from "no-reply <noreply.service.tw@gmail.com>". The subject is "郵件帳戶同步至HTC手機". The message body contains a warning about Google+ synchronization to an HTC phone and includes a "取消並禁止同步授權申請" (Cancel and prohibit synchronization authorization application) button.
- Screenshot 3 (Right):** Shows another email from "no-reply <noreply.service.tw@gmail.com>". The subject is also "郵件帳戶同步至HTC手機". The message body is identical to the one in the middle screenshot, including the warning and the "取消並禁止同步授權申請" button.

為避免冒用，Google 不會使用 gmail.com 結尾的電子信箱來寄送任何 Google 系統信件，因為 Gmail.com 任何人都能註冊

偽裝官方類型(3/3)

不肖的開發人員模仿蘋果要求輸入Apple ID資訊的介面(右)，以假亂真騙取使用者的帳號密碼



中華資安國際

眼花撩亂類型

自由時報
Liberty Times Net

即時 熱門 政治 社會 生活 健康 國際 地方 莊奇 影音 財經 娛樂
汽車 時尚 體育 3C 評論 玩咖 食譜 地產 專區 TAIPEI TIMES 求職

i跟I分不清 科技公司錯看1字被詐2000萬元

The screenshot shows four messages in an email thread:

- Message 1: 奇件人 : vertraulic@europe.com
主旨 : 我是老闆，我現在要執行一件要事，請立即匯款美金580
萬元到 xxx-xxxxxxxxxxxx 戶頭
- Message 2: re : vertraulic@europe.com
請問老闆，是匯款美金580萬元到 xxx-xxxxxxxxxxxx 戶頭嗎？
- Message 3: 奇件人 : vertraulic@europe.com
是的，快點匯過來
- Message 4: re : vertraulic@europe.com
老闆，我會過去了，請問有收到嗎？

竄改商務郵件詐騙一覽

ver tra ulic @ e u r o p e . c o m	小寫 1
ver tra ulic @ e u r o p e . c o m	數字 1
v o r g a n @ E U R O P E . C O M	英文 O
v o r g a n @ E U R O P E . C O M	數字 0
a d v i c e @ m i c r o s o f t . c o m	
a d v i c e @ r n i c r o s o f t . c o m	

如何預防被騙

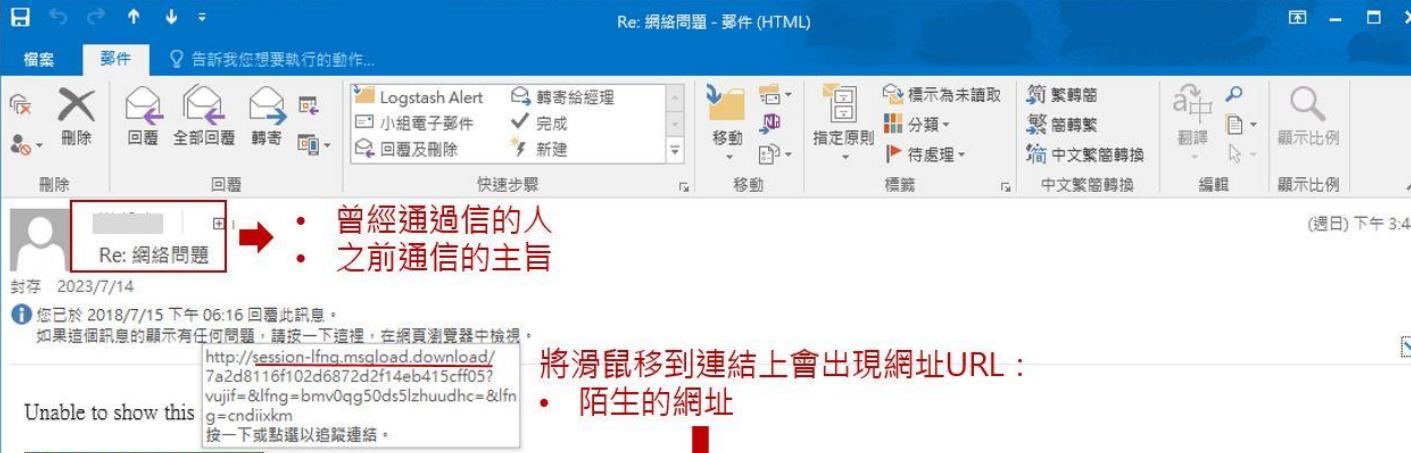
- 收信時，仔細分辨來信 Email 帳號有無異樣之處
- 收到關於變更貨款/匯款帳戶郵件，勿僅依郵件指示操變更
- 聯繫窗口如為外商公司，建議致電或其他管道，進一步確認正確性
- 變更字形或善用 Google
 - vertraulic@europe.com (字型 : Calibri)
 - vertraulic@europe.com (字型 : Calibri)



中華資安國際

入侵攻擊類型

- 駭客可能已潛伏在電腦內擷取通信紀錄



Re: 網絡問題 - 郵件 (HTML)

• 曾經通過信的人
• 之前通信的主旨

封存 2023/7/14

① 您已於 2018/7/15 下午 06:16 回覆此訊息。
如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。
<http://session-lfng.msgload.download/7a2d8116f102d6872d2f14eb415cff05?vujif=&lfng=bmv0qg50ds5lzhudhc=&lfng=cndixkm>
按一下或點選以追蹤連結。

Unable to show this

Click here to view message

Pop3 message delayed: lfNG - Date: 07/15/2018 7:43:53 (ntu)

將滑鼠移到連結上會出現網址URL：
• 陌生的網址

↓



→ 仿造logo

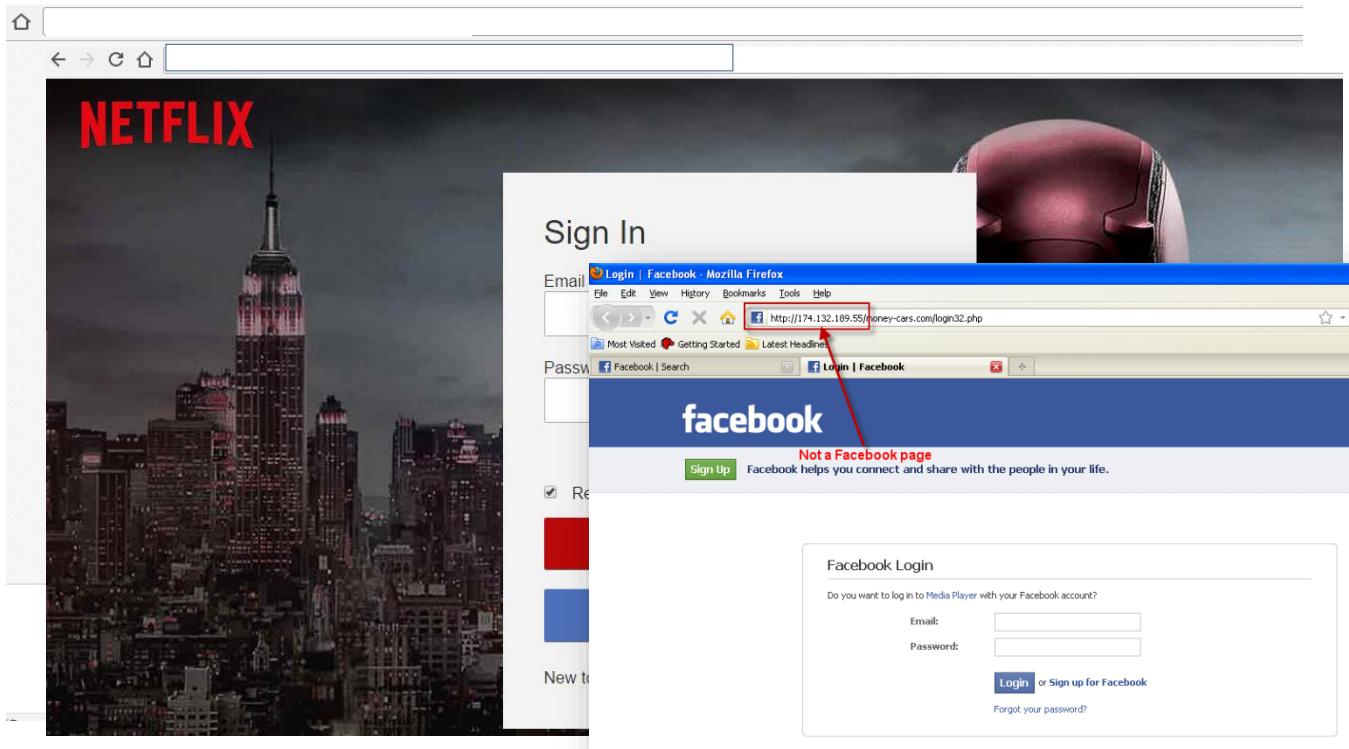
→ 騙取密碼

社交工程...不是只有釣魚

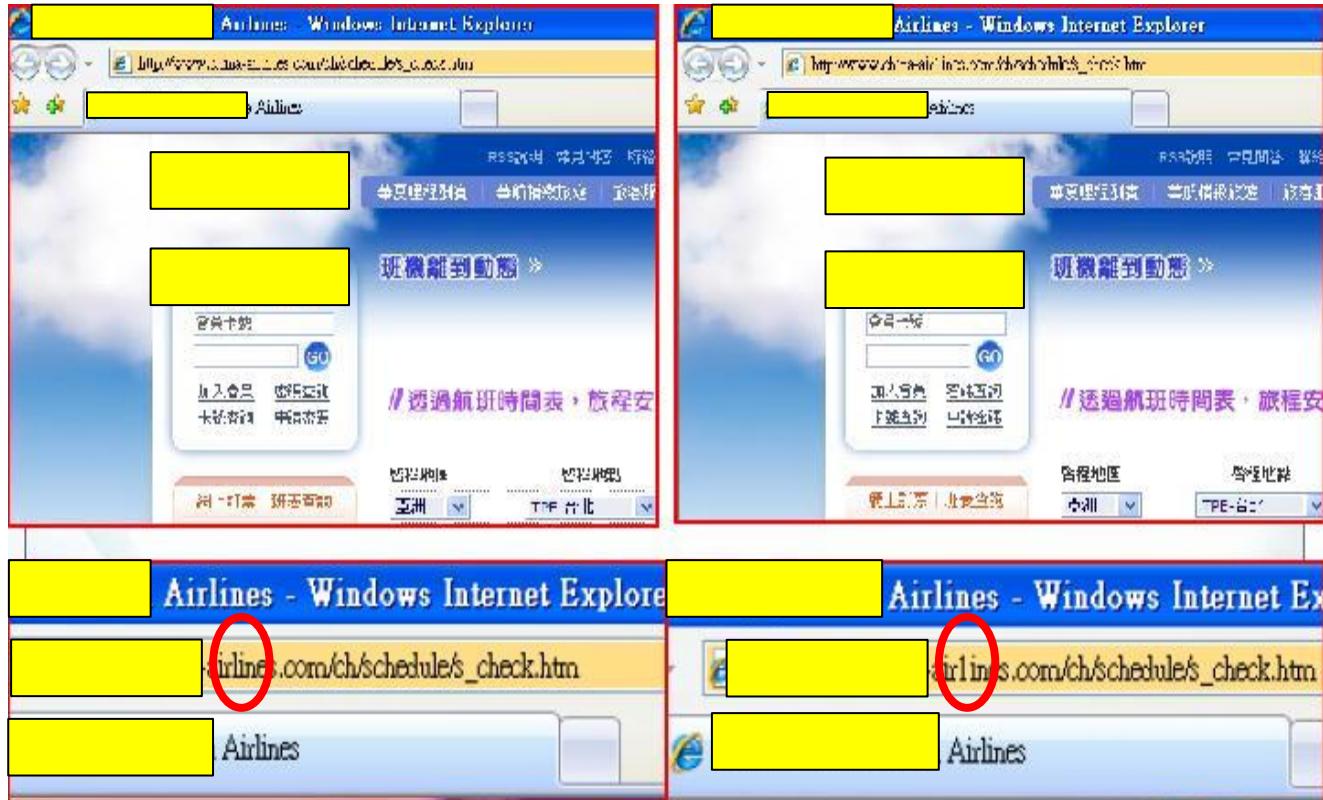
- 釣魚(Phishing)
 - 釣魚郵件 (phishing mail)
 - Spearing phishing
 - Whaling
 - 釣魚網站(phising site)
- 肩窺 (Shoulder surfing)
- 翻垃圾桶(Dumpster diving)



