中華資安國際
CHT Security

資安與生活

資訊安全教育訓練

講師：中華資安國際 林孟勳

日期：2025.12.24

中華資安國際
CHT Security

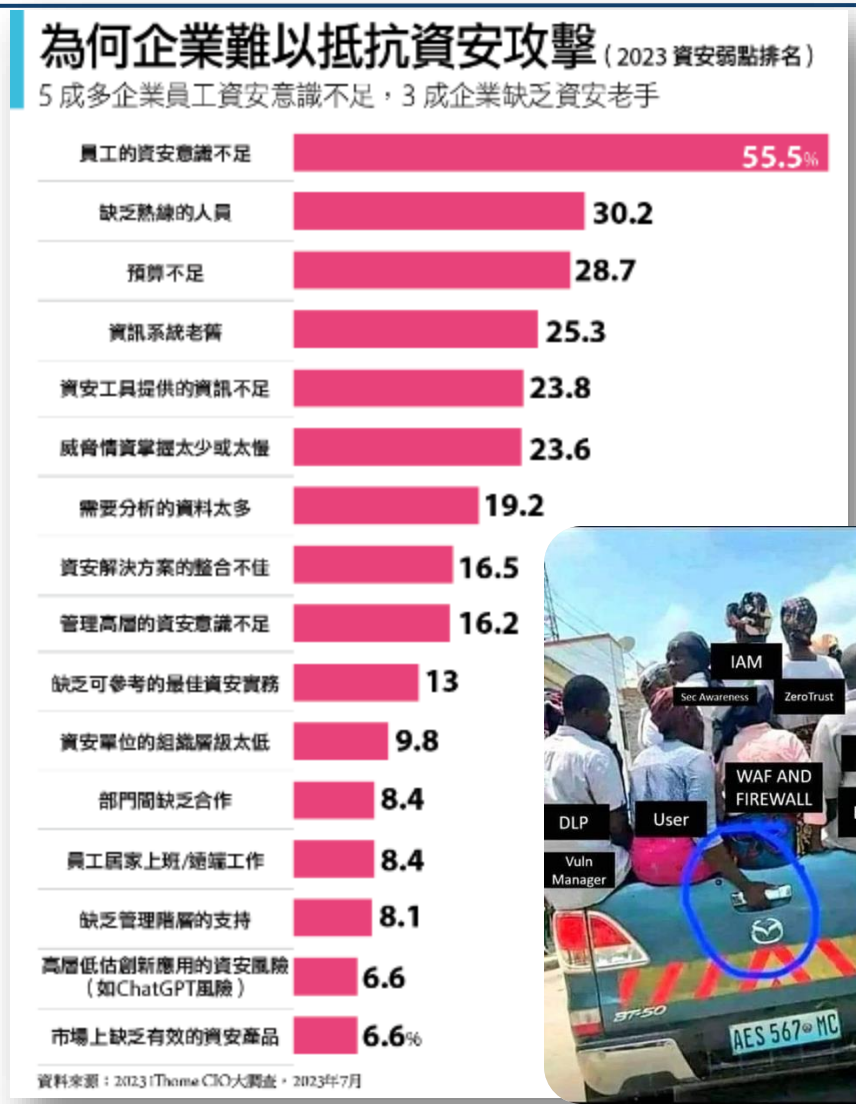
前言

你為什麼在這?

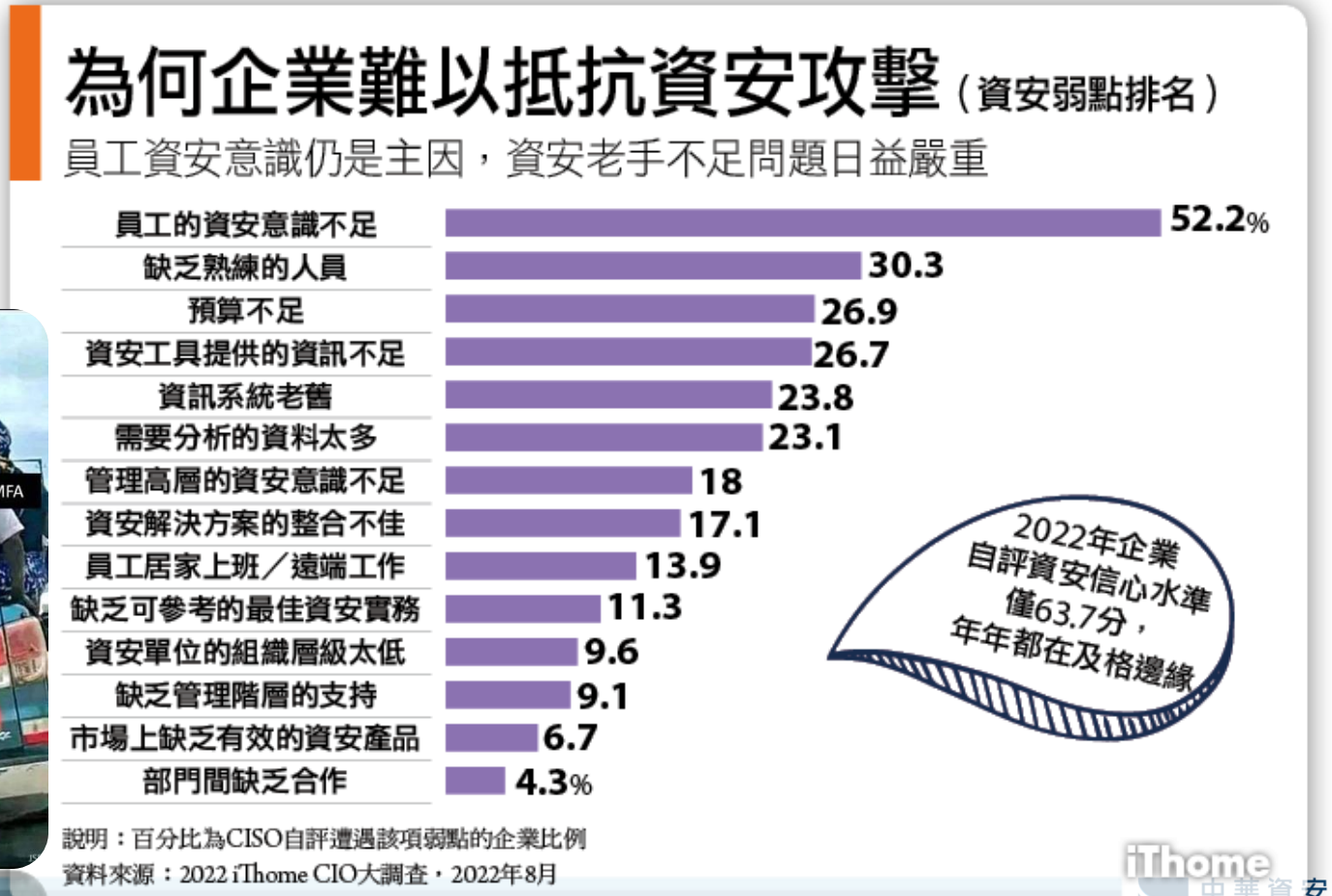
- 依「資通安全責任等級分級辦法」規定，一般使用者及主管，每人每年應接受3小時以上之一般資通安全教育訓練，

資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
	資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
	一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。