疏忽甚麼？偽冒網站



疏忽甚麼？偽冒網址



USB.feat社交工程



存在已久的USB攻擊手法

報告指近一成 IT 資安事件原因為外接儲存裝置

作者 Unwire Pro | 發布日期 2022 年 03 月 10 日 7:45 | 分類 儲存設備, 資訊安全

分享

分享

Follow

閱讀 10

分享

Top attack
vectors

JANUARY

2022

Monthly Attack Trends

1 Phishing

2 Removable Media

3 Valid Credentials

4 Web Delivery

eXpel®

<https://technews.tw/2022/03/10/top-attack-vectors-january-2022/>

變臉詐騙



變臉詐騙 Business Email Compromise / BEC

手法一：透過偽造的郵件、電話或傳真要求匯款給另一個詐騙用帳戶



偽造郵件、
電話及傳真
(溝通管道)

要求處理機密及
急迫的事情

要求配合提供機
敏資料或
匯款至另一帳戶

資料來源：<https://www.softnext.com.tw/focus/BEC/qa.html>
<https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes/>



中華資安國際

變臉詐騙 Business Email Compromise / BEC

情境一：「偽造發票騙局」、「供應商詐騙」和「發票變造騙局」

小心詐騙》當供應商說「我們要改匯款帳號」



模仿一個與原供應商很相似的email，姓名一樣、語氣一樣、簽名檔一樣，如果不仔細看，還真看不出電子郵件最後的「.com」變成「.conn」也可能是「.corn」。不分清紅皂白就匯款，很可能貨款就落入駭客口袋。

避免方式：

- 1.匯款帳號：不隨意更動
- 2.設定SOP：「變更帳戶」需等待生效，爭取充足查證時間
- 3.使用不同管道確認：電話相互驗證

資料來源：<https://www.businessweekly.com.tw/business/blog/3008477>

變臉詐騙 Business Email Compromise / BEC

手法二：詐騙者自稱為高階主管（CFO、CEO、CTO等）、
律師或其他類型的權威者



偽造郵件、電話及
傳真(溝通管道)

自稱是高階主管、
律師、法官、警察、
等

要求處理機密及急
迫的事情，要求匯
款至另一帳戶

資料來源：<https://www.softnext.com.tw/focus/BEC/qa.html>
<https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes/>



中華資安國際

變臉詐騙 Business Email Compromise / BEC

情境二：詐騙者自稱為高階主管（CFO、CEO、CTO等）



芭比生產商遭電郵詐騙 320萬美元匯溫州

美泰公司總部的財務總監，早前收到一份**冒充公司總部高層管理人員發來的郵件**。對方在郵件中說要**收購一家公司**，需**320多萬美元**，財務總監於**本月2日上午**，將這筆美元匯至對方指定帳戶上。

避免方式：

1. 使用不同管道確認：電話相互驗證。
2. 匯款：需提供相關資料等待生效，爭取充足查證時間

<https://www.epochtimes.com/b5/15/5/5/n44270>

變臉詐騙 Business Email Compromise / BEC

情境二：詐騙者假冒權威者寄信



健保署提醒，發現有惡意人士冒用健保署網址名稱，寄發有關補充保費明細資料的郵件，**內含惡意檔案【檔名：**

『DPR602859651100125001V1100125154830E.pdf.zip』回執聯檔案】，請民眾如果收到可疑信件，千萬不要打開郵件，並直接刪除。

避免方式：

1. 開啟郵件時請注意提高警覺
2. 收到陌生/可疑來信請勿隨意開啟
3. 使用不同管道確認：撥打健保署電話驗證

偽造郵件、電話及傳真
(溝通管道)

自稱是高階主管、律師、
法官、警察、權威等

要求處理機密及急迫的事
情，要求匯款至另一帳戶

<https://www.epochtimes.com/b5/15/5/5/n4427076.htm>

變臉詐騙 Business Email Compromise / BEC

手法三：駭客入侵員工的電子郵件帳號



潛伏於電子郵件 帳號中

等待時機偽造
被害者寄發信件

要求處理機密及急
迫的事情，要求匯
款至另一帳戶

資料來源：<https://www.softnext.com.tw/focus/BEC/qa.html>
<https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes/>



中華資安國際

變臉詐騙 Business Email Compromise / BEC

情境三：駭客入侵員工的電子郵件帳號

Google、Facebook 乖乖把錢匯入「他的」帳戶，東歐駭客「代收」廣達 38 億驚奇



他騙走 Google 2,300 萬美元、Facebook 9,800 萬美元，創下全球社交工程被駭金額新紀錄，即使人抓到了，還有 1,730 萬美元不知去向。

關鍵 1：郵件帳號被駭客監控

關鍵 2：真資訊加假帳號突破控管

關鍵 3：製造斷點阻絕追查

避免方式：

- 1.開啟郵件時請注意提高警覺
- 2.匯款：需提供相關資料並需等待時間才可生效，爭取充足查證時間
- 3.使用不同管道確認：撥打廠商電話驗證

資料來源：<https://technews.tw/2019/07/14/hacker-fraud-google-facebook-quantatw/>

駭客利用虛擬會議發動變臉詐騙 BEC 商業郵件詐騙攻擊

- BFI提醒企業留意可疑的線上會議邀請，防範駭客假冒公司高層身分要求員工匯款
- 情境一、冒充公司CEO /CFO發送電子郵件加入虛擬會議，會議中冒用CEO/CFO的靜態照片，宣稱鏡頭或麥克風故障無法操作，有的用基於人臉偽造技術而成的音效，有時不發聲音，要求員工透過虛擬會議平臺或後續的電子郵件匯款。
- 情境二、利用CEO /CFO郵件帳號插進員工的虛擬會議中「旁聽」，以蒐集公司業務或研發活動資訊。
- 情境三、竊用CEO /CFO電子郵件帳號發信要求員工代為匯款，聲稱自己的電腦被用來開虛擬會議無法自行作業。

身分偽造

竊密/竊聽

社交攻擊



中華資安國際

當心工作詐騙！門檻很低待遇卻超好的陷阱職缺

柬埔寨為何淪詐騙天堂？外媒揭和3件事有關

07:00 2022/08/17 | 中時新聞網 | 吳映璠



中華資安國際
61

美CISA公布網路釣魚演練結果

網釣攻擊**突破防護與成功的機率**，可能比你想要更高

- 每10個接受CISA模擬網釣測試的人中，就有1人點擊連結或下載附件，且每10間企業組織就有8間至少1人淪為模擬網釣測試的受害者

教育員工要有防護意識不被誘騙，也要知道**發現事件應該通報**

- 1阻擋2防誘3回報

美CISA公布網路釣魚演練結果，每10間就有8間企業有員工被網釣成功，教育員工回報網釣與實施抗網釣MFA成新重點

近期美國網路安全暨基礎設施安全局（CISA）公布一份網路釣魚資訊圖表（Phishing-infographic），當中揭露了CISA模擬網釣測試評估的結果，同時還彙整出防範網釣攻擊應關注的4大面向及具體行動

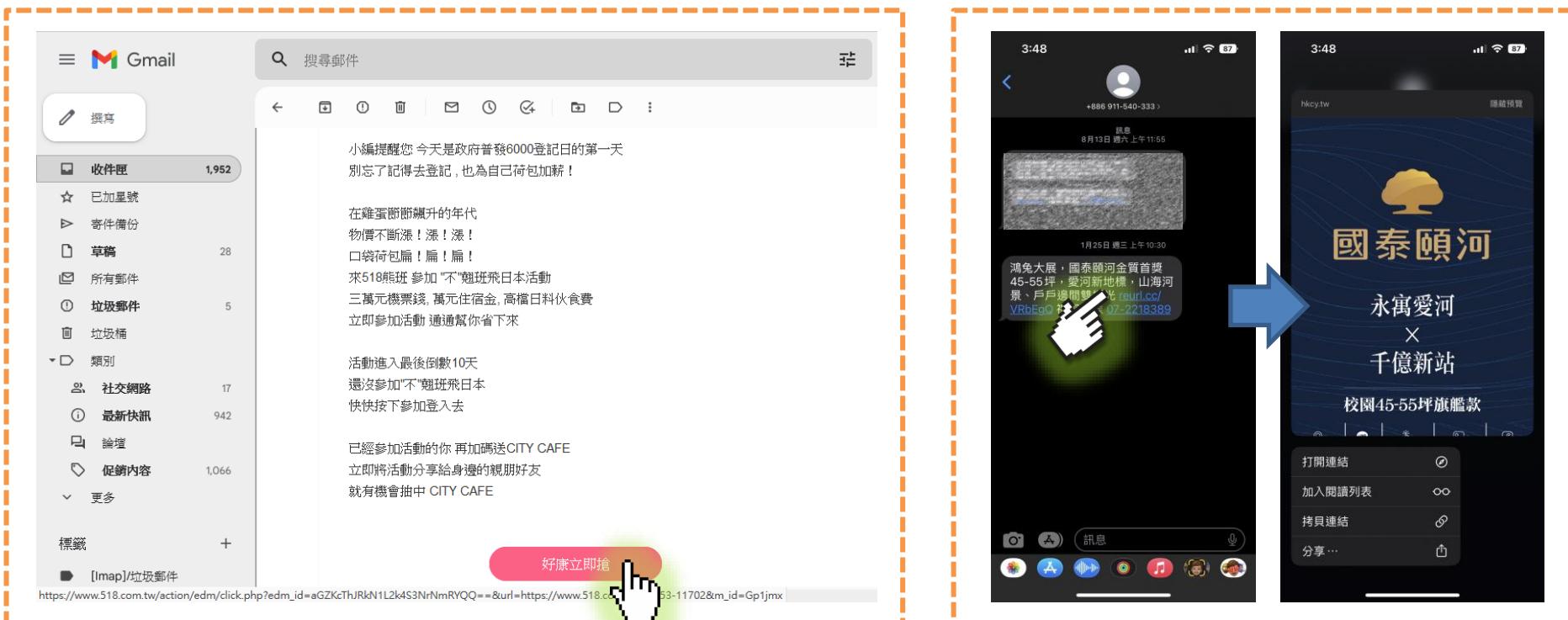
文/ 羅正漢 | 2023-02-01 發表

閱讀 27 分享

<https://www.ithome.com.tw/news/155324>

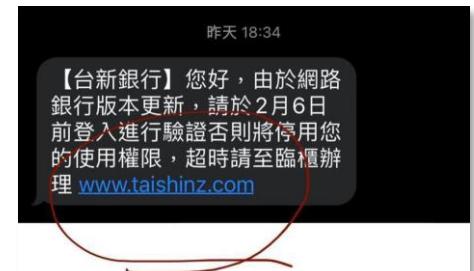
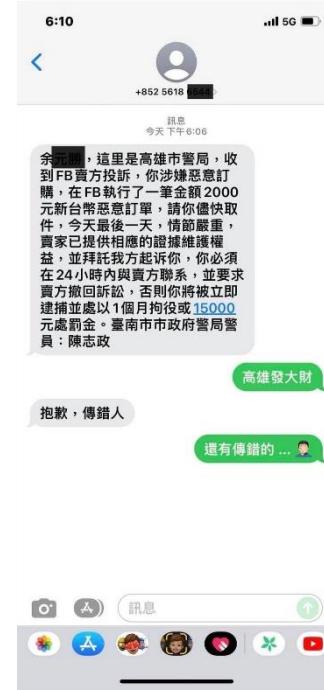
善用瀏覽功能(多次確認)