企業自評難抵禦資安威脅原因



- 根據iThome 調查，『員工資安意識不足』連續 5 年成為企業擋不住攻擊的主因

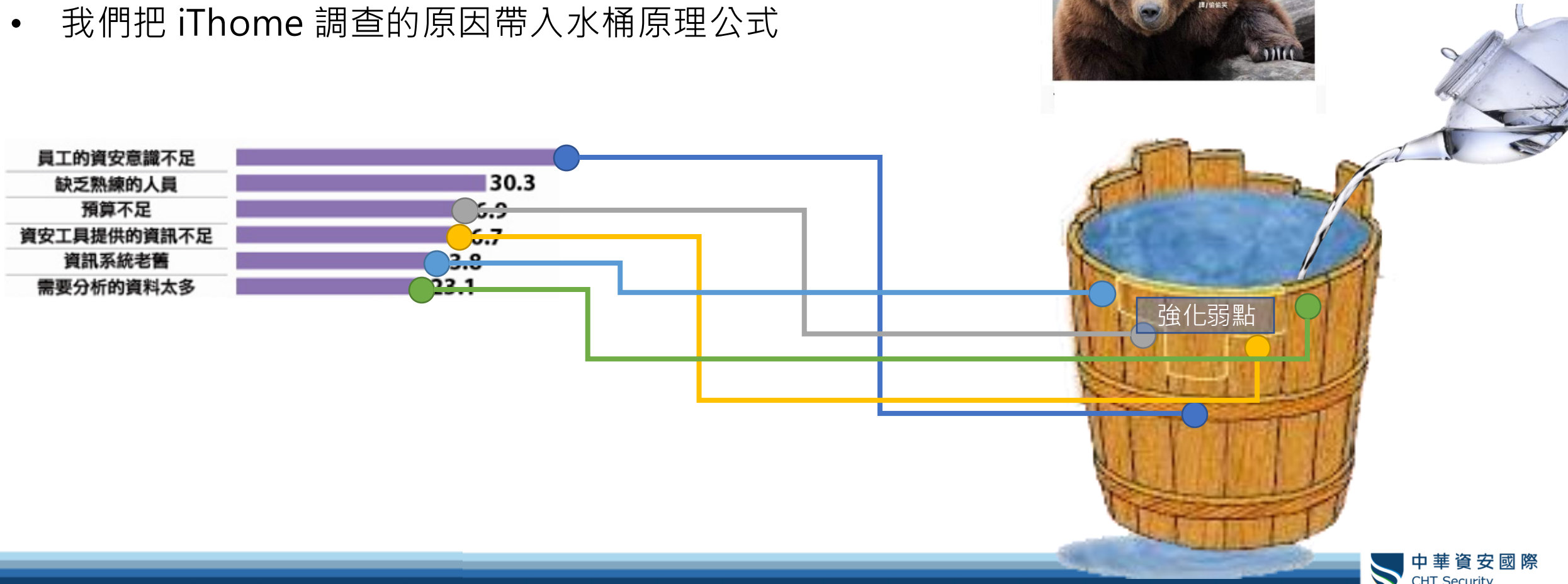


https://www.ithome.com.tw/article/156845

https://www.ithome.com.tw/article/153104

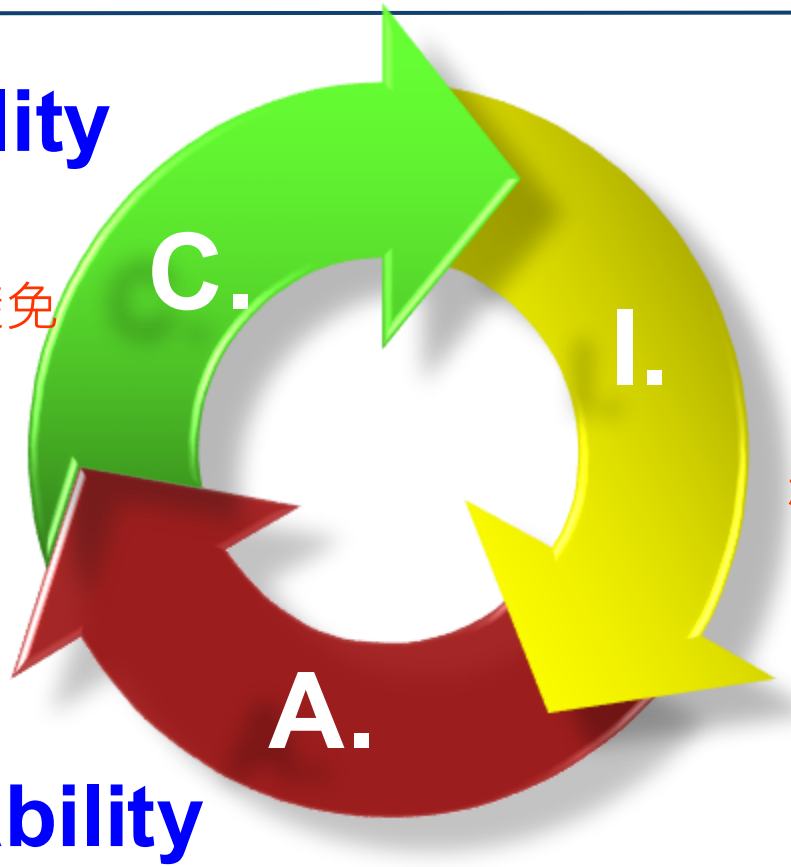
水桶原理

- 水桶原理：水位會往最低的木板邊(資安最弱的環節)流出
- 我們把 iThome 調查的原因帶入水桶原理公式



資訊安全三大要素

Confidentiality
(機密性)
確保資訊隱密性並避免遭到非法存取



Integrity
(完整性)
確保可提供正確與完整的資訊

Availability
(可用性)
確保可適時提供可用及正確之資訊

其他安全性要求:
- 不可否認性
- 身分鑑別
- 存取權限控制
- 可歸責性

資通安全法三讀通過(107.5.11)

- 做不好(第19-21條)
  - 公務機關→行政處份
  - 非公務機關未依規定通報資安事件，可處30萬元以上500萬元以下**罰鍰**，並得按次處罰
  - 非公務機關未訂定、未實施資通安全維護計畫，或未依規定訂定資通安全事件通報及應變機制等，得令其限期改正，屆期未改正者，按次處10萬元以上100萬元以下罰鍰。

- 做得好(第15條)
  - 公務機關所屬人員對於機關之資通安全維護績效優良者，**應予獎勵**

中華資安國際
CHT Security

資安新聞事件

資安新聞

Coupang資料外洩，波及3,370萬用戶

南韓最大電子商務網站酷澎（Coupang）傳出因內賊引發的資安事故，導致3千多萬名客戶的姓名以及通訊資料外洩

文/ 陳曉莉 | 2025-12-01 發表

讚 69 分享

- 目前僅限韓國地區帳戶
- 前（外籍）員工竊資
- 共同住戶大門密碼外洩

https://www.ithome.com.tw/news/172539

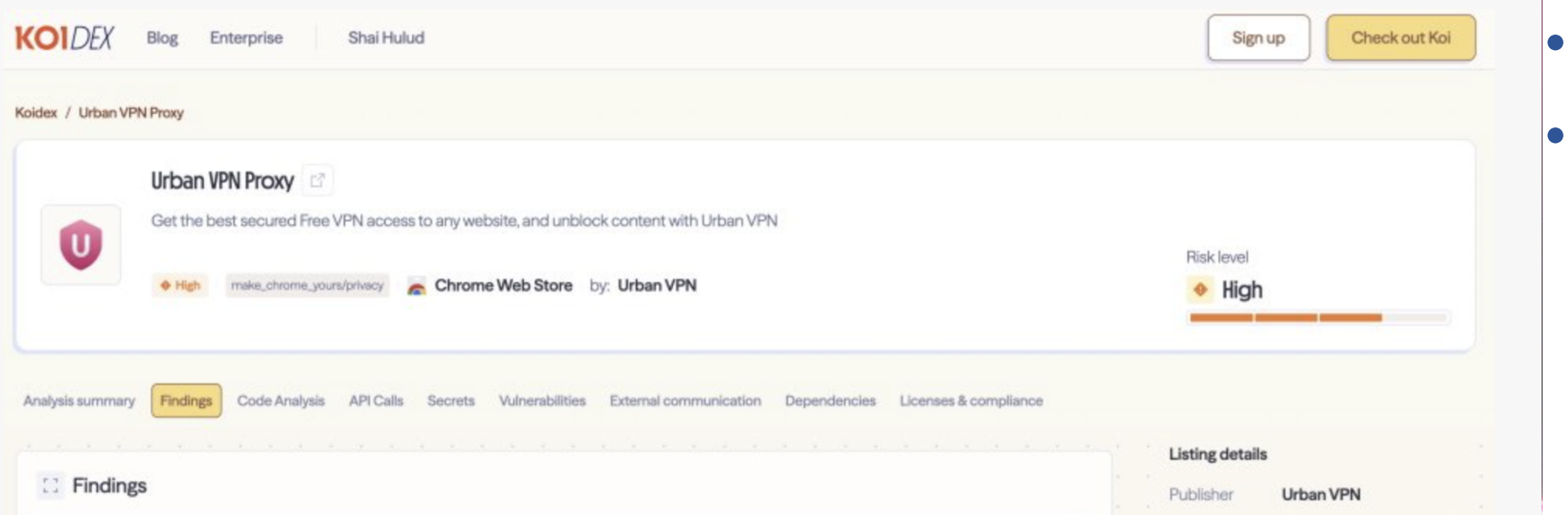
資安新聞

安裝數逾800萬的4款擴充程式，被揭攔截AI對話資料

以色列資安業者Koi Security發現Chrome及Microsoft Edge市集中，有4款擴充程式會監看、記錄並傳輸使用者與AI的對話，都是由同一家開發商所發布

文/ 陳曉莉 | 2025-12-22 發表

讚 13 分享



- Urban VPN Proxy
- 1ClickVPN Proxy
- Urban Browser Guard
- Urban Ad Blocker

https://www.ithome.com.tw/news/172964

資安新聞

- 烏克蘭YouTube主播如何被用AI「變身」俄羅斯人

奧爾加·洛伊克（Olga Loiek）看到自己的臉出現在中國社交媒體上的各種影片中，而這些影片由網上簡易的生成式人工智能（AI）工具製作。

「我可以看到我的臉，聽到我的聲音。但這一切都令人毛骨悚然，因為我看到自己說了一些我從未說過的話。」這位就讀於賓夕法尼亞大學（University of Pennsylvania）的21歲學生告訴BBC。

奧爾加發現大約有35個賬戶使用她的肖像。

https://www.bbc.com/zhongwen/trad/world-69014941

資安新聞

駭客利用深偽技術線上應徵工作得逞，資安業者KnowBe4傳出不慎僱用北韓駭客，察覺異狀並尋求FBI協助調查

北韓駭客尋求為他國企業工作，替政府賺取資金並從事間諜行動的情況，如今真實在一家資安業者上演！資安意識教育訓練業者KnowBe4公布他們經歷的內部威脅事故，並指出對方在取得相關職位後，就開始使用惡意軟體於公務電腦意圖從事不法行為

文/ 周峻佑 | 2024-07-25 發表

讚 47 分享

圖片來源: KnowBe4

兩年前美國政府發出警告，北韓政府派出具備IT開發能力的商業間諜，透過自由工作者招募平臺、社交網站、數位支付系統等管道，於全球市場求職，但這些人士不光只是為北韓政府賺錢，一旦企業僱用他們，就

駭客利用深偽技術線上應徵工作得逞，資安業者KnowBe4傳出不慎僱用北韓駭客，察覺異狀並尋求FBI協助調查 | iThome

資安新聞

英國電信業者開發「AI 阿嬤」 詐騙集團傻傻分不清被詐騙

2024-11-20 16:06 聯合新聞網／三嘻行動哇 Yipee!

https://youtu.be/RV_SdCfZ-0s?si=gVK_veJ2t5Hp2kWj

https://tech.udn.com/tech/story/123454/8372908

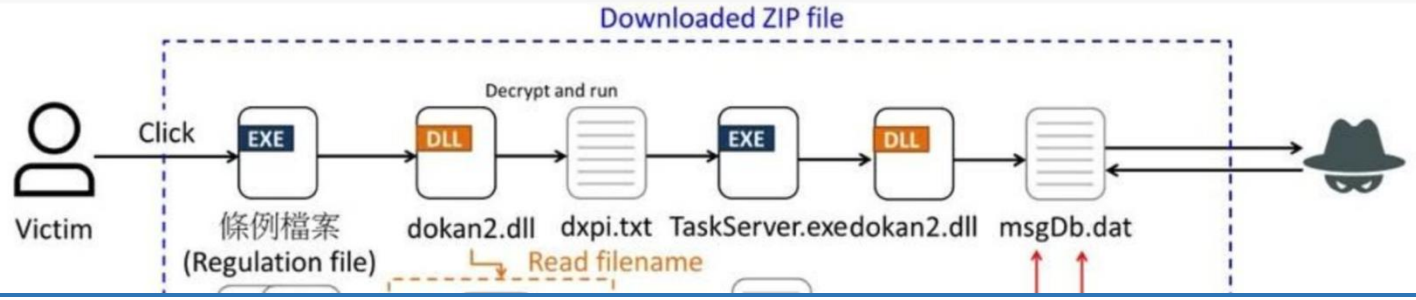
資安新聞

駭客假冒政府機關與商業夥伴，在臺灣散布惡意軟體HoldingHands RAT、Gh0stCringe

惡意軟體Winos 4.0以國稅局查稅為幌子在臺散布的攻擊事故仍在持續蔓延，資安業者Fortinet指出，他們自3月看到駭客使用更為複雜的手段從事相關活動，並開始散布新的惡意軟體HoldingHands RAT（Gh0stBins）、Gh0stCringe

文/ 周峻佑 | 2025-06-18 發表

讚 16 分享



- 冒充海關總署，以進出口稅務通知為由
- 冒充財政部的名義，佯稱營業稅電子申報繳稅程式發布新版並提供下載
- 佯裝其他政府部門或商業夥伴的情況，他們使用稅收、養老金、發票等名目為誘餌