不管是連結、圖片，網址多看一點



造成情緒起伏請冷靜

■ 會造成情緒起伏的內容，先讓自己冷靜後再做判斷



注意可疑電子郵件特徵

確認信件資訊是否正確

① 寄件者：業務主管-王小明 <abc123@gmail.com> 寄件日期：2023/3/27 (週一) 上午 3:27

收件者：葉承翔 <benyeh@chtsecurity.com>

副本：

主旨：不匯款將對貴公司提出告訴

 |  匯款帳號.rar

④

⑤ 亲

最近我们公司帐号有更改

⑥ 请立即将款项汇入到 10248-458404480484084-454

⑦ 如不方便汇款，请连线以下网址

并依照附件档案指示步骤完成延迟汇款登记

⑧ [點我延遲匯款](#)

⑨ 以确保本案没有违约疑虑

如于今日尚未回覆，本公司将对贵公司提出告诉

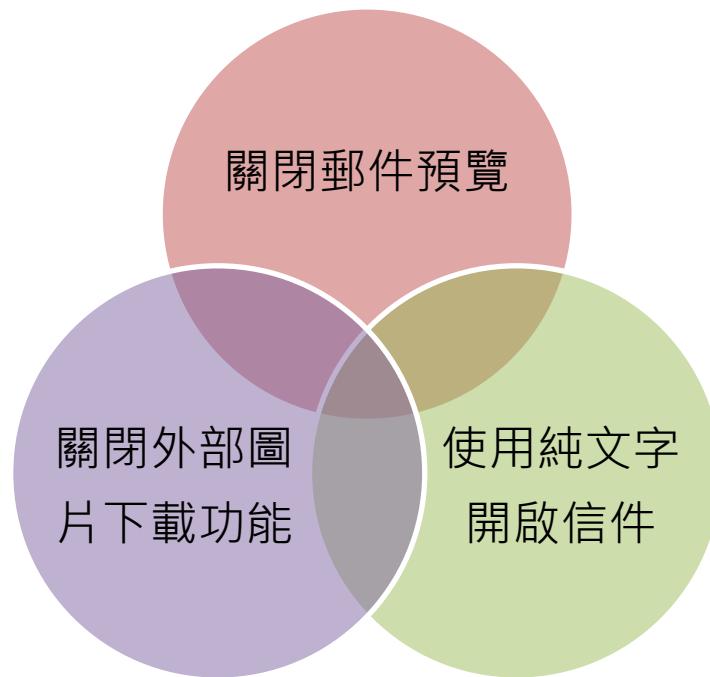
请维护贵公司权益

- ① 寄件者為公司同仁，但郵件位址非公司網域
 - ② 以非公務信箱寄送公務信件，或與自身業務
信件內容無關
 - ③ 觀察是否為不正常發信時間
 - ④ 主旨過於聳動的主旨與緊急要求、附件是否
有異常或與自身業務相關
 - ⑤ 注意內文的字是否為繁體中文，或與其習性
不符
 - ⑥ 要求立即執行
 - ⑦ 要求依照步驟/指示操作
 - ⑧ 確認網址是否異常
 - ⑨ 造成心情情緒起伏
 - ⑩ 無法判定，可撥電話與本人確認或請資訊單
位協助判斷
- ※※ 如發現異常，請透過不同管道詢問 ※※



中華資安國際

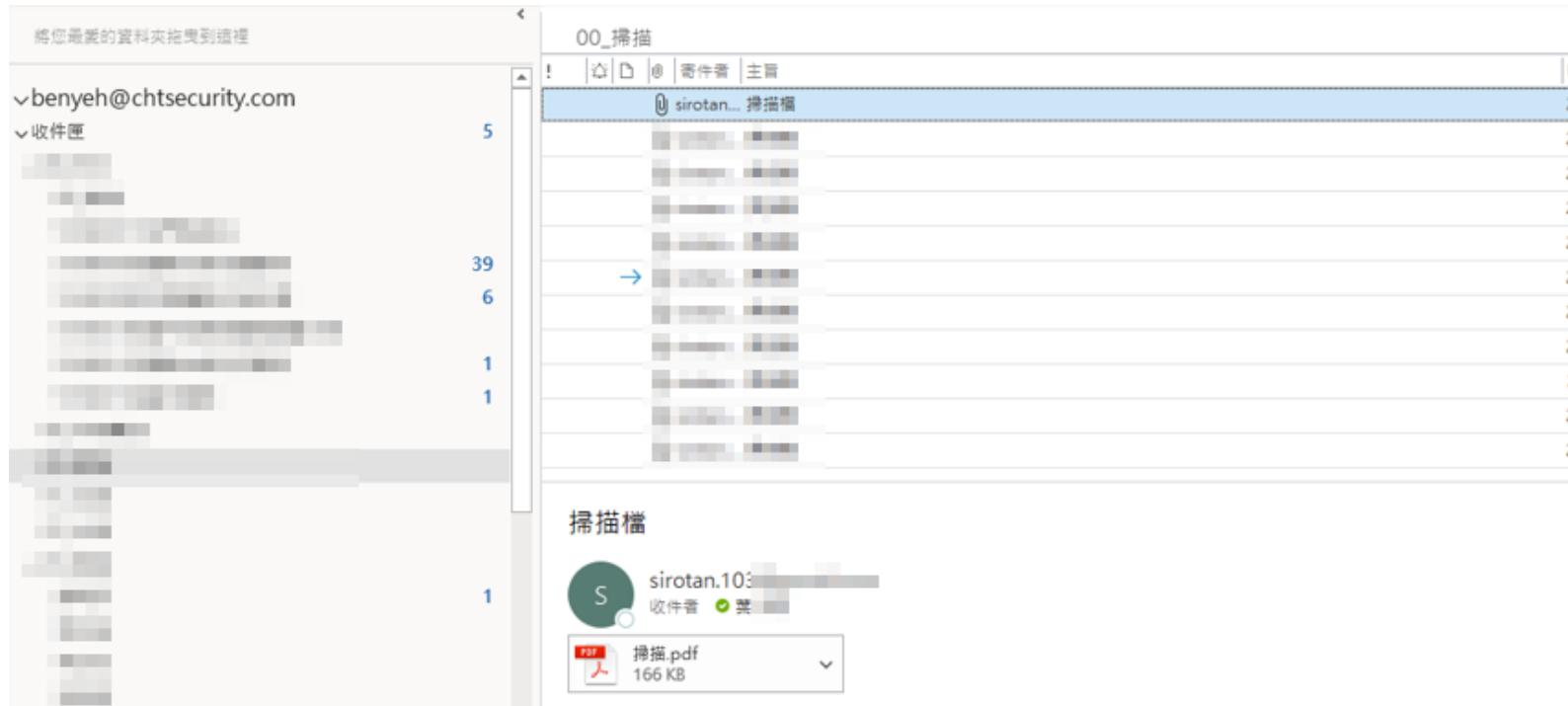
郵件軟體安全設定



中華資安國際

郵件軟體安全設定

- 避免誤觸惡意信件，建議關閉信件預覽



中華資安國際

郵件軟體安全設定

使用純文字開啟信件

2017/8/10 (週四) 上午 01:32
Steven Kao <steven.kao@citrix.com>
[外部郵件] 敬邀參加8月24日【Citrix Synergy Direct 2017 Taipei】盛會，將Synergy 精華盡收眼底！
收件者 undisclosed-recipients:
我們已將此郵件轉換為純文字格式。

Dear Sir,

敬邀參加 8/24 於華南國際會議中心舉辦的 Citrix Synergy 台北場，台北場的 Synergy 是整理出美國場 Synergy 的精華，特別針對與安全上的挑戰，內容絕對精采 (詳如下所述)，有興趣者可直接按“立即報名”來參加，謝謝。

Steven Kao 高林裕
Sales Manager , Taiwan
Citrix Systems Information Technology Ltd.
Tel: +886-2-8758 2929 <<tel:+886287582929>>
Fax: +86-2-8758 2999
Cellphone: +886-910 926 035 <<tel:+886910926035>>
Mailbox: steven.kao@citrix.com <<mailto:jason.shi@citrix.com>>

From: iThome 電腦報訊息快報 [<mailto:BestEvent@ithome>]
Sent: Tuesday, August 8, 2017 2:17 PM
To: daphne@mail.ithome.com.tw
Subject: (no header) 敬邀參加 8 月 24 日【Citrix Synergy Direct 2017 Taipei】盛會，將 Synergy 精華盡收眼底！

<HTML>

<HEAD>

- 1.<TITLE>標題列
- 2.<STYLE>樣式

</HEAD>

<BODY>

- 1.網頁主體
- 2.<H1>字最大，字型
- 3.圖片
- 4.超連結
- 5.<TABLE>表格，<TR>列，<TD>格
- 6.<FRAMSET cols= rows= >框架
- 7.<FORM>表單，<INPUT type= >