然而不論上述的那一種釣魚信，收信人都會被導向特定的檔案下載網頁，要求下載受到密碼保護的ZIP壓縮檔，其內容包含合法的執行檔、DLL檔案、經加密處理的Shell Code，以及對應的惡意程式載入工具，一旦依照指示開啟特定檔案，電腦就可能被植入前述的惡意軟體。

https://www.ithome.com.tw/news/169600

資安新聞

- 2025/7/11 通過
- 2025/7/12 開始有詐騙簡訊

https://mofy-gov.net/tw

https://mofb-gov.net/tw

https://6000-mof-tw.net/tw

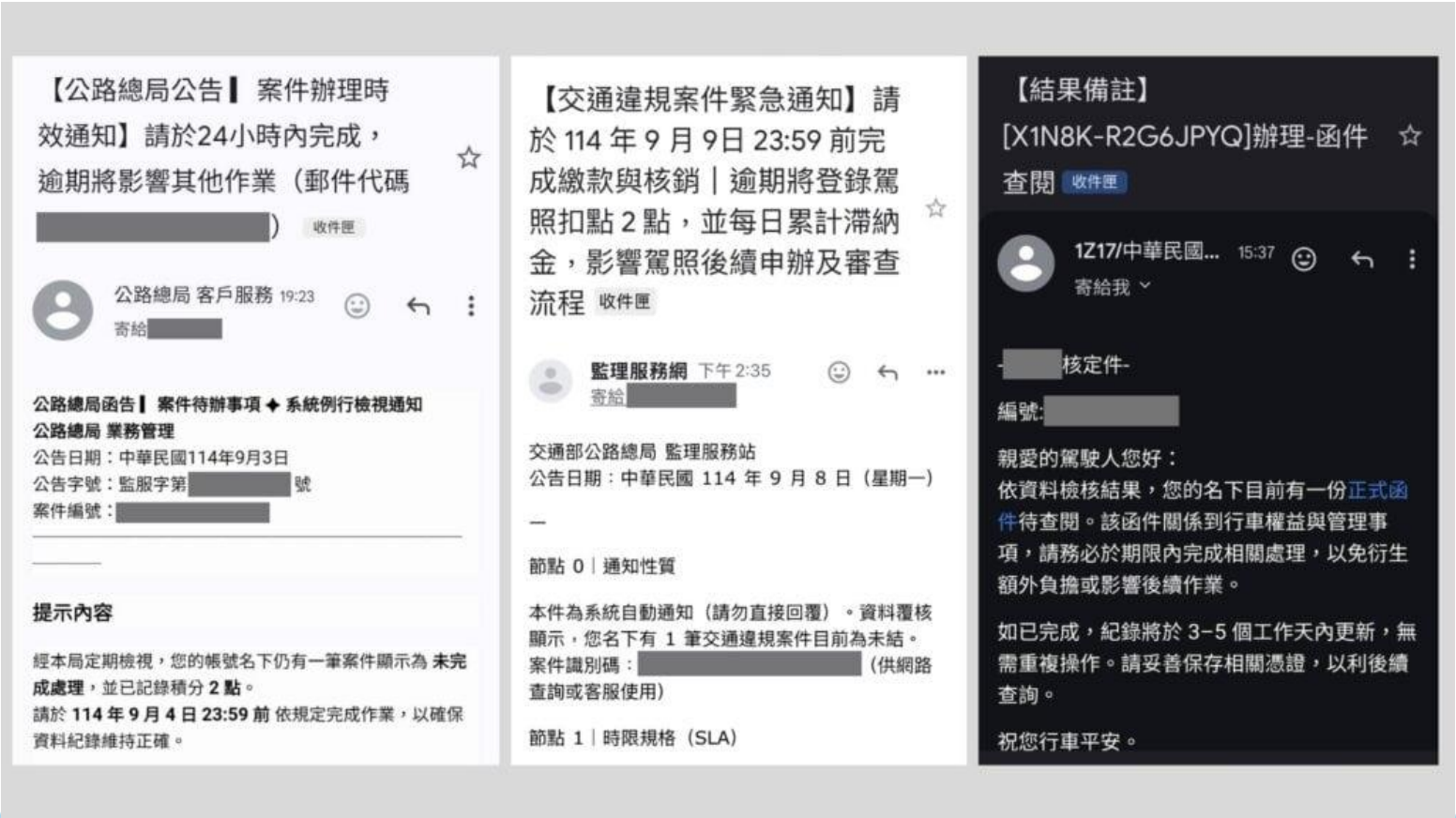
真網站：
https://10000.gov.tw/

https://www.cmoney.tw/forum/article/172406898 https://www.ftvnews.com.tw/news/detail/2025923W0298?utm_source=yahoo&utm_medium=InArticl

資安新聞

網傳「監理服務站透過電子郵件，要求限時登入連結繳納罰鍰」？

詐騙訊息，公路局已停止透過電子郵件通知交通違規或罰鍰



https://tfc-taiwan.org.tw/fact-check-reports/fake-traffic-violation-email-alert-thb/

資安新聞-實例

【最終催繳通知】交通違規罰鍰案件（案號：T8K9L3M-4N55-77842）逾期未結，請立即處理

已封鎖部分影像以保護您的隱私權。 下載影像

監 **監理服務管理處**
do_not_reply@on24event.com ···

收件者: 您 [redacted]

9月18日 星期四, 12:56

敬啟者：

經查，臺端有下列一筆交通違規罰鍰案件迄今尚未結案，相關資訊如下：
- 案件編號：T8K9L3M-4N55-77842
- 違規事由：累積違規點數2點
- 處理期限：114年9月15日（已逾期）
- 當前狀態：催繳程序中

根據《道路交通管理處罰條例》第六十五條規定，請於文到三日內完成下列處理事項：

[redacted]案，相關資訊如下：
- 案件編號：T8K9L3M-4N55-77842
- 違規事由：累積違規點數2點
- 處理期限：114年9月15日（已逾期）
- 當前狀態：催繳程序中

根據《道路交通管理處罰條例》第六十五條規定，請於文到三日內完成下列處理事項：
1. 至各區監理單位臨櫃繳納
2. 或利用監理服務網線上繳費系統辦理

逾期未辦理者，本局將依規定移送法務部行政執行署所屬分署強制執行，屆時將額外產生執行必要費用。

案件查詢與繳費連結： https://mvdis-gov-twyv.net/tw

如有任何疑問，請於辦公時間洽詢：
- 服務專線：(02) 2763-0153
- 服務時間：週一至週五 08:00-17:00

※ 此為系統自動發送訊息，請勿直接回覆本郵件 ※

交通部公路總局
中華民國一百一十四年九月十八日

https://mvdis-gov-twyv.net/tw

資安新聞-實例


監理服務網-首頁
交通違規(含強制險)查詢及繳納
一、交通違規紀錄不會即時更新，需待舉發機關入案後，才可於線上查詢到。
二、請注意，若使用本功能繳費完成，每筆違規皆會收取一筆手續費！
違規紀錄如下：
請注意：您一年半內 機車駕照共記 2 點
步驟一：查詢交通罰鍰
步驟二：查看欲繳納的罰鍰
步驟三：繳納費用
可線上繳納
下列罰單可做線上繳納：
違規日
事由
罰鍰
應到案日
114年08年06日
在禁止臨時停車處所停車
900
114年09年21日
線上繳費


一、交通違規紀錄不會即時更新，需待舉發機關入案後，才可於線上查詢到。
二、請注意，若使用本功能繳費完成，每筆違規皆會收取一筆手續費！
本站熱門網頁
選號及轉帳作業
交通違規查詢結果
汽燃費查詢及繳費
駕駛人及車輛資料
號牌標售
意見信箱暨申訴平
網站使用說明
步驟一：查詢交通罰鍰
步驟二：查看應繳納的罰鍰
步驟三：繳納費用
本次繳費清單：
違規日
事由
114年08月09日
在禁止臨時停車處所停車
信用卡繳費
持卡人名字
kkk lin
信用卡卡號
4444 5555 6666 7777
此字段有誤，请检查
有效日期
11/29
安全碼CVV
225
確定金融帳號資訊
信用卡繳費
持卡人名字
信用卡卡號
0000 0000 0000 0000
有效日期
MM/YY
安全碼CVV
123
確定金融帳號資訊
交通罰鍰查詢及繳納注意事項

資安新聞

冒牌電腦版Line針對臺灣而來，恐導致電腦被植入木馬

趨勢科技提出警告，他們發現疑似針對臺灣使用者的網釣攻擊行動，駭客佯稱提供即時通訊軟體Line的電腦版本，一旦使用者安裝，電腦就有可能被植入木馬程式

文/ 周峻佑 | 2025-04-16 發表

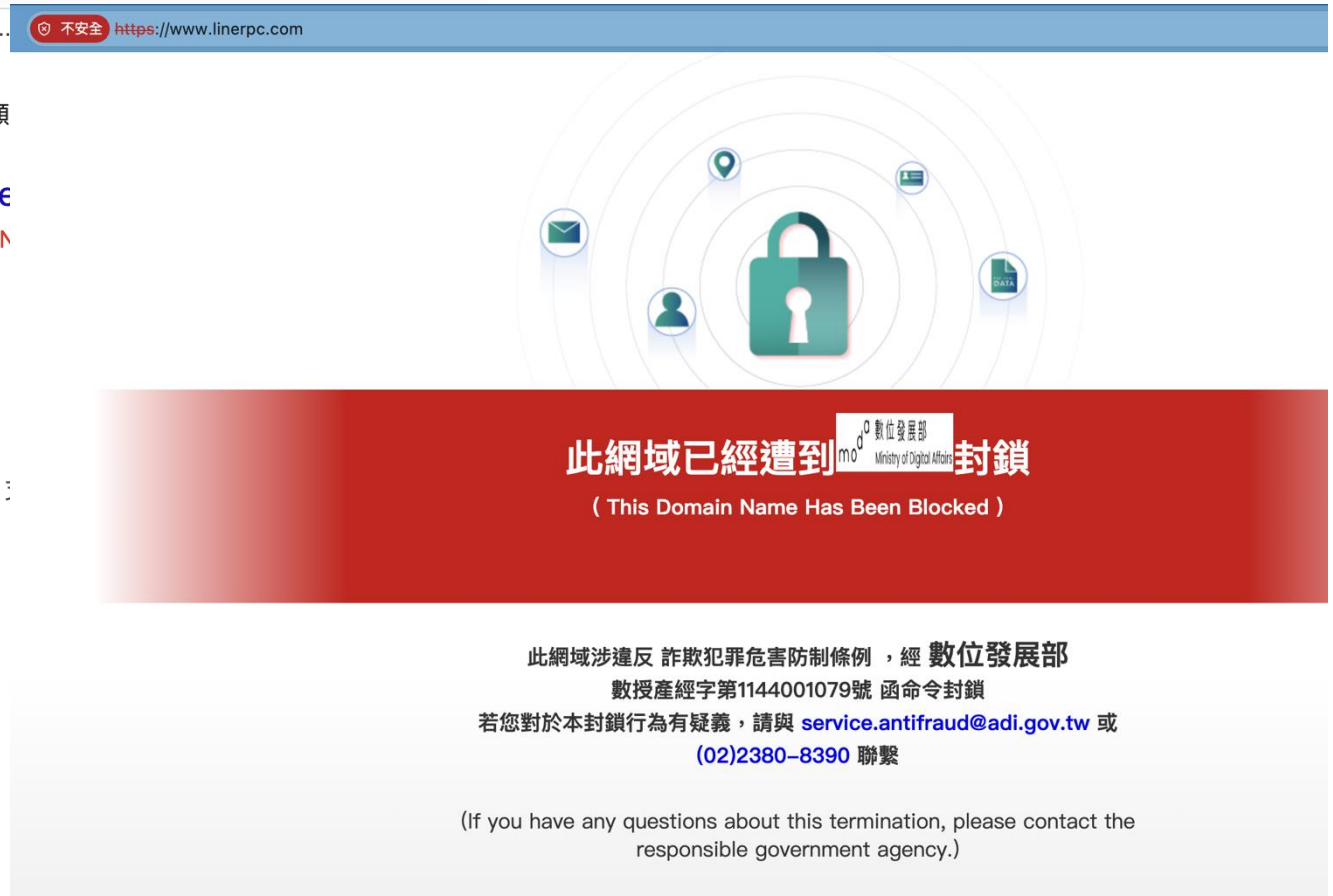
讚 17　分享

- 研究人員公布他們看到的假網站網域名稱，包括：
- www[.]linec-tw[.]OOO
- line-chinese[.]OOO
- line-tw[.]OOO
- windows-line[.]OOO

https://www.ithome.com.tw/news/168431

資安新聞(續)


https://www.google.com/search?q=line+電腦版+下載&sca_esv=0b6cd31ca70c40ac&sxsrf=AE3TifMVa2LFIXB_rkLrIDFt3LpnW6x5-
Google
line 電腦版 下載
for Desktop」的下載連結。選擇Mac 版本，並點擊下載按鈕。安裝檔將會下載到 ..
Facebook · UNIKO x AMD x PC 粉絲萬事屋 | 電腦零組件組裝、改裝、超頻
超過 10 則留言 · 4 個月前
請大家告訴大家，正版的LINE 電腦版下載網址是www.line
請大家注意！搜尋引擎出現多個假的LINE 下載頁面，排名還相當前面。 要下載LIN
址line. me，才不會裝到奇怪的東西。
linerpc.com
https://www.linerpc.com
LINE電腦版- LINE 下載
LINE電腦版. LINE 結合即時訊息、貼圖互動與多媒體傳輸，提供完整的通訊體驗.
同步，讓使用者隨時隨地保持溝通順暢. 发现新鲜事 ...


不安全 https://www.linerpc.com
此網域已經遭到 數位發展部 封鎖
(This Domain Name Has Been Blocked)
此網域涉違反 詐欺犯罪危害防制條例 ，經 數位發展部
數授產經字第1144001079號 函命令封鎖
若您對於本封鎖行為有疑義，請與 service.antifraud@adi.gov.tw 或
(02)2380-8390 聯繫
(If you have any questions about this termination, please contact the
responsible government agency.)

資安新聞(續)

- https://phishingcheck.tw/

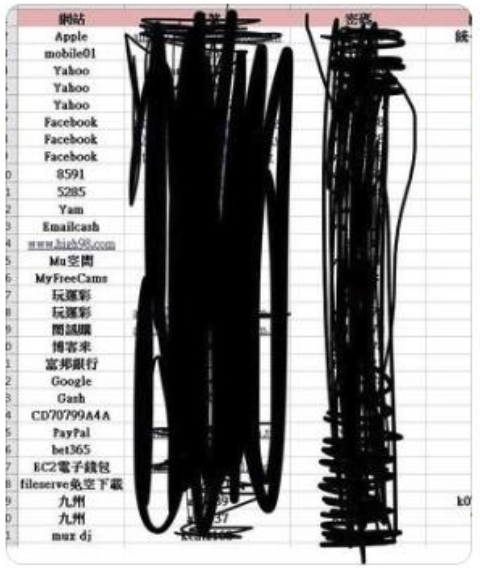
資安新聞事件

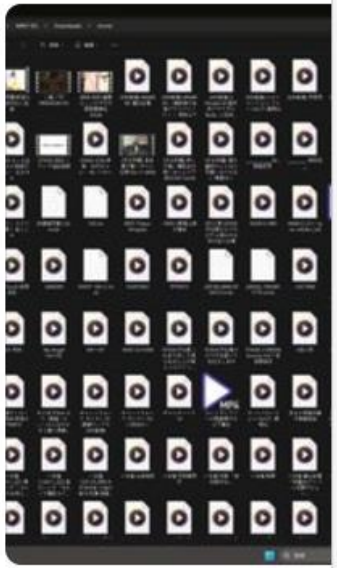
https://www.threads.net/@zawahiro0116/post/DBrjj25TeHC

串文

zawahiro0116 2024-10-29

剛剛去倒垃圾時發現有台報廢電腦被丟在電器回收區
於是我就發揮diy垃圾佬精神把能用的零件幹回去（硬碟、cpu、ram條之類）
結果檢查硬碟健康度時發現裡面有一大堆資料
包括但不限於：
珍藏的謎片（大概512gb）
帳號密碼（從銀行到fb都有）
跟家人朋友的親民合照
這個故事告訴我們在報廢任何有個資的設備時記得一定！一定！一定！要把硬碟物理銷毀！！！！
不然那天銀行帳戶被盜用、珍藏的d槽被看光都有可能
（已經把硬碟徹底格式化了）





資安新聞

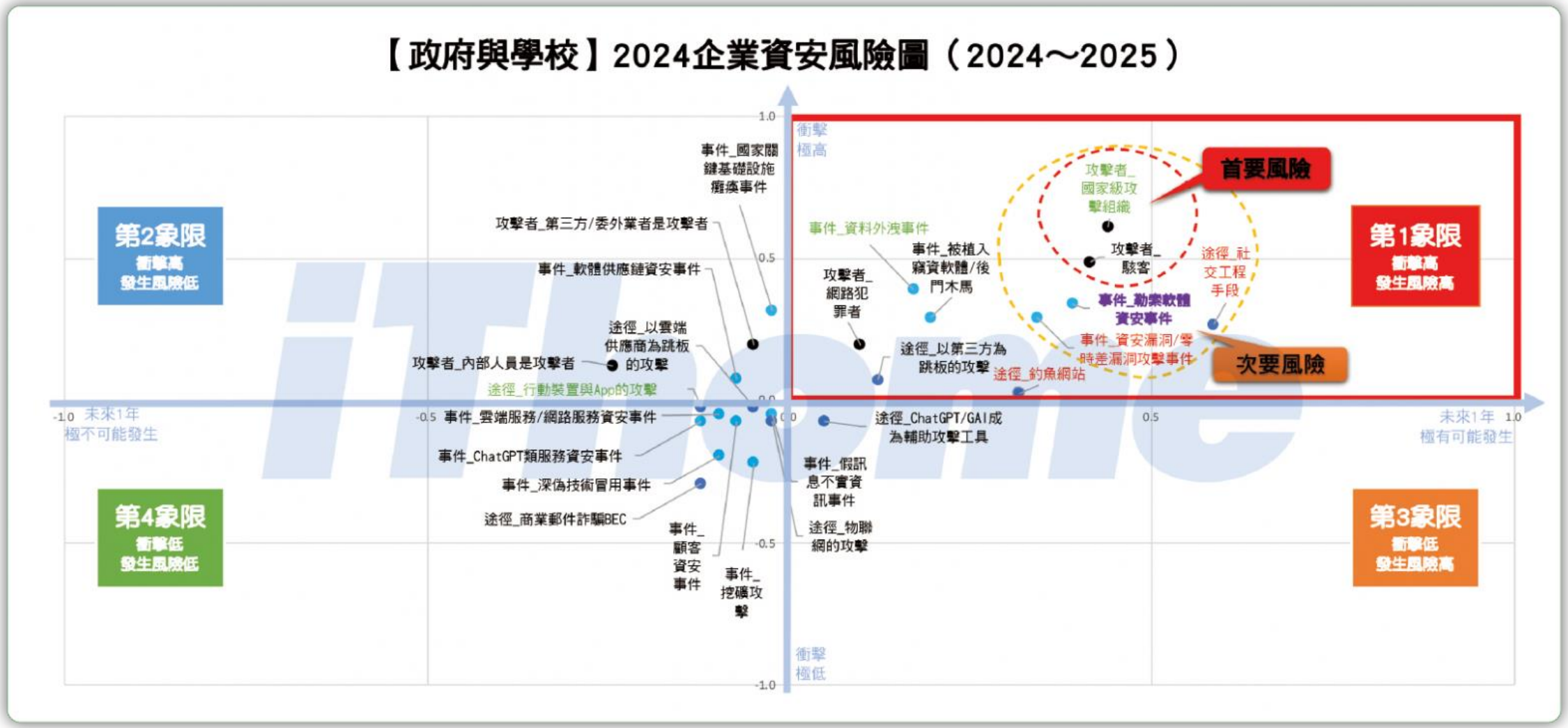
英國14歲少女自殺 法院判社群平台「殺人」

英國14歲少女羅素在2017年自殺，其生前瀏覽過許多帶有負面訊

- 法院認證少女的自殺與社群平台的貼文有「直接關係」
- 自殘，死前罹患憂鬱症，並在網路上看了大量有負面作用的內容
- 因為演算法的關係，推送並未主動查詢的內容
- Meta與Pinterest

https://news.ltn.com.tw/news/world/breakingnews/4076306 https://www.youtube.com/watch?v=WRaMGRs3EBA