</BODY>

</HTML>

<<http://seminar.ithome.com.tw/mail/img/401/confirm-setting/kv.jpg>>

郵件軟體安全設定

■ 關閉外部圖片自動下載功能

寄件者：業務主管-王小明 <abc123@gmail.com> 寄件日期：2023/3/27 (週一) 上午 3:27

收件者：葉承翔 <benyeh@chtsecurity.com>

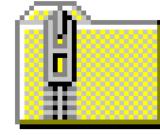
副本：

主旨：不匯款將對貴公司提出告訴

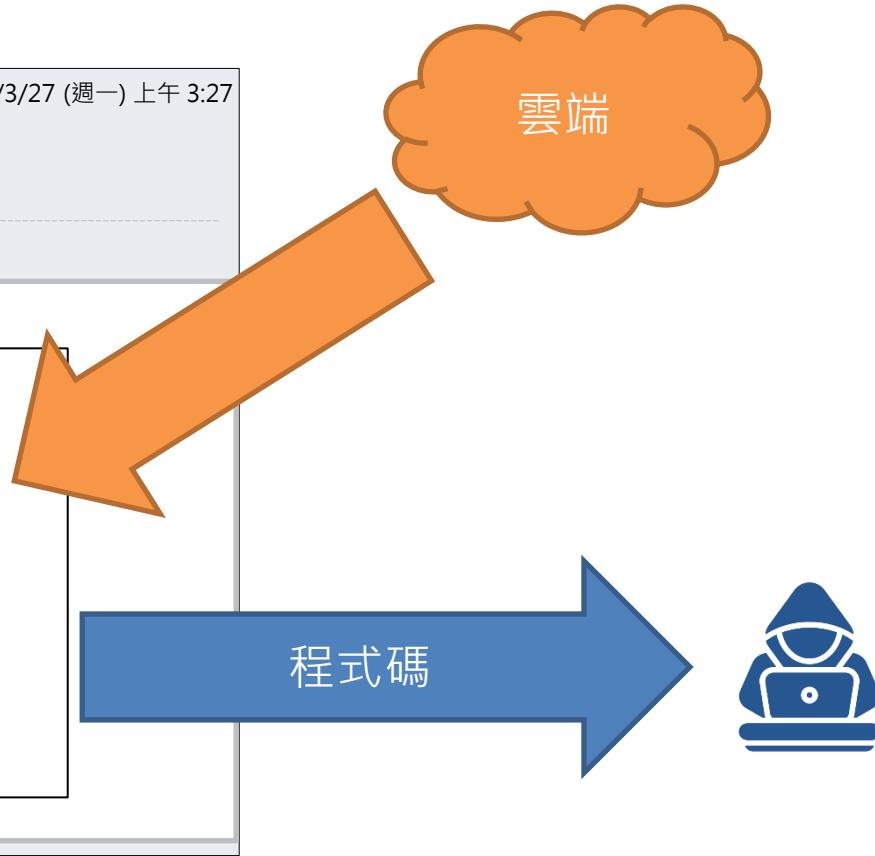
 |  匯款帳號.rar

我是一張圖

Save this image and change the extension to .zip!



source_code.zip



中華資安國際

社交工程注意事項

- 公私分明：將公務/私人的郵件/通訊**軟體分開**
- 疑人勿信：**勿點擊**可疑郵件/連結
- 提高警覺：陌生寄件者與**可疑信件要有警覺**，
從不同管道確認郵件內容正確性
- 付款驗證：供應商付款變更須有時間**再次查證**
- 資金轉移：使用**雙因子認證**
- **定期教育訓練**，培養資安意識及警覺性
- 建立及宣傳**回報機制**



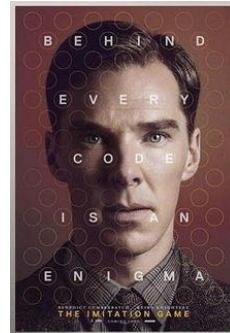
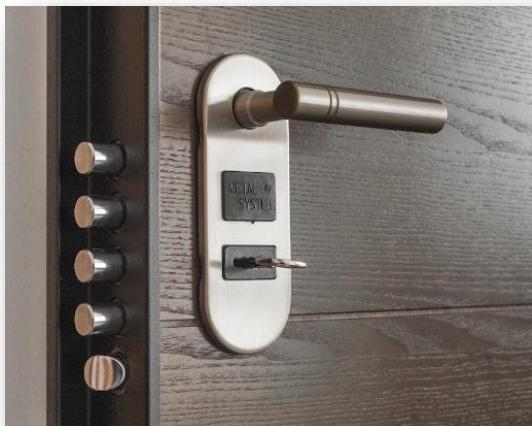
中華資安國際

密碼與密碼的未來



什麼是密碼？

- 密碼像什麼：好比家裡的門鎖
- 密碼功能：保護你的資產/個人隱私
- 最早的密碼：源於公元前1900年



<https://www.pexels.com/>

讓案例來說—密碼的重要性

7家證券期貨商遭「撞庫攻擊」 金管會祭3大措施

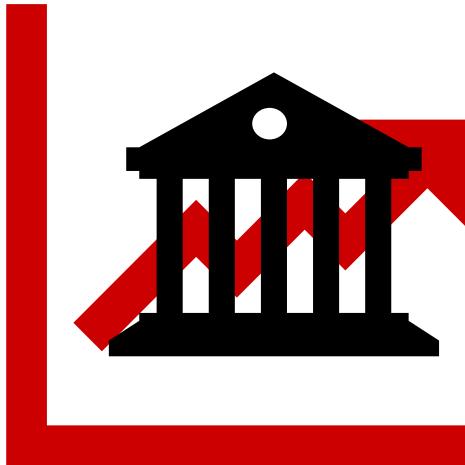
2021/12/15 07:40

「密碼撞庫攻擊」：是駭客利用民眾大量外流的電子郵件地址和密碼，再搭配自動化程式，冒用客戶登錄到券商網路下單系統進行交易；駭客不斷登錄網路服務，直到某一組帳號密碼被「撞」成功為止。

若為了方便好記，都取同一組帳號密碼，
駭客將暢行無阻



讓案例來說—密碼防護by券商



1. 加強宣導客戶定期更新使用者密碼
 - 應使用優質密碼設定並進行管控，確實執行密碼輸入錯誤次數達3次，必須予中斷連線。
2. 多因子認證方式
 - 提供網路下單服務，應於網路下單登入時落實採多因子認證方式，例如：下單憑證、綁定裝置、OTP、生物辨識等機制，強化憑證換發的驗證機制，以確保為客戶本人登入。
3. 每日針對核心系統的帳號登入失敗紀錄、非客戶帳號登入嘗試紀錄
 - 進行監控及瞭解分析異常登入原因、異常IP登入時通知投資人，並留存相關紀錄。



中華資安國際

讓案例來說—密碼防護by個人

密碼獨一無二，帳戶萬無一失

許多人為了記憶使用方便，常常會相同的用戶名和密碼來註冊，這就容易提供駭客不法攻擊的機會。

妥善保管，不隨意交給他人

金融機構提供的帳號及密碼，是作為客戶身分識別、認證及各項交易服務授權之主要工具，呼籲民眾要妥善保管，不要隨意交給他人。

避免於公共場所登入

民眾應避免使用圖書館、網咖、機場等地之公用電腦從事交易及輸入敏感性高的資訊，不宜在開戶證券商及期貨商以外之網站，提供或共用登入之帳號及密碼或交由他人保管，以免帳號遭冒用下單。



中華資安國際

用弱密碼，就好比....



這些都不要用喔!

<https://official-blog-tw.line.me/archives/37682230.html>



中華資安國際

密碼強度不足

- 老師說，密碼要這樣設才對

密碼複雜度要夠

大小寫英文
數字
特殊符號

定期變更密碼

每3個月變更1次
3代密碼不重複

密碼長度要夠

長度12碼以上

經過20年的努力，終於成功訓練
人們使用人腦很難記住，但電腦
很好破解的密碼



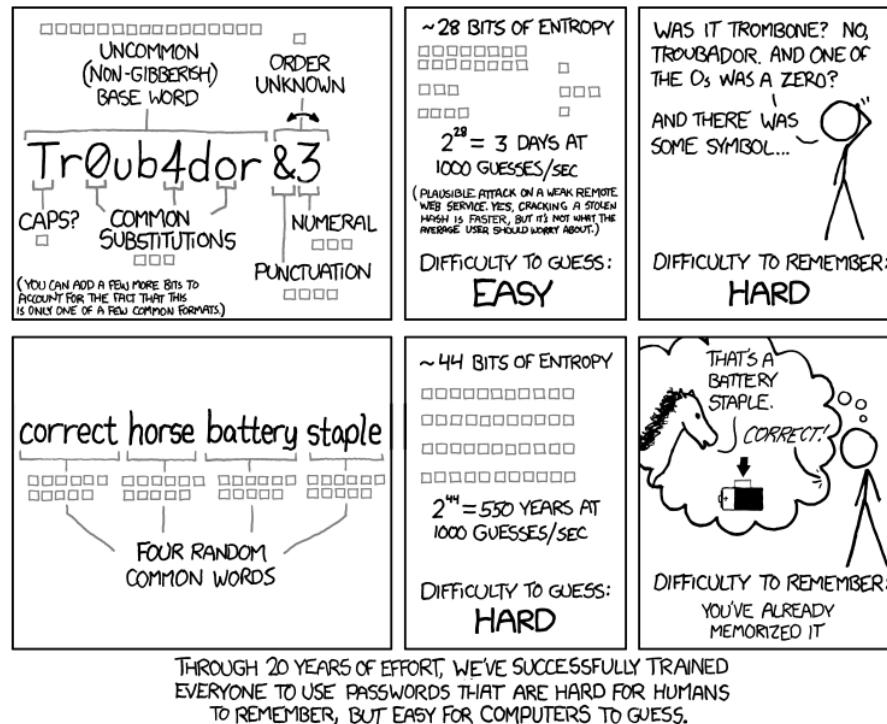
中華資安國際

密碼的安全性，跟你想的不一樣

(1) 平常大家想密碼時，總是思考大小寫、數字、特殊符號，結果卻讓**密碼複雜到難以記得，毫無關聯的密碼連回想都難！**

(2) 但這樣的密碼，其實對現行的電腦來說相當**簡單**，因為**密碼長度有限**。

(3) 但若是我們取密碼都用聯想的方式把單字串成片語，不僅簡單記憶，就算忘了也可以用聯想法回憶，對人腦來說是既方便又快速！



(4) 但聯想的片語密碼，對現行的電腦來說非常困難，因為他們要猜非常多的組合才能完美拼湊出你的片語密碼。

(5) 取密碼小建議：
將密碼使用單字組成一段片語，這個片語你可以使用聯想法記憶，方便人腦回憶的同時，也阻絕了電腦的猜測方式(暴力破解)，一舉兩得！

圖片來源：<https://xkcd.com/936/>



中華資安國際

現在風向變了

- ❖ 密碼複雜度規則發明人表示：對不起，我錯了
- ❖ 華爾街日報文中提到：這些難以記住的密碼、大小寫及定期更新的規則，並不是防止密碼外洩的最佳方式

THE WALL STREET JOURNAL.