2024企業資安風險圖-政府與學校



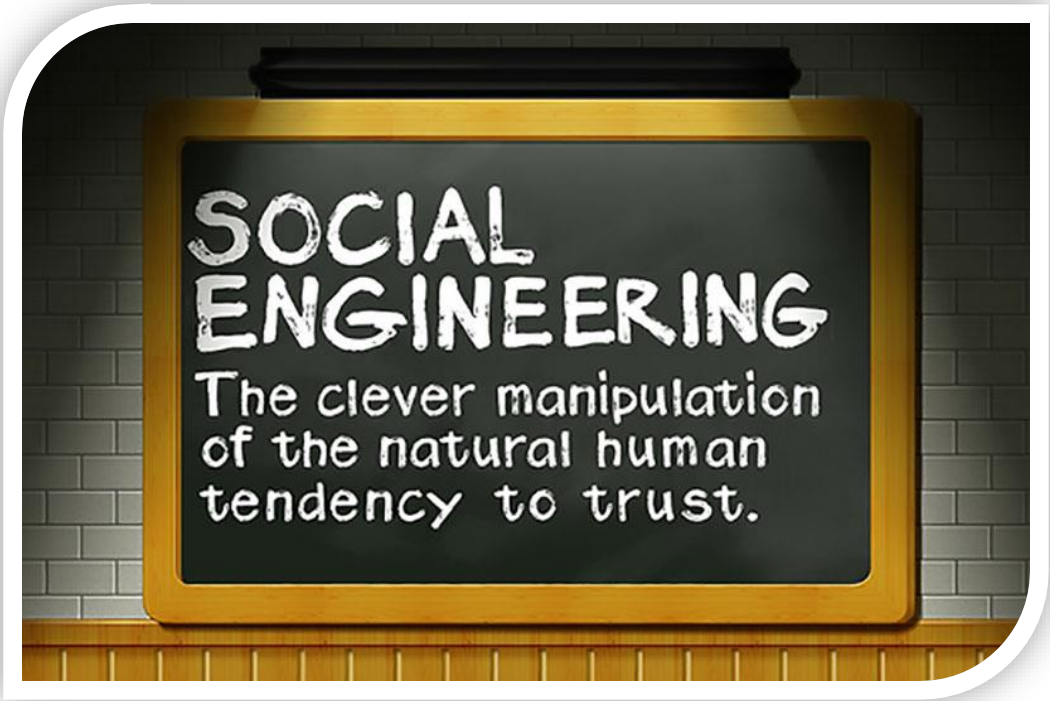
https://www.ithome.com.tw/article/162263

中華資安國際
CHT Security

社交工程

什麼是社交工程

- 利用人性弱點、人際交往或互動特性所發展出來的一種的詐騙技術。



網路釣魚(Phishing)

非完全技術的攻擊手法，資安設備也無法完全阻擋

- Phone + Fishing = Phishing
  - 工具:電子郵件+釣魚網站

- 利用**欺騙性**的電子郵件，**偽裝**商務網站或是登入網站，**誘騙**輸入帳號、密碼、信用卡號等個人敏感資料的詐騙活動

- 透過電子郵件進行目標式攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括0day攻擊)

網紅的一天

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

藝人的IG 帳號連本人都要不回來

假冒寄件者

利用電子郵件

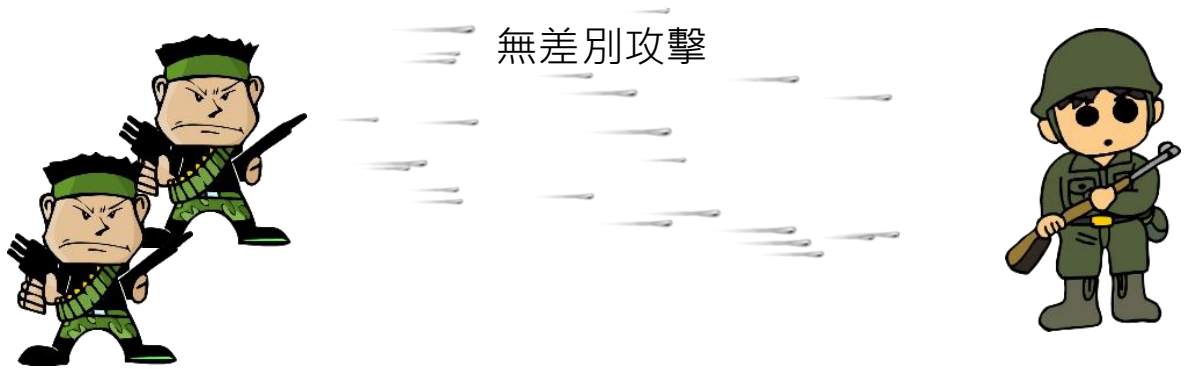
感興趣的內容

造成損失

攻擊手法介紹：APT

- 進階持續性滲透攻擊 (Advanced Persistent Threat, APT)

一般駭客　　目標　　APT



個人或駭客結盟

亂槍打鳥，速戰速決

針對性

組織性

長期、持續性、多樣化

經常是零時差漏洞的攻擊，確保達成攻擊目標

漏洞生命週期

駭客發現了漏洞不一定要通報廠商

駭客製作出攻擊程式，打遍天下無敵手

空窗期(1) → 空窗期(2) → 修補期 → 安全期

發現軟體弱點 | 公佈軟體弱點 | 發佈修補程式 | 系統更新完成

0-day 漏洞

n-day 漏洞

Zoom攻擊程式在黑市叫價50萬美元

雲端視訊會議Zoom的爆紅，讓全球駭客都在找它的安全漏洞，根據報導，黑市出現鎖定Zoom零時差漏洞的攻擊程式，Windows版更標榜開採了尚未曝光的零時差漏洞，喊價到50萬美元

文/ 陳曉莉 | 2020-04-16 發表

因微軟大幅降低回報獎金，研究人員直接公開最新Windows 系統權限漏洞

by ClaireC — 2021 年 11 月 26 日 In 最新科技新聞

零時差 (0-day) 案例

6月初開始，只要用**IE**上雅虎奇摩網頁：tw.yahoo.com 而**Flash元件沒更新**的話，光瀏覽tw.yahoo.com的首頁

遇到某聯播廣告觸發Flash漏洞，就會觸發**neutrino-exploit-kit**，而讓**Crypz勒索病毒**找上你！

參考來源文章

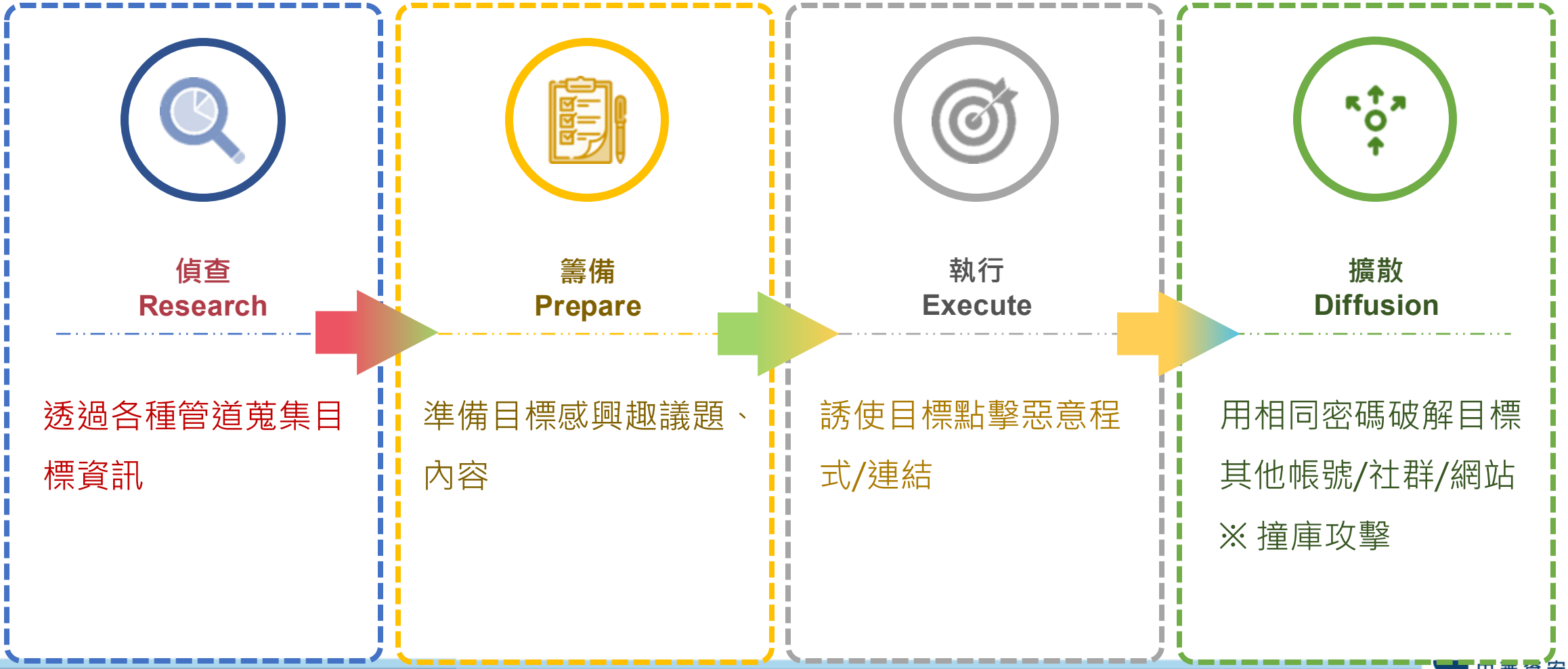
https://blog.malwarebytes.com/cybercrime/2016/06/neutrino-exploit-kit-fills-in-for-angler-ek-in-recent-malvertising-campaigns/

現象描述:

1. 6/3 開始，陸續發現有大量的勒索病毒案例發生，調查結果，這些使用者沒有收到可疑郵件，所以沒有開啟有毒的附件。
   但這些使用者都有訪問tw.yahoo.com首頁後發作。但不是每個有訪問該網站都會發作。
2. 調查結果屬於Malvertizing活動，即一種有毒廣告輪播的攻擊活動。駭客集團找到漏洞後，購買合法廣告，透過neutrino-exploit-kit攻擊套件植入惡意程式。
3. Yahoo在6/8至6/9間，收到通報，並且將相關的惡意廣告下架。
4. 如果使用Win7(含以上)的使用者，該漏洞由於會竄改啟動程序，因此會跳出UAC確認，不理它沒事，不小心按了確認後，就開始加密勒索的過程...

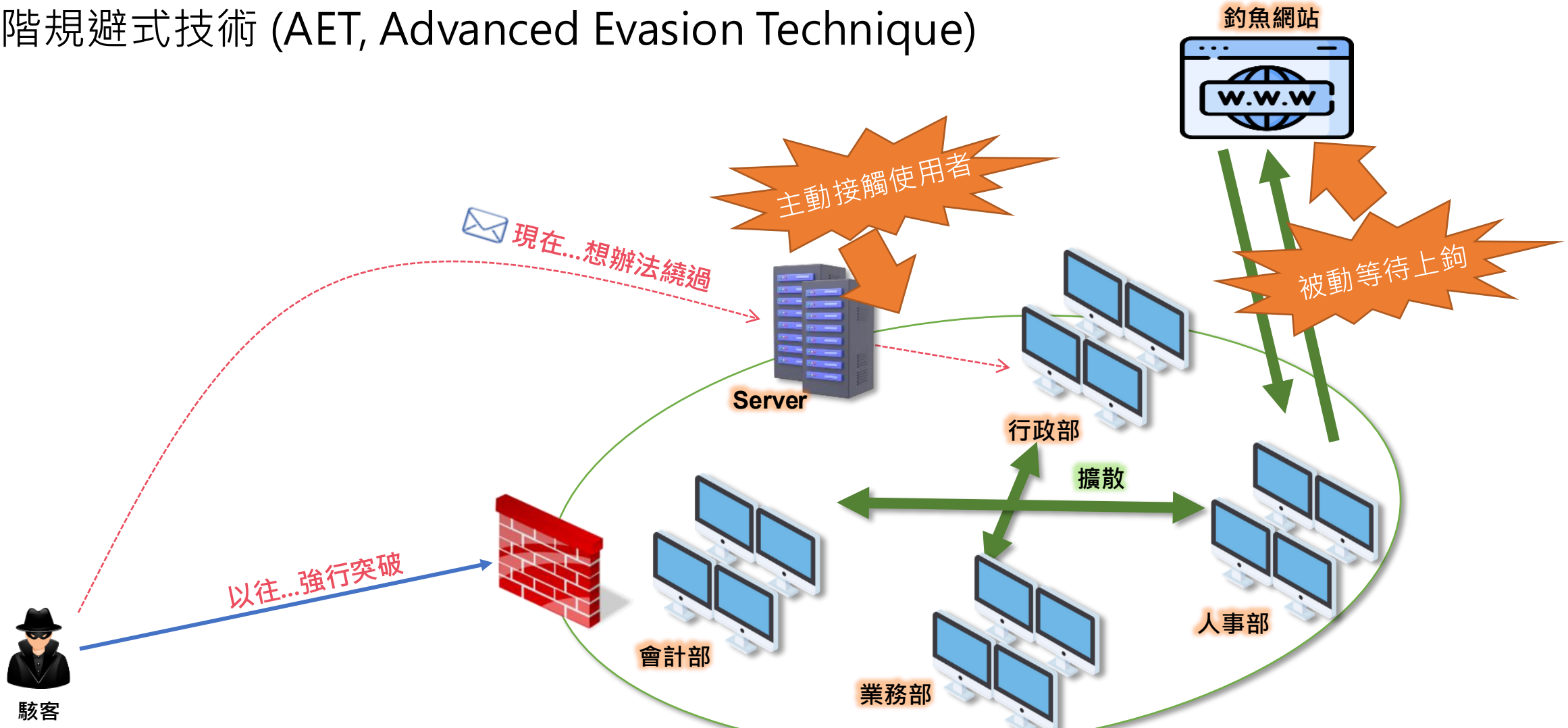
影片的啟發

- 影片中的社交攻擊流程



攻擊手法介紹：AET (1/2)

- 進階規避式技術 (AET, Advanced Evasion Technique)



攻擊手法介紹：AET (2/2)

- 進階規避式技術 (AET, Advanced Evasion Technique)

Call Home:

https://www.microsoft.com/abc.exe

https://2016.com/public/infected.exe

https://xxxxxxxx.com/aaa.bat

dropbox

onedrive

google cloud

AET 攻擊手法範例：把檔案加密

- 目的：規避資安設備/人工檢查
- 加密後，資安設備不知道密碼
- 但是駭客會將密碼透過各種管道讓使用者知道

寄件者: [redacted]　　寄件日期: 2011/6/24 (週五) 上午 04:30
收件者: [redacted]
副本:
主旨: 免費楓之谷洗錢機

副檔密碼是 123 喔

還在當乞丐和人要錢嗎?不用要了 快來下載吧!楓之谷洗錢機用過的人都說讚喔

別當小偷小白

記得回 3Q

載點:下載請按我 載點在副檔

安裝說明都有寫

AET 攻擊手法範例：短網址

短網址還原網站

短網址：

↓
https://goo.gl/FahH3J
↓
https://www.dropbox.com/s/qfyc2t8hnurzllk/%E5%9B%9E%E5%9F%B7%E5%96%AE.apk

AET 攻擊手法範例：短網址案例

AET 攻擊手法範例：短網址

- 善用滑鼠停留功能

範例一：網址	範例二：說明	範例三：圖片	範例四：檔案
tw.yahoo.com	點我抽獎		

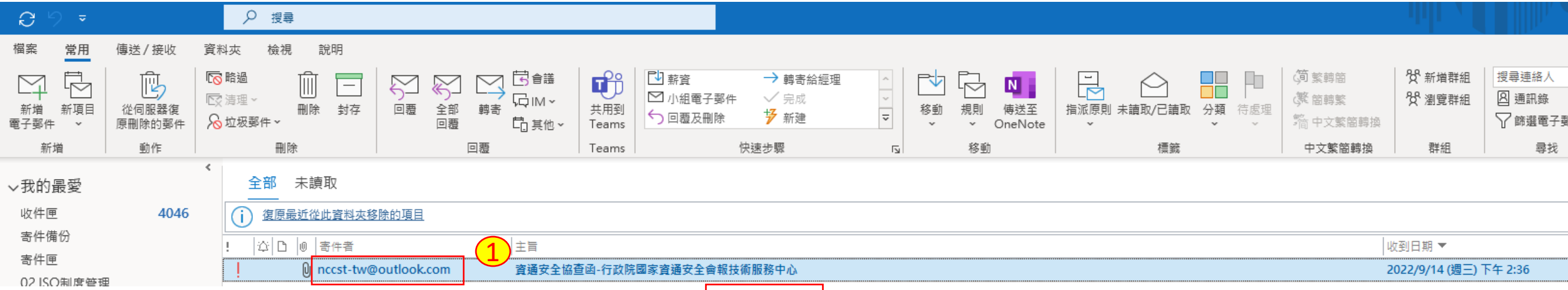
遇到網址務必多停留一秒確認

注意可疑電子郵件的特徵

- 過於聳動的主旨與緊急要求
- 觀察為不正常的發信時間
- 收到陌生人或少往來對象來信
- 認識的人來信但主旨或內容與其習性不符
- 要求輸入私密資料送出
- 附件有加密但內文直接提供密碼

真實案例：APT郵件攻擊

行政院技術服務中心發來的Email?!



信件內容

Subject: 資通安全協查函-行政院國家資通安全會報技術服務中心

資通安全協查函

2 各收信單位：

進期，行政院國家資通安全會報技術服務中心、國家電腦網絡危機處理暨協調中心，偵測到台北固網鏈路節點、台中固網鏈路節點存在可疑網絡流量，經專家團隊研判，初步判定為境外惡意網絡攻擊。3

現依據我國資通安全管理法[A0030297]（詳見第三章“特定非公務機關資通安全管理”），資通安全事件通報及應變辦法[A0030305]（詳見第三章“特定非公務機關資通安全事件之通報及應變”）相關條文，對涉事相關單位開展緊急資通安全管

為確保此次資安審查真實性，本次審查采用不提前知會，不發佈公告隨機抽樣的審查方式進行。收到此封郵件，代表你需按要求參加此次資通安全審查。請下載郵件所附資通安全審查工具和說明流程，在9月15日之前，完成此次資通安全審查。

依照國家資通安全管理法，未按要求完成此次資通安全審查，并因此造成三級及以上資通安全事件的（依據111年8月23日發佈的資通安全事件通報及應變辦法定級），將按照國家資通安全管理法依法追究相關人員之法律責任。

國家資通安全管理法(https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297) 4

資通安全事件通報及應變辦法(https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030305) 5

行政院國家資通安全會報技術服務中心

National Center for Cyber Security Technology

附注：壓縮檔案之解壓密碼統一爲nccst@2022 6

附件：附件1-NCCST資通安全審查[1110912].zip

對於電子郵件應有的警覺性

- 「為何我會收到這封郵件」
  ✓應確認寄件來源及寄件者。
- 「我是否應該收到這封郵件」
  ✓應確認郵件主旨及郵件內容。
- 「我是否應該開啟這封郵件」
  ✓是否與業務工作相關。
  ✓不開啟(點選)連結是否有影響。
  ✓審慎查證（寄件者或資訊中心）。

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)

報電話集點的危險

- 報會員電話被找到FB

那身分證呢?

他去超商結帳報電話累積點數 回家收到陌生男「恐怖訊息」

2020-12-14 11:53 聯合新聞網 / 綜合報導

+ 超商

https://udn.com/news/story/120911/5090794

手機APP-會員卡功能


會員卡
新增會員卡
屈臣氏
全家
HappyGO
寶雅
跟著商業獅，逛街吃飯都有優惠
加入即領全台10大夜市優惠券！
已加入的會員卡
VIP
尚未新增會員卡
可以將你常購買的會員卡(如加油、購物...等)消費的店家通通存進來唷～
選擇會員卡
其他會員卡
全家
中油
OK便利商店
美廉社
家樂福
新光三越
寶雅


LINE Pay『我的會員卡』新上線，會員/載具/付款全面整合！
LINE Pay 使用教學
發布時間：2020年12月30日18:09
119
LINE Pay
7-ELEVEN 搶先體驗！
「我的會員卡」新上線
掃一次就OK
會員、載具、付款全面整合！


ゆうう
@youki1mahler9va
第一次搭乘新幹線的綠色車廂，我發現車內坐滿了SP(保全警察)，讓我覺得可能有重要人物在附近。結果一看共享的網路名稱，我就知道是誰了。
到京都後，我從後排座位看到總理下車時，再次確認沒錯。然而，考慮到有時需要隱密行動，我認為改一下手機共享網路名稱可能是增加隱密性的好方法。
Wi-Fi
インターネット共有
5G
總理秘書官付のiPhone
總理秘書的iPhone
iPhone (142)
上午11:54 · 2023年10月9日 · 1,430.3萬 次查看
646
1.7萬
7.7萬
3,025

電影賞析-原本以為只是手機掉了

https://www.youtube.com/watch?v=kbnr3JzU0Pk

https://www.youtube.com/watch?v=U5KkTCYR-Is

個資與隱私安全

個資法小複習

個資法第2條第1款明確定義了個人資料，主要包括但不限於以下幾種：

- **基本資訊**：：姓名、出生年月日、國民身分證統一編號、護照號碼等。
- **特徵與身體資訊**：：特徵、指紋、病歷、醫療、基因、健康檢查等。
- **生活與身分資訊**：：婚姻、家庭、教育、職業、社會活動等。
- **聯繫與財務資訊**：：聯絡方式、財務情況。
- **其他敏感資訊**：：性生活、犯罪前科等。
- **其他足以識別個人之資料**：：任何能與其他資料組合、比對後直接或間接識別出特定個人的資訊，也屬於個人資料的範疇。