[Subscribe](#) | [Sign In](#)

Asia Edition ▾ | May 31, 2019 | Print Edition | Video

[Home](#) [World](#) [U.S.](#) [Politics](#) [Economy](#) [Business](#) [Tech](#) [Markets](#) [Opinion](#) [Life & Arts](#) [Real Estate](#) [WSJ. Magazine](#)

Search 

A-HED

The Man Who Wrote Those Password Rules Has a New Tip: N3v\$r M1-d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

he regrets the error

【註】Bill Burr：密碼複雜度規則發明人

【資料來源】<https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118>

NIST改變心意

- NIST(美國國家標準暨技術研究院)文件 SP 800-63B
- 密碼複雜度要求過高，往往導致使用者設定更好猜測或有規則性的密碼，或直接將密碼記在便條紙上
 - Password1234變成P@\$\$w0rd1234
 - 你知道，我知道，黑客當然也知道
- 應該重視的是密碼的長度



圖片來源：<https://www.techbang.com/posts/11472-funding-is-the-biggest-vulnerability-people-united-kingdom-prince-william-public-attention-which-exposed-united-kingdom-forces-funding-concepts-how-bad>

密碼強度很足

- 現在的你，密碼可以這樣設！

密碼長度要夠
長度12碼以上

定期變更密碼
每3個月變更1
次
3代密碼不重複

密碼複雜度要夠
大小寫英文
數字
特殊符號

1. 使用多個英文單字連結起來的長密碼
2. 選擇幾個沒有關聯的詞語
3. 但對自己來說有意義且容易記住的英文單字加以組合



2022年最常見的10組密碼(台灣)

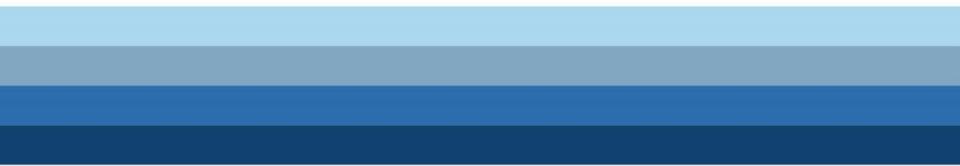
RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	vip	< 1 Second	27,458
2	123456	< 1 Second	4,110
3	1234	< 1 Second	3,421
4	000000	< 1 Second	1,361
5	1qaz2wsx	< 1 Second	1,219
6	12345	< 1 Second	1,197
7	12345678	< 1 Second	1,059
8	1111	< 1 Second	882
9	123	< 1 Second	847
10	123456789	< 1 Second	800

<https://nordpass.com/most-common-passwords-list/>



中華資安國際

強化你的密碼安全



多因子認證 Multi-factor authentication/MFA

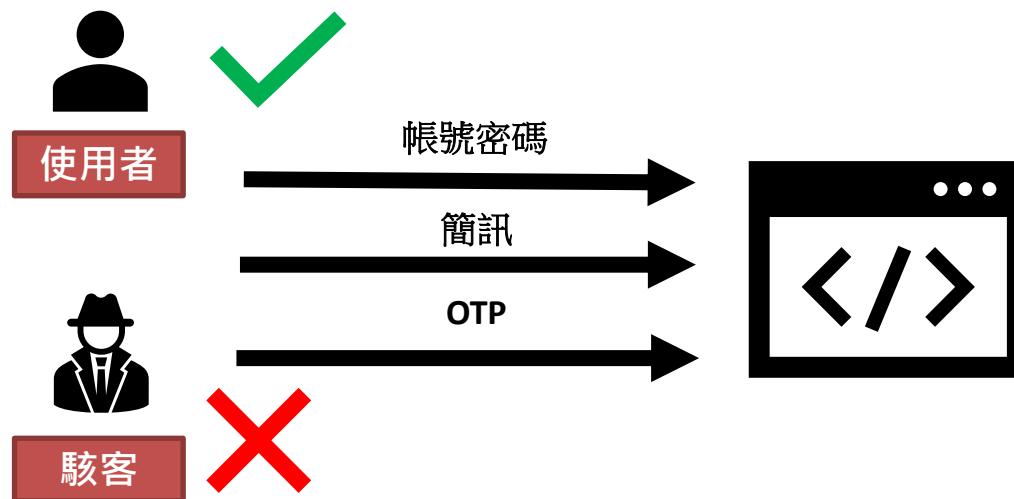
使用者要通過兩種以上的認證機制之後，才能得到授權，例如：

1. 知識因素：例如密碼、PIN碼或者安全問題的答案。
2. 物理因素：例如智能卡、USB密鑰、手機或其他可穿戴設備等。
3. 生物特徵因素：例如指紋、面容識別、聲音識別、虹膜識別等。



多因子驗證的保障

在多因子認證中，用戶需要提供多個身份驗證因素，而攻擊者必須同時攻擊多個身份驗證因素才能夠繞過身份驗證，因此多因子認證可以提高身份驗證的安全性。



廣泛運用的多因子認證

- 多因子認證已經廣泛應用於許多不同的場景，例如在網上購物、網上銀行、企業資源管理、政府網站等。對於敏感性高的信息和操作，例如金融交易、個人身份識別、敏感性企業數據等，多因子認證是非常重要的。



中華資安國際

多因子認證的隱憂

駭客可利用社交工程攻擊，來獲取受害者的身份驗證因素，請隨時保持警惕，勿隨意透露自己的身份驗證因素。此外，多因子認證需要額外的設備或APP支援，對於用戶和系統管理員都需要增加成本和管理費用。



開啟多因子認證，強化安全性



多因子認證是甚麼？

The image consists of two main parts. On the left, there is a screenshot of a web-based MFA login page. It features four input fields: '身分證字號' (Identity Card Number), '使用者代號' (User ID), '使用者密碼' (User Password), and '驗證碼' (Verification Code). The '驗證碼' field contains the number '589169'. Below these fields is a large red button labeled '登入網銀' (Log in to Online Banking). On the right side, there is a conceptual diagram titled '多因素身份驗證' (Multi-factor Identity Verification). This diagram is divided into three columns: 'What you know' (包含密碼, 圖形鎖, 手勢; 身份證字號, 使用者代號, 使用者密碼), 'What you have' (包含自己的設備, NFC 卡片, 穿戴裝置; 手機), and 'What you do' (包含地理位置, 網路行為, 擊鍵模式; 手指點擊). Each column has a corresponding icon: a lock for 'What you know', a smartphone for 'What you have', and a hand interacting with a keyboard for 'What you do'.

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9150

密碼的未來



無密碼該怎麼登入？



中華資安國際
91

FIDO聯盟

- 主推動開放式標準和技術，**提高身份驗證的安全性和便利性**。
- FIDO成員為硬軟體和服務供應商、金融機構、企業和政府等各種組織，其中包含**Google**、**APPLE**、**Microsoft**、Visa、Mastercard、Paypal、Samsung、Intel、Qualcomm等知名企業。
- 技術框架**支持多種身份驗證方法**，包括生物識別、PIN碼、指紋、聲紋、面部識別等。這些驗證方法可以與現有的技術和協議結合使用，例如OAuth、OpenID Connect等。



無密碼新時代

- 身分保管責任分散在裝置端，伺服器不集中保存密碼
- 仰賴兩大關鍵技術的成熟——生物辨識與安全模組
- 支援使用者以實體安全金鑰的裝置

【全面解析FIDO網路身分識別】無密碼新時代將至！解決網路密碼遭竊與盜用問題

傳統密碼安全性不足的問題不斷，帳號遭盜用的事件層出不窮，為了擺脫這些困境，新世代的網路身分識別FIDO標準興起，並在2019年將有大幅成長態勢，不少雲端業者都看中此一發展，陸續開始支援這樣的應用

文/ 蘿正漢 | 2019-02-05 發表

Traditional authn model (e.g. password) for web applications

The diagram illustrates the difference between traditional authentication models and FIDO authentication models. In the traditional model, a user enters their ID and password (ID + PWD) into a computer, which then sends the information to an Authentication server. The server performs Identification and Verification steps to determine if the credentials are correct (OK). In the FIDO model, the user has a FIDO Client (which includes a User, Authenticator, and Credential). The client performs its own Verification step and sends the results to a FIDO Server. The server then performs its own Identification step to verify the results. A purple arrow labeled 'separation' points from the traditional model towards the FIDO model, indicating that the FIDO model separates the verification process from the authentication server.

FIDO authn model

User, Authenticator, Credential

Verification results

OK

Identification

Verification

Authentication

ID + PWD

OK

Identification

Verification

FIDO Authentication

FIDO Client

FIDO Server

separation

【FIDO認證模式的一大重點，伺服器端將不再保管祕密】不同於傳統網路服務的密碼驗證，FIDO認證模式是將身分「驗證」與「識別」拆分開，用戶端需搭配認證器，來做到身分驗證，並採公私鑰架構來保障安全，同時，在FIDO伺服器上，只有保存公鑰不保存密碼或私鑰，因此也就不存在分享秘密的問題。圖片來源 / FIDO聯盟



中華資安國際

Apple官方對Passkey與其他保存密碼方式的比較

The screenshot shows a video player interface from the Apple Developer website. The title of the video is "Authentication methods". Below the title is a comparison table:

Protects against	Memorized password	Password manager	Password manager + SMS/TOTP	Passkey
Guessing	✗	✓	✓	✓+
Credential reuse	✗	✓	✓	✓
Device theft	✓	✗	✗	✓
Phishing	✗	✗	✗	✓
Server leaks	✗	✗	✗	✓

曾於2022/06率先宣布將新推Passkey，利用一張表說明與密碼記憶、密碼管理器，以及密碼管理器加上SMS/TOTP相比，Passkey在5個威脅層面（猜密碼、帳密再利用、裝置失竊、網路釣魚、帳密伺服器資料外洩）上的差異與優勢。



中華資安國際

正在步入無密碼世界

iThome



【2023資安趨勢2：無密碼網路身分識別】

無密碼身分驗證朝向普及應用

多家國際業者開始支援Passkey登入

PassKey將帶動新一波應用潮流，臺灣金融FIDO應用正要成形，IoT身分認

企業類型	公司或網站服務名稱
資訊科技業者	微軟、Nvidia、DocuSign、Zoho、FormX.ai、Horizon Pics、Pastery、Virgin Media
金融服務業者	PayPal、Robinhood、Arpari、Card Pointers、Money Forward ID
電商購物平臺	Best Buy、eBay
社交平臺	Mangadex、omg.lol
旅遊與休閒業者	Kayak、Scrooge Games
身分安全供應商	Authgear、Corbado、Hanko、Passage
房地產服務業	The Hendrix

資料來源：1Password，iThome整理，2023年1月 註：統計截至2023年1月11日止

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9150



中華資安國際

密碼總結

絕對不要採用的密碼類型

下列為不安全的密碼設定，請千萬要避免：

1. 不設定密碼（空白密碼）
2. 使用簡單字元組合或全部都是數字（如 1234、abcd、111111 等）
3. 密碼與帳號相同
4. 使用生日、身分證字號、英文名字等個人資料
5. 使用公司、部門、單位名稱
6. 使用與系統管理相關專有名詞（如 admin、password 等）
7. 鍵盤順序組合（如 asdfgh、1qaz 等）



中華資安國際

密碼注意事項

- **不重複使用帳號密碼**：雞蛋不放同個籃子，帳號密碼請不要都取同一個！
- **定期更換密碼**：跟駭客的時間賽跑，千萬不要賭自己會贏！更換密碼讓終點遙不可及！
- **請勿將帳號提供予他人**：多打一把鑰匙給陌生人，讓陌生人可以任意進出你家！



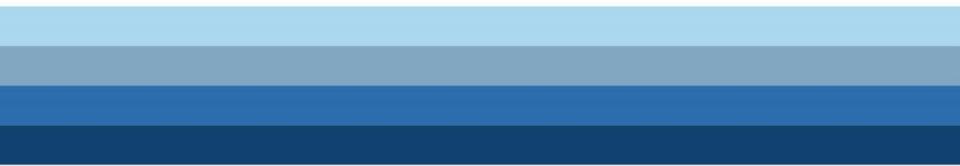
https://isafe.moe.edu.tw/pack/2293?user_type=4&topic=9