判斷標準

判斷某項資訊是否屬於個人資料，關鍵在於該資訊是否能直接或間接識別出特定的個人。即使是匿名化或去識別化的資料，若有方法能還原而間接識別出個人，仍可能被視為個人資料。

https://www.pdpc.gov.tw/News_Html/100/

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/ 林妍溱 | 2019-05-06 發表

讚 6.1 萬 按讚加入iThome粉絲團 讚 549 分享

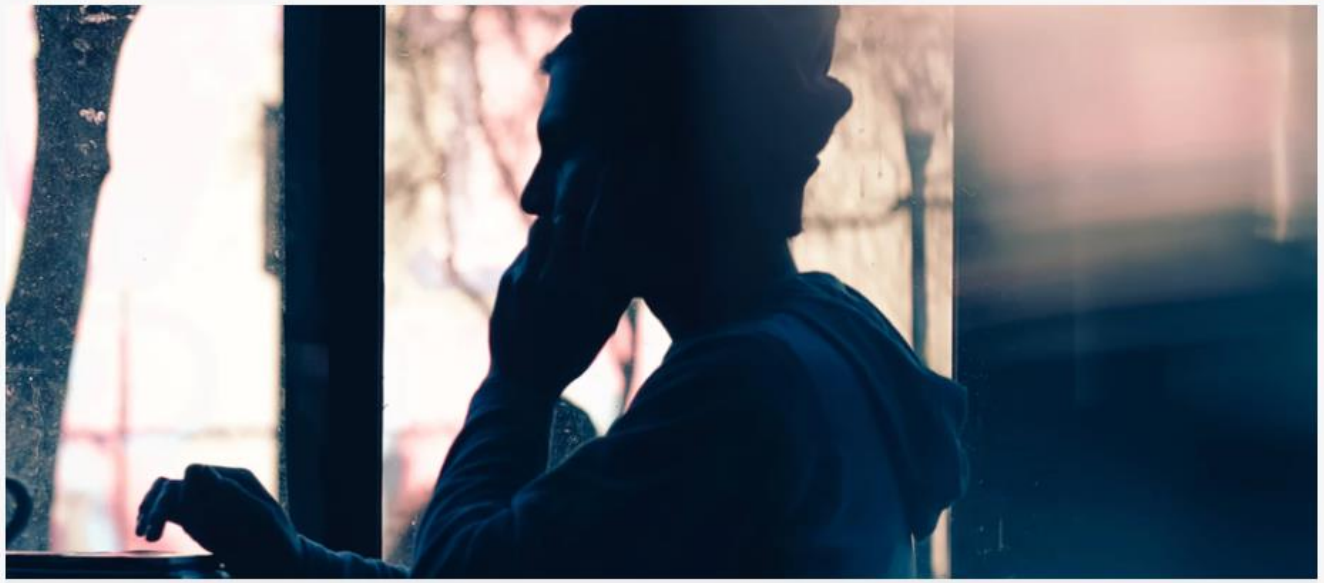


Photo by Hannah Wei on Unsplash

熱門新聞

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

資料來源：iThome https://www.ithome.com.tw/news/130416

台北卡蒐集個資

台北卡蒐集個資包山包海　沒填收入、配偶、信用評等不能申辦

更新時間： 2020/05/30 13:24

資訊局稱個資項目僅預列
局處依實際業務需要使用

台北卡升級台北通，北市府竟要求民眾同意蒐集收入配偶名等個資，議員苗博雅批便宜行事。翻攝台北卡APP

資料來源：
https://tw.appledaily.com/life/20200530/RSSCL7XWRPBLSMPPX4MHNQ7HAM/

103年起至今已陸續整合

1. 數位學生證
2. 敬老服務
3. 二代健康服務
4. 愛心服務
5. 愛心陪伴服務
6. 兒童優惠服務
7. 圖書借閱證
8. 原民服務等8項卡證服務

後續將陸續整合

1. 教育生活卡
2. 低收入戶卡、中低收入戶卡
3. 身障證明卡
4. 兒童醫療補助證
5. 志願服務榮譽卡
6. 第三胎證明卡
7. 小巨蛋冰宮會員卡、小巨蛋冰宮學習卡
8. 北投會館
9. 大稻埕戲
10. 城市舞台
11. 文山劇場
12. 職安卡等

蒐集個人資料之類別：

1. 識別類：C001辨識個人者(例如：姓名、相片、通訊及戶籍地址、行動電話、通訊及戶籍電話、電子郵件地址、網路平臺申請之帳號、提供網路身分認證或申辦服務之紀錄及其他任何可辨識資料本人者等)、C003政府資料中之辨識者(例如：本人與配偶之身分證字號、IC晶片卡卡號、居留證號、統一證號、護照證號、出入境許可證、家庭戶號)。
2. 特徵類：C011個人描述(例如：性別、生日)。
3. 家庭情形：C021家庭情形(例如：新移民之配偶姓名、戶長姓名)。
4. 社會情況：C038職業(例如：職業)。
5. 財務細節：C083信用評等(例如：收入狀況與等級)。
6. 教育、考選、技術或其他專業：C052資格或技術(例如：學歷)。
7. 健康與其他：C111健康紀錄(例如：身心障礙種類)、C113種族或血統來源(例如：原住民身分)。

中華資安國際
CHT Security

社群軟體安全設定

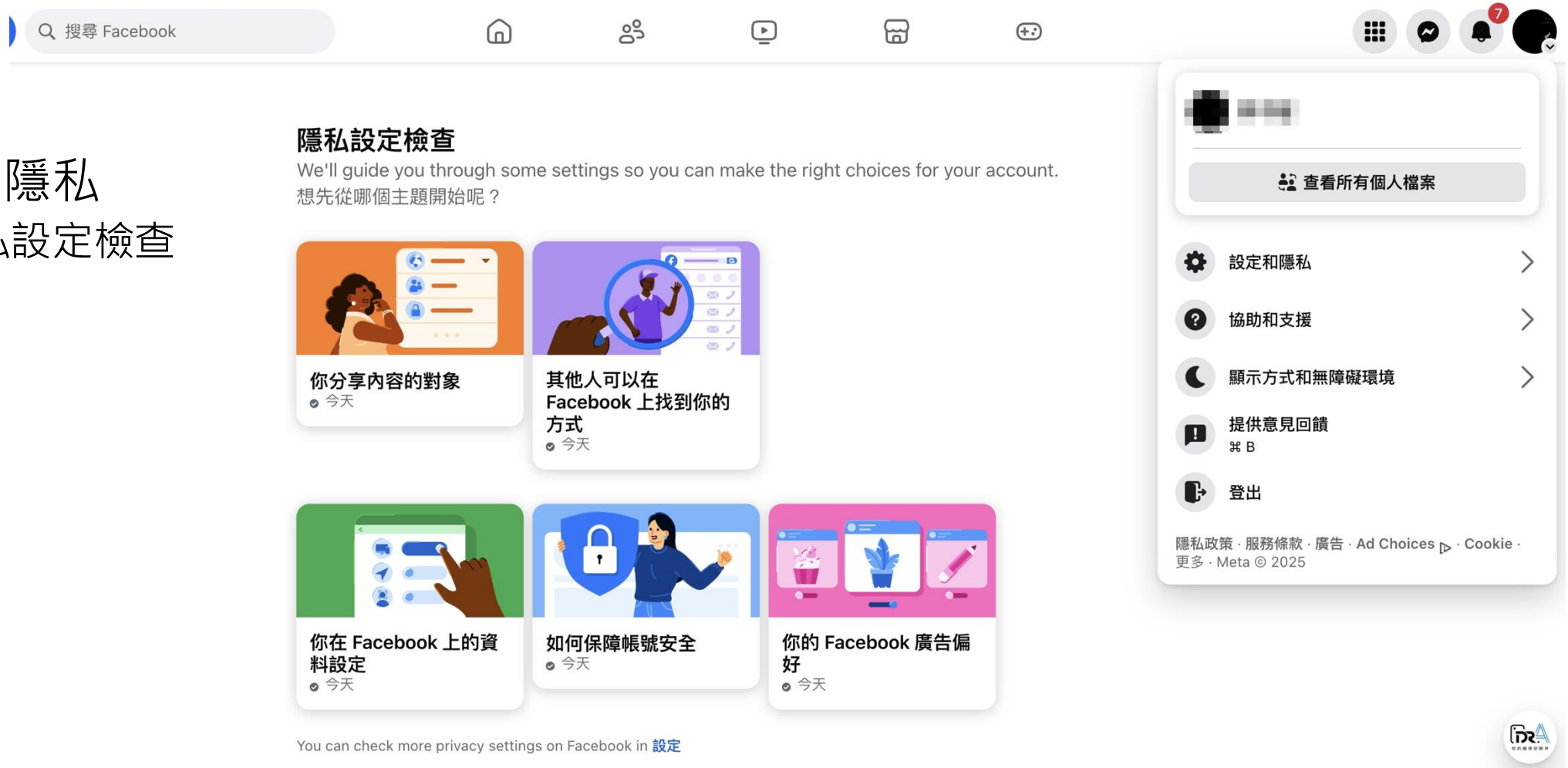
Facebook(FB, 臉書)

- 曝露太多個人資料、隱私
  - 親友同事、學經歷、生日、興趣、聯絡資料、活動記錄、消費習慣、政治傾向、宗教信仰...
- 已成為社交工程攻擊之工具
  - 假冒好友，傳遞惡意連結或影像、借錢
  - 假冒俊男美女誘加好友，騙取個資及財物
  - 利用抽獎/投票，騙取個資、按讚
  - 利用假新聞，影響社會輿論
  - 賣假貨、網路霸凌、肉搜、...