<https://www.pexels.com/zh-tw/>

輸入密碼時，看到以下網址列訊息該如何判斷？



WIFI與IoT設定



WiFi設定不良



Wireshark · Follow TCP Stream (tcp.stream eq 11) · wireshark_547FD3C2-C975-44C3-AEE4-D7CD69E549_20200618115037_a20792

HTTP/1.1 200 OK

... [33;1mPTT.[m .P
.. [1m140.112.172.11 .[m.P ...
.z.w.{ .[33;1m.....~.{[m ..
.x.[1m.V.[m.{ .[imptt.cc .[m ..
.x.[1m.V.[m.{ .[imptt.cc .[m ..
.w.{ .x.z.w.w.{ .P ..
.t .[33;1m.V.[m.x .P
.x.z.w.w.w.{ .[47m.i.
.z.w.r.{[1m.V.[33m.V.[m | ...[47m.i.
.x.[1m.V.V.[m ...[47m.i.
.....[H.[2]
...[47m ...[43m...
.[47m .[43m*[33;47m
.30;47m.o .[43m.d.e"
.47m .[43m.n.[30m=d
.34;47m.k.[30m=d
.30;43m*. [37m@
.44m .[34;43m.k.[30m=9
.44m .[34;43m.d.[37m@
.44m .[30m...[32;40m...42
.44m .d.[30m.f.[37;40m /-[42m
.44m .[47m .[40m|[30;42m
.44m .[47m .[40m|[30;42m
.44m .[34;47m.k .B.[37;40m.k...
.44m .[34;47m.j \|[37;40m }
.44m .[34;47m{ [37;40m.k.d
.44m .[34;47m\ .[37;40m.g.[3
.44m .[34;47m.o / ..
.33m.w....[1;36m.....~.{[33m
...[1m.....e...].**@ntu.edu.tw ...U.b...C.[m
.21;1H.[K.[0;1;37;41m...N...z...s.u...w...l.m.[21;1H.[K.[m.....J.N...A...H guest ...[A...H new ...U: .[7m
.....ANSI...x.....mmyyuusseerrnnnaamme
.m.[22;1H.[K.[m.....J.z...K X: .mypassword
.22;1H.[K.[m...b...d.b...P...X:[22;1H.[K.[m.K.X.....L...b...C.....j.p.g.....L...J...~.C.[21;1H.[K.[m.....J.N...A...H guest ...[A...H new ...U: .[7m
.....

明碼傳輸，易遭竊聽

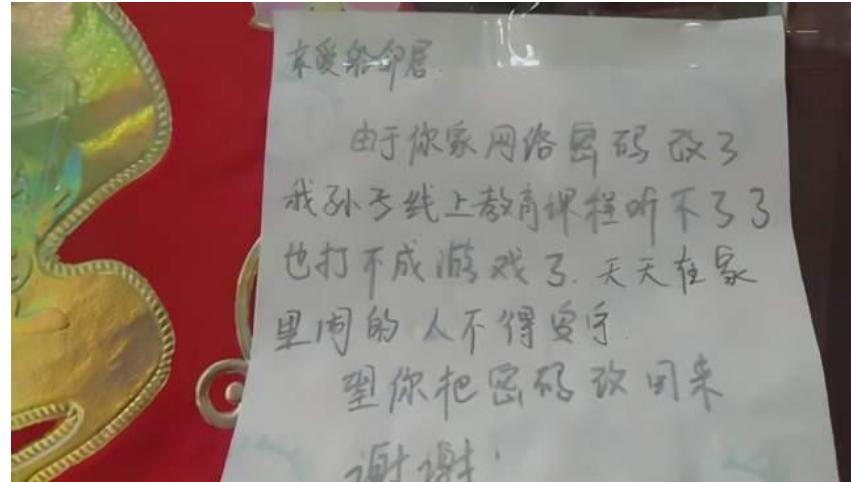
27 client pkts, 16 server pkts, 27 total
Entire conversation (3769 bytes) Show and save data as ASCII
Find: Stream 11



中華資安國際
100

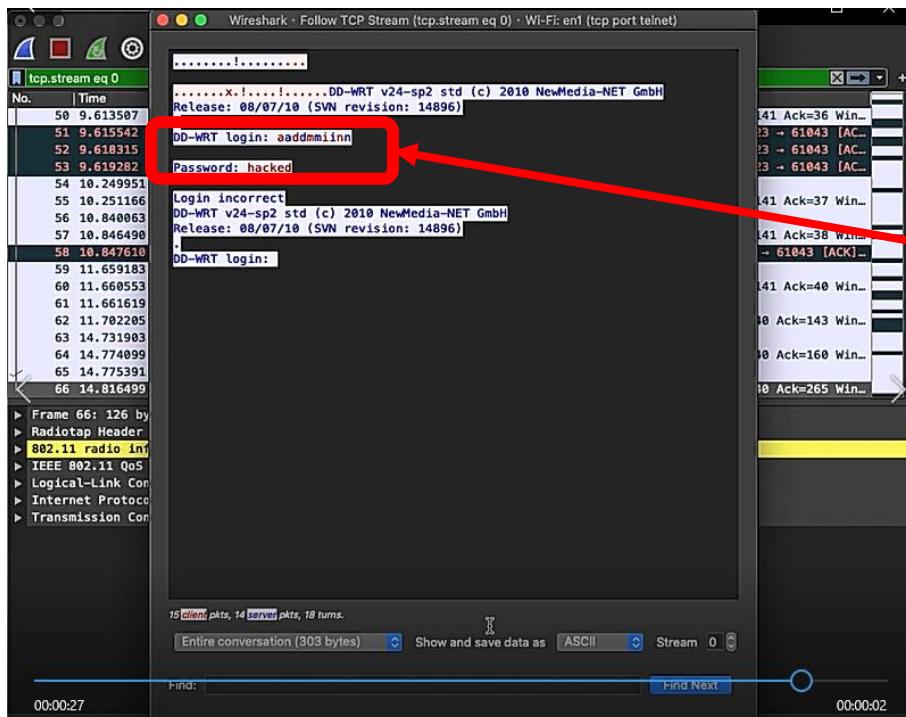
WiFi 密碼的重要

- 避免被偷用
 - 影響頻寬，看劇卡卡
 - 流量側錄資料外洩
- 避免背鍋
 - 當跳板、肉雞
 - 釣魚網站



<https://www.bilibili.com/s/video/BV1P7411Z7SY>

來看看沒加密的連線有多危險



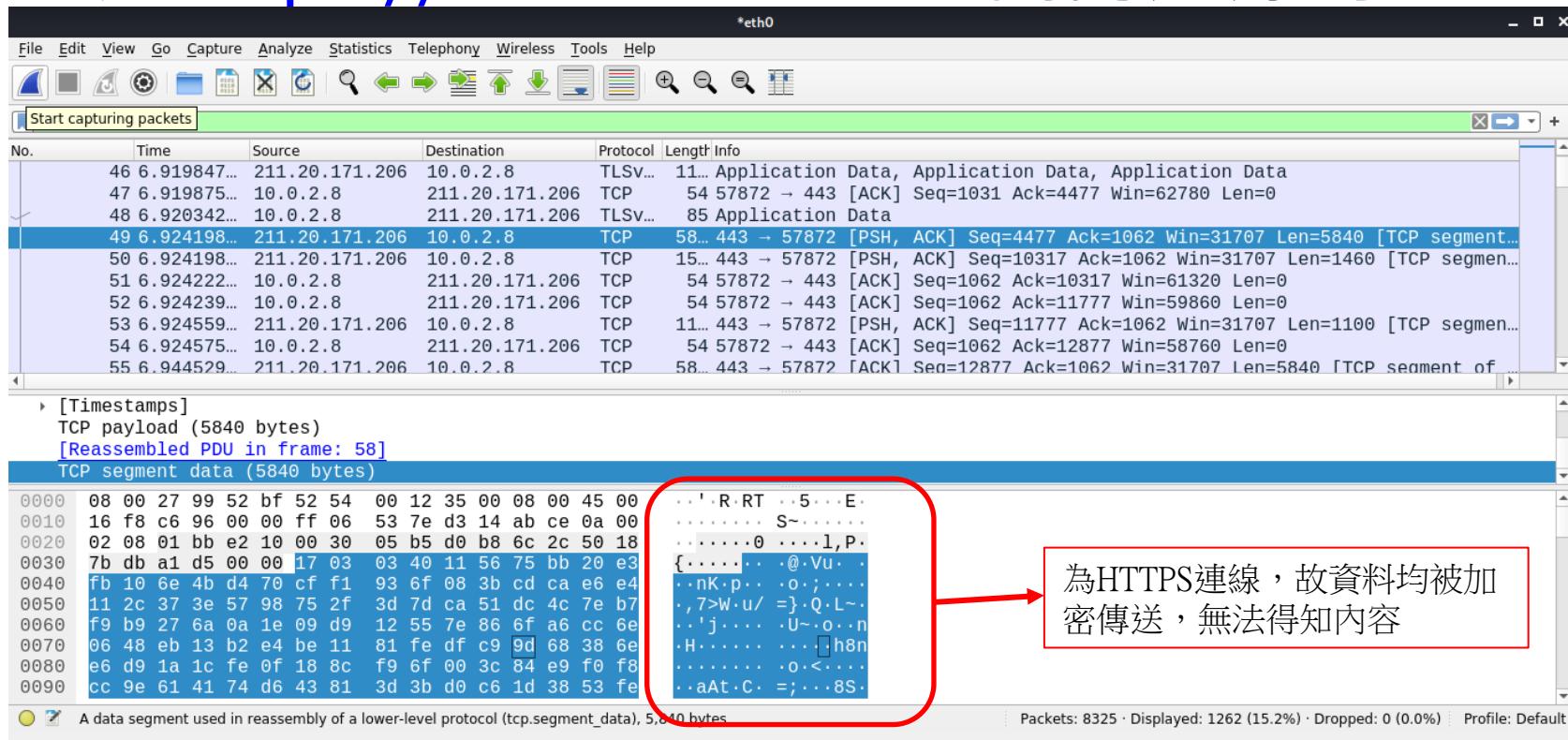
惡意人士電腦，遠端截取網路封包
(使用特殊網卡，不需連線至任何WiFi AP)



受害者電腦，在未加密WiFi環境下使用
telnet連線(未加密連線方式)

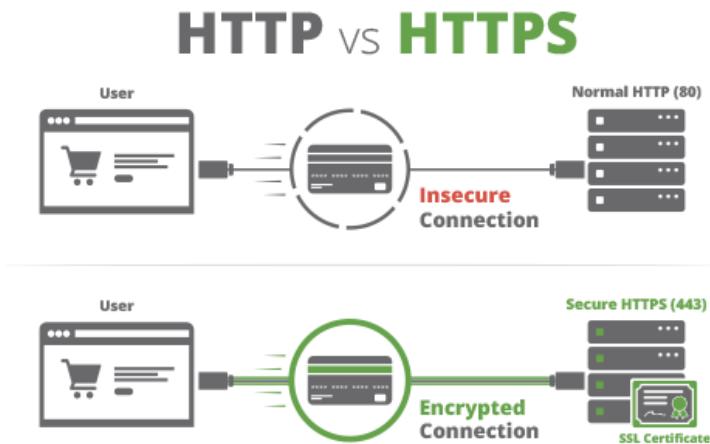
有加密的連線，比較安全一點

- 與 <https://www.hinet.net> 間的連線封包



HTTP/HTTPS 與 SSL/TLS

- 一般網頁(web)使用HTTP協定傳輸資料
 - 傳輸資料未加密
 - 易遭竊聽，導致機密資料外洩
- 建議使用HTTPS協定，加密傳輸資料
- HTTPS支援2種加密協定
 - SSL(Secure Sockets Layer)
 - 較老舊，弱點多，例如SSL 3.0的POODLE弱點
 - TLS(Transport Layer Security)
- 建議使用TLS V1.2以上版本，關閉SSL，以強化安全性



瀏覽網頁時，注意網址列的「鎖頭」圖示



安全!



小心!，網站可能未使用HTTPS連線，傳輸資料易遭竊取



小心!，HTTPS所使用的憑證，簽發者不受信賴，可能是假冒的網站



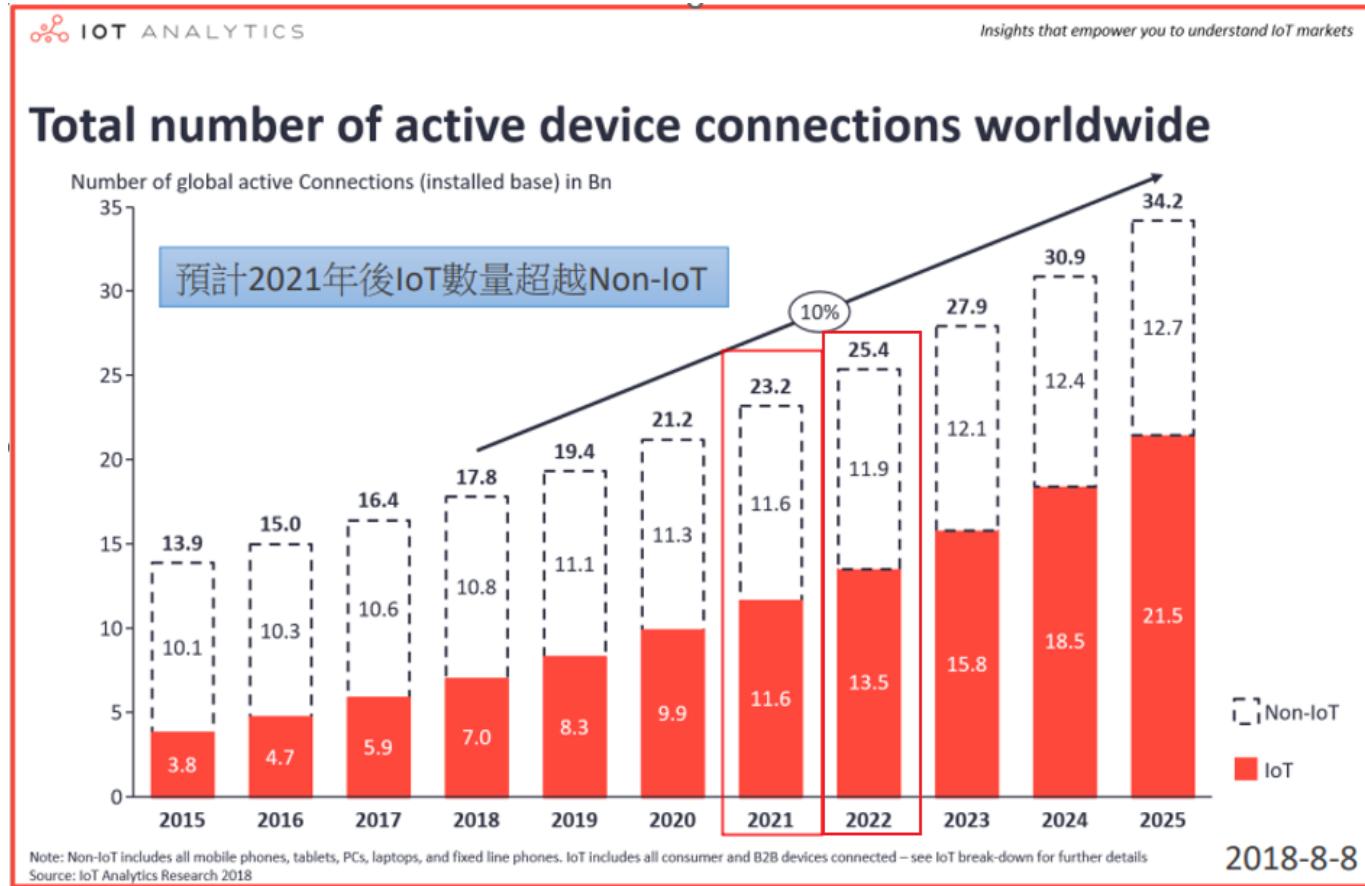
【註】以上以chrome瀏覽器為例

IoT特性與資安困境

- 定義涵蓋廣泛（萬物聯網、IoT）
 - • 攝影機、汽車、印表機、投影機、電視、手機...
- 效能與資源限制
 - • 電量限制、運算能力低、儲存空間不足
 - • 網路流量低、可能採間隔喚醒/睡眠機制
 - • 大多採取明文傳輸（加密成本高）
 - • 認證方式簡易
- 生態系多元，不易標準化管理
 - • 客製作業系統、更新速度緩慢
 - • 自訂Protocol
 - • 各類無線通訊(WLAN/WPAN/LPWAN/Cellular/WNAN)
- 家庭應用缺乏資安預算與安全法規



IoT發展趨勢 – 設備數量預測



物聯網時代的商業趨勢

1. 資料販售與交換（羊毛出在狗身上，豬來買單）

特徵：資料為王EX：Nest

硬體價值壓縮：廠商販售或交換使用者的資料盈利

2. 產品即服務

特徵：有感服務EX：Tesla、奇異、中興保全MyVITA、Dropcam

透過軟體升級，提供給使用者更好的服務：廠商售出硬體產品後，利用大數據分析、軟體升級、直接提供人力、售後服務盈利

3. 產品共享EX：YouBike、Irent

特徵：共有共享

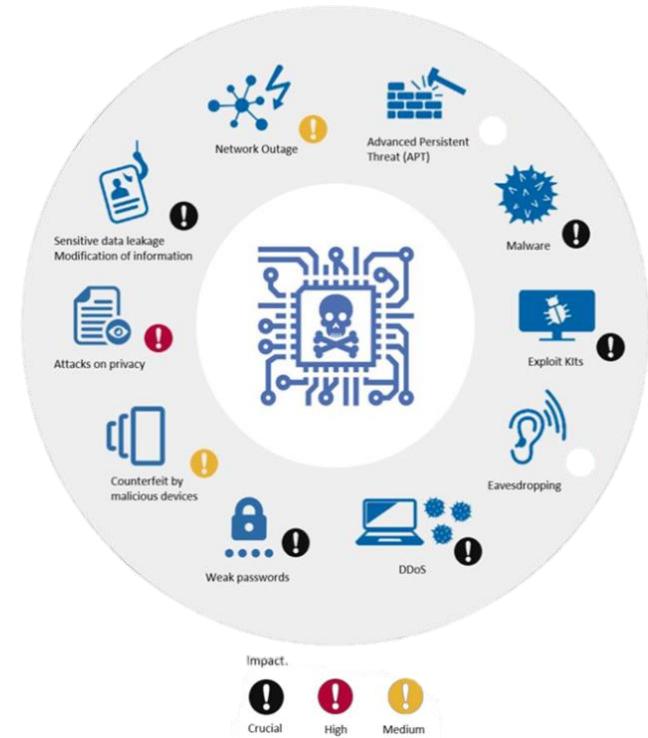
廠商擁有硬體產品，使用者依硬體使用量付費



<https://www.marketersgo.com/marketing-tools/201601/sheep-dog-pig/>

無所不在的威脅

- 物聯網帶來許多前所未有的全新攻擊面向
- 駭客只要有電話線跟傳真號碼就能攻陷企業印表機
- 駭客從智慧溫度計無線介面侵入賭場資料庫，撈出豪賭大戶名單
- 只要設備中有麥克風和揚聲器，設備之間就可以用聲音進行數據傳輸
- 研究人員證實可以利用雷射光聲控家中的Google Home、Alexa、Siri
- 研究人員透過聲音在電燈泡玻璃表面上產生的微小振動遠端竊聽
- 你家裡的掃地機器人會監聽你！？資安專家發現最新監聽技術！



個資與隱私安全

APP 追蹤你...



中華資安國際
111

個資是什麼？

自然人之姓名、出生年月日、
國民身分證統一編號、護照號碼、
特徵、指紋、婚姻、家庭、教育、職業、
病歷、醫療、基因、性生活、健康檢查、犯罪前科、
聯絡方式、財務情況、社會活動
及其他**得以直接或間接方式識別該個人之資料**

特種個資

特種個資原則上不得蒐集、處理與利用

個資法第6條例外狀況：

- 一.法律明文規定
- 二.公務機關執行法定職務或非公務機關履行法定義務且事前或事後有適當安全維護措施
- 三.當事人自行公開或其他已合法公開
- 四.公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的
- 五.協助公務機關執行法定職務或非公務機關履行法定義務且事前或事後有適當安全維護措施
- 六.當事人書面同意



個人資料無所不在，個資事件層出不窮



這些資料外洩了，怎麼辦？



英國國稅局蒐集聲紋違反GDPR

英國國稅局蒐集聲紋違反GDPR，將刪除5百萬筆民眾紀錄

為加速作業流程，英國民眾在打電話給國稅局時，會被要求錄下語音並存放於聲紋資料庫，隨著GDPR上路，這項蒐集聲紋資料的行為也被質疑合法性

文/ 林妍潔 | 2019-05-06 發表

1 論 6.1 萬 按讚加入iThome粉絲團 1 論 549 分享

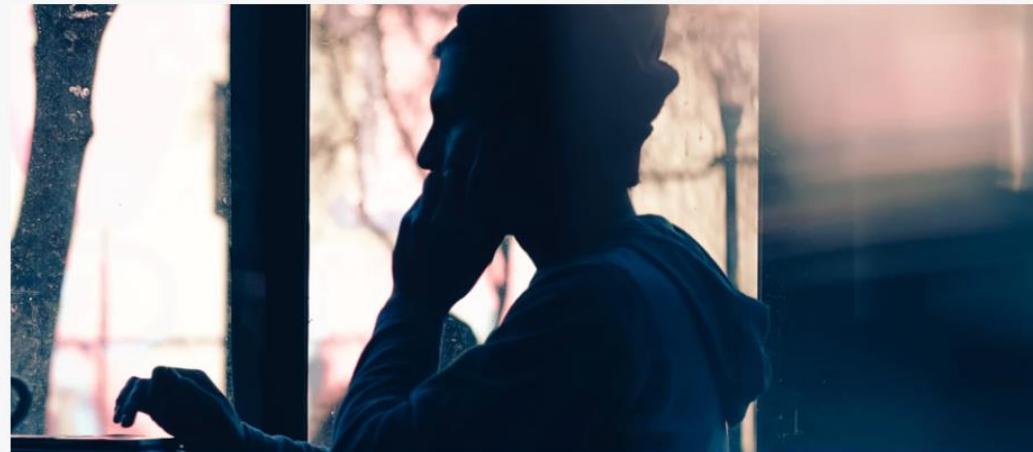


Photo by Hannah Wei on Unsplash

便民

用於驗證身份
加速民眾服務流程

VS

自由行使同意或拒絕權利
揭露或告知其用途及處理方式

合法

男大生買書遭詐13萬控個資外洩



https://www.youtube.com/watch?v=aS9_DaPow2g

爆資安疑慮 近150萬筆個資全都露

- 自由電子報 2021-02-03
- 台中市府舉辦為期2個月「台中女麗購」，以天天抽、

A	B	C	D	E	F	G	H	
499985	NO_00999985	W7H1E	U000274385	林	987	9871	NULL	
499986	NO_00999986	W7HSX	U000434708	陳	937	9377	NULL	
499987	NO_00999987	W7J2I	X	U000443290	楊	910	9102	NULL
499988	NO_00999988	w7tNS	U000431645	黃	961	9613	NULL	
499989	NO_00999989	w7TQ'	U000143615	盧	921	9217	NULL	
499990	NO_00999990	W7tyE	U000441115	劉	NULL	9319	a093199	
499991	NO_00999991	w7uLz	U000168713	陳	939	9395	NULL	
499992	NO_00999992	W7VB	U000437963	詹	963	9631	NULL	
499993	NO_00999993	w7v0t	U000353527	Tan	937	9375	tammy_h	
499994	NO_00999994	W7VU	j	U000105662	林	9114	www881	
499995	NO_00999995	w7V2x	U000195665	陳	939	9395	NULL	
499996	NO_00999996	w7W3	I	U000343569	黃	916	9162	NULL
499997	NO_00999997	W7W7	U000443017	陳	NULL	9524	sandy10X	
499998	NO_00999998	W7wdl	U000428855	詹	919	9196	NULL	
499999	NO_00999999	w7wcc	U000436971	楊	930	9305	NULL	
500000	NO_01000000	w7wEI	U000394282	李	955	9551	NULL	
500001							normal	
500002							normal	
500003							normal	

20210201年檢(第2稿).xlsm

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，主辦的經發局仍負連帶損害賠償責任。

員工疏忽、欠缺資安意識 危言聳聽？



[REDACTED] "身分證"

X |

全部

新聞

圖片

地圖

影片

更多

設定

工具

約有 1,700 項結果 (搜尋時間 : 0.28 秒)

[http://\[REDACTED\]](http://[REDACTED]) › enable › uploads ▾ XLS

轉出

1, 寒暑假轉入學生名單校內通報表. 2, 班級, 學號, 姓名, 性別, **身分證字號**, 北市, 外縣市/國外. 3,
104, 100078, 陳 [REDACTED] 4, 104, 100079, 鄭 [REDACTED]

<http://www.cchs.tp.edu.tw> › 重慶國中保有個人資料... ▾ XLS

工作表1 - 重慶國中

14, 5, 外聘教師鐘點費印領清冊, 依人事行政管理取得個人資料, 為辦理學生畢業旅行, 辦理參加
老師保險, 002人事行政管理, C003**身分證**字號, 訓育組.

[http://www3\[REDACTED\].gov.tw](http://www3[REDACTED].gov.tw) › PDF XLS

成績 [REDACTED]

2019年5月7日 — 5, 編號, 中文姓名, 英文姓名, 學號*, E-mail(帳號), **身分證**字號(即密碼), 出生日期(西元年), 科目, 版本, 班級, 試場, 試場位置, 姓名資料確認, 需修正 ...

全台個資洩？有地址查全家



APP 追蹤你...

- 從 iOS 14.4 開始，Apple 要求所有上架 App Store 的 App 需要提供該 App 使用與追蹤了客戶哪些隱私資料

The Apps collecting your data for their own benefit

| FB 與 IG 蒐集最多個人資料

在所有被調查的 App 中，Facebook 與 Instagram 蒐集了最多個資並使用在對其有利的方面，蒐集了高達將近 86% 的個資來向使用者販售相關產品以及投放廣告，而這兩個 App 都是 Facebook 旗下的產品；再來是 Uber 和 Uber Eats，他們搜集使用者的數據分析後，可以知道你在每一週的何時比較常出沒與使用 App 的地區及時間，便會針對該日及該地點相關資訊向您提供廣告。

Rank	App	Category	Privacy Score (%)
6	Uber Eats	Food Delivery	57%
7	eBay	Commerce	50%
8	Just Eat	Food Delivery	50%
9	LinkedIn	Professional Network	50%
10	Twitter	Social Media	50%

<https://applealmond.com/posts/92060>

FACEBOOK 隱私設定

- 路徑：帳號 > 設定和隱私 > 隱私設定檢查

隱私設定檢查

我們將會引導你進行設定，以便為帳號選擇適合的選項。

想先從哪個主題開始呢？

...

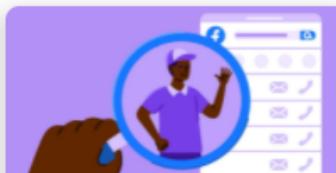


你分享內容的對象

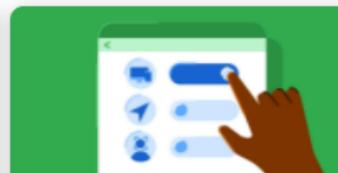


保障帳號安全的方式

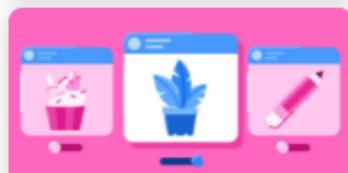
約 1 個月前



其他人可以在 Facebook 上找到你的方式



你在 Facebook 上的資料設定



你的 Facebook 廣告偏好

4 天前



中華資安國際
120

FACEBOOK 隱私設定

• 分享內容的對象



個人檔案資料

請檢查來自你個人檔案的這些資料，並決定你想讓誰看。資料可能只佔你個人檔案的一部分。

未來貼文

選擇哪些人能查看你未來發佈的貼文。此分享對象將可以查看你的貼文，直到你再次變更分享設定。你每次建立新貼文皆可變更分享對象。

限時動態

控制哪些人能查看你的限時動態。限時動態會在 Facebook 和 Messenger 顯示 24 小時。

限制舊貼文分享對象

將分享對象為「所有人」或「朋友的朋友」的舊貼文變更為僅限「朋友」。所有被標註在這些貼文中的用戶和他們的朋友可能仍然看得到貼文。

封鎖

你封鎖某人後，對方將無法再看到你在自己動態時報上發佈的內容、標註你、邀請你參加活動或社團、與你開始對話或加你為朋友。

提示：你封鎖某人後，我們不會通知對方你已封鎖他們。

+ 新增用戶到封鎖名單

返回 繼續

只限本人



中華資安國際
121

FACEBOOK 隱私設定

• 保障帳號安全的方式



保障帳號安全
我們將逐步指引你保
護你的密碼安全度。
啟用雙重驗證
開啟登入警告

密碼是否只有你自己知道？
如果你將 Facebook 密碼用於其他網路空間，選擇安全度較高的密碼，以保護你和你的 Facebook 帳號。

密碼設定祕訣

- 選擇你並未在其他網路空間用過的密碼。
- 密碼應可讓你輕鬆記住，但其他人難以猜測。
- 切勿向他人透露你的密碼。

更改密碼

返回 **繼續**

加強保護帳號安全
你啟用雙重驗證後，如果我們發現有人嘗試從不明裝置或瀏覽器登入，就會要求你提供驗證碼。

安全提示

- 你可以使用一組密碼。
- 你無法將已用過的密碼再用。

控制登入警告
說明你偏好的通知方式，以便我們在有人從不明位置登入你的帳號時通知你。我們會告訴你對方使用的裝置和所在地點。

Facebook 我們會傳送 Facebook 通知給你。

Messenger 我們會傳送 Messenger 通知給你。

電子郵件地址 我們會寄送通知到 [redacted]

返回 **繼續**

FACEBOOK 隱私設定

- 其他人可以在 Facebook 上找到你的方式

其他人可以在 Facebook 上找到你的方式

我們將會一一說明各個選項

交友邀請

你可以控制誰能傳送交友邀請給你。

誰可以傳送交友邀請給你？

提示：如果你收到過多不想要的交友邀請的朋友。

待確認的交友邀請

確認 刪除

確認 刪除

返回 繼續

手機號碼和電子郵件地址

選擇誰可以使用你的手機號碼和電子郵件地址找到你。

手機號碼

電子郵件地址

提示：用戶同名同姓的情況並不罕見，因此我們有幾位在 Facebook 找到彼此。

搜尋引擎

搜尋引擎（例如 Google）可以連結你的個人檔案，協助用戶更容易找到你。

關閉此設定後，如果其他人搜尋你的姓名，還是可以在 Facebook 找到你的個人檔案。

是否要讓 Facebook 以外的搜尋引擎連結你的個人檔案？

返回 繼續

所有人
所有 Facebook 的用戶和非用戶

朋友的朋友
你的朋友的朋友

朋友
你的 Facebook 朋友

只限本人

FACEBOOK 隱私設定

- 你在 Facebook 上的資料設定

The image contains two screenshots of the Facebook mobile application interface.

Screenshot 1: 應用程式和網站 (Applications and Websites)

This screen shows a list of apps and websites that have used the user's Facebook account. It includes icons for each app, the app's name, and a 'Remove' button. A modal window is open in the foreground asking if the user wants to remove the "全民社造行動計畫" (Public Welfare Action Plan) app.

Screenshot 2: 臉部辨識 (Facial Recognition)

This screen displays a setting where the user can enable or disable facial recognition for photos and videos. A toggle switch is shown in the off position. A note at the bottom indicates that users can change settings here or in the general settings menu.

Modal Window (Foreground): 移除全民社造行動計畫 ?

This modal asks if the user wants to remove the "全民社造行動計畫" app from their Facebook account. It provides options to delete posts and notifications from the app, and checkboxes for both options are selected. Buttons for "取消" (Cancel) and "移除" (Remove) are at the bottom.

FACEBOOK 隱私設定

- 你的 Facebook 廣告偏好

你的 Facebook 廣告偏好

我們將為你說明各個選項，以確保

- 瞭解廣告
- 個人檔案資料
- 社交互動

舉例來說，假如你對某個正在刊登廣告的粉絲專頁按讚，你的朋友看見該廣告時，我們可能會讓他們知道你曾對該粉絲專頁按讚。以下為示意圖：

個人檔案資料

感情狀況

公司名稱

職稱

學歷

祕訣：這些設定只會影響個人檔案資料如會變更你個人檔案上的資料或該資料的分

誰可以在廣告旁看到你的社交互動？

你的朋友

返回 繼續

中華資安國際

125

聲控取代了一切的生活會是什麼模樣呢？

譯: 姆士捲

影片: REMA1000



中華資安國際
126

Q & A