圖片來源：https://www.facebook.com/banai.shunz

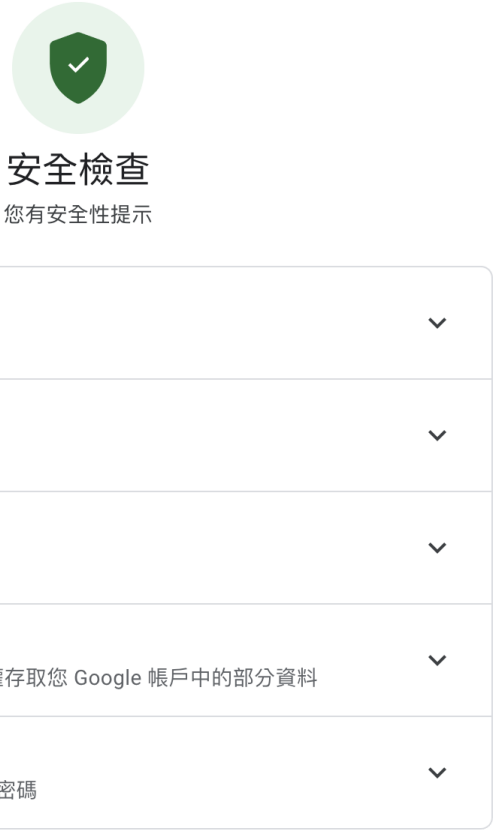
FACEBOOK-隱私設定檢查

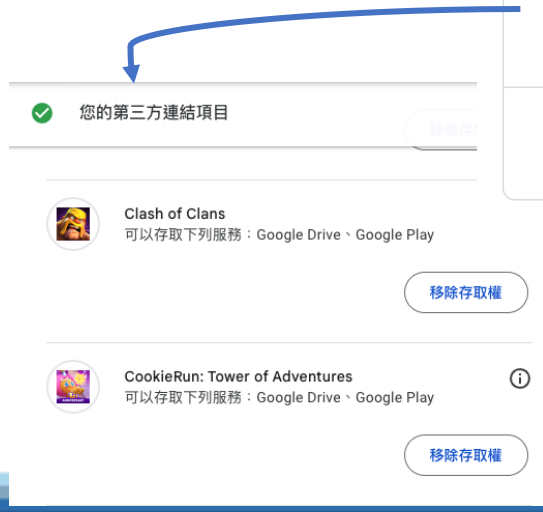
- 帳號
  - 設定和隱私
    - 隱私設定檢查



GOOGLE 帳號安全檢查

- 執行官方的「安全檢查」
  - https://myaccount.google.com/security-checkup
  - 檢查已登入的裝置
  - 近期安全性事件
  - 登入和救援選項
  - 第三方應用程式存取權
  - 已儲存的密碼
- 使用雙重驗證



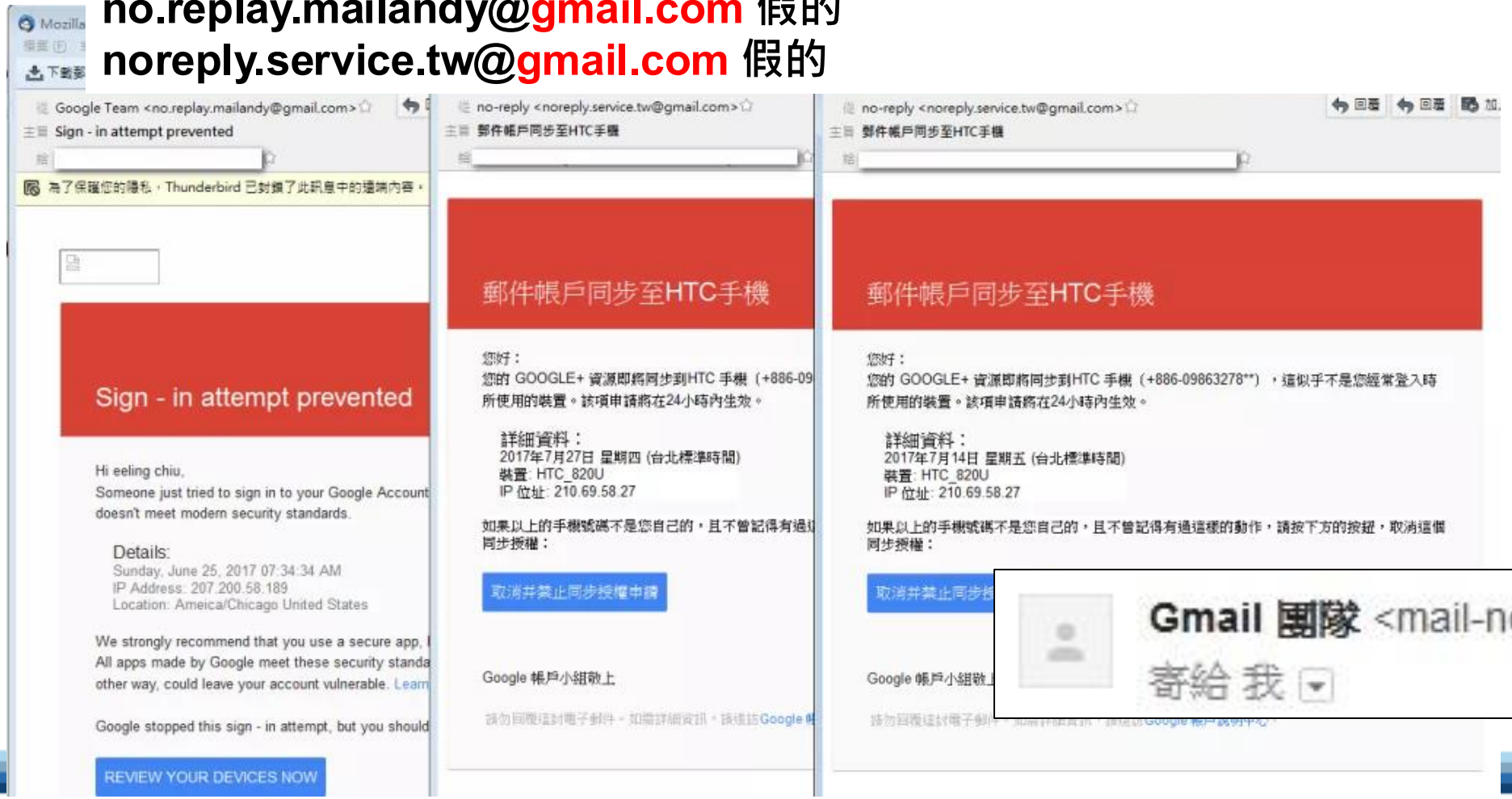


Google官方通知信

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。

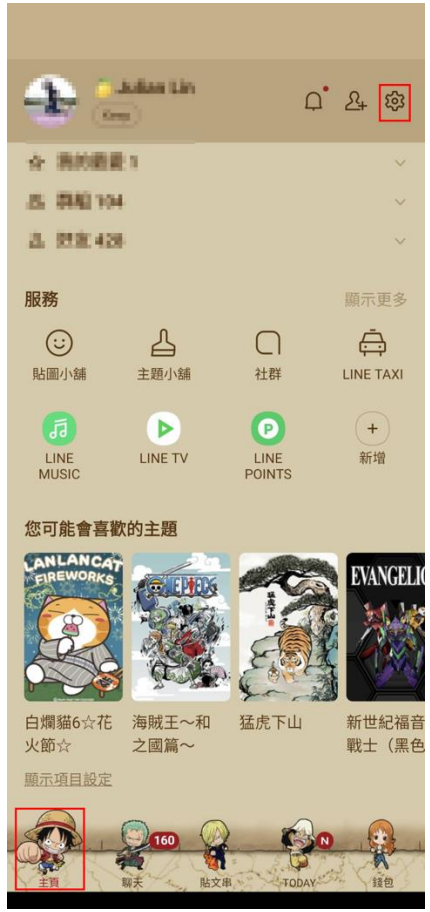
no.replay.mailandy@gmail.com 假的

noreply.service.tw@gmail.com 假的



LINE 安全設定

- Letter Sealing設定位置



- 確認是否開啟

https://official-blog-tw.line.me/archives/78352086.html

LINE 安全設定

- Letter Sealing

可套用Letter Sealing功能的資訊

在Letter Sealing功能開啟的狀態下收發訊息時，以下內容將自動加密。

·文字訊息（不包含透過YouTube等其他服務傳送的訊息）
·位置資訊
·圖片／影片／語音訊息
·檔案

·1對1聊天室的語音／視訊通話

Letter Sealing的保護範圍：
LINE 群組的話，50人以內的群組，超過 50 人 不支援。

⚠ 請注意

·圖片／影片／語音訊息／檔案可能會因LINE版本或使用環境等因素而無法加密。
·基於保護資訊安全的觀點，Letter Sealing功能無法關閉。
·移動帳號後，過去傳送及接收的聊天記錄可能因Letter Sealing功能影響而無法顯示。
發生此情況時，請確認顯示「無法解密此訊息」等訊息而無法查看聊天訊息的說明。

https://help.line.me/line/ios/?contentId=50000087&lang=zh-Hant https://www.lycorp.co.jp/en/privacy-security/security/transparency/encryption-report/2024/

LINE安全設定


隱私設定
密碼鎖定
若您忘記密碼，必須先刪除LINE，再重新安裝。
請留意：您過去的聊天記錄將會被全數刪除。
允許利用 ID 加入好友
其他用戶可透過 ID 搜尋將您加入好友。
阻擋訊息
開啟本功能後即可阻擋不是來自好友的訊息。
Letter Sealing
使用進階加密功能可保護訊息。但僅限於和同時開啟Letter Sealing功能的好友聊天時有效。
更新行動條碼
外部應用程式存取
將您加入好友的用戶若允許外部應用程式存取其好友名單資料時，您在此處的設定可允許或拒絕該外部應用程式存取您的個人檔案。
提供使用資料
廣告相關設定


我的帳號
Facebook
開始同步
連動中的應用程式
透過LINE登入或允許存取而與LINE帳號連結的服務。
顯示項目設定
登入安全性
連動其他裝置
允許自其他裝置登入
開啟此設定後，您可在其他裝置（如電腦、智慧手機、平板及智慧手錶）上登入您的LINE帳號。
網頁登入雙重認證
以LINE登入其他網頁時可開啟雙重認證。
部分服務需執行雙重認證才能登入。
使用密碼登入
若您已啟用生物辨識登入，建議可關閉此設定，以便您管理登入安全性。關閉此設定後，仍可使用其他方式登入。
登入中的裝置

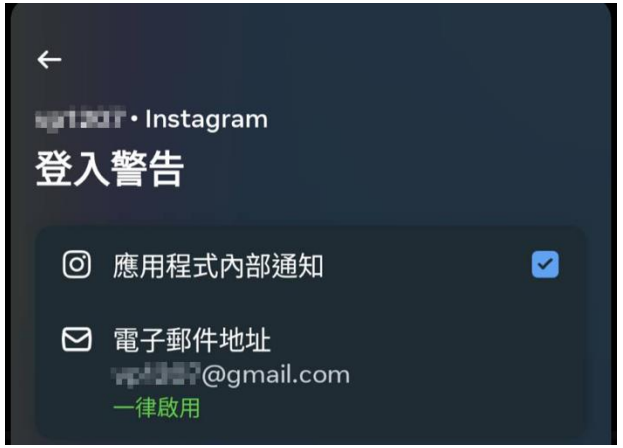
Instagram

- 設定和動態> 帳號管理中心>密碼和帳號安全
  - 帳號安全檢查

- 你登入的位置

- 最近的電子郵件

- 登入警告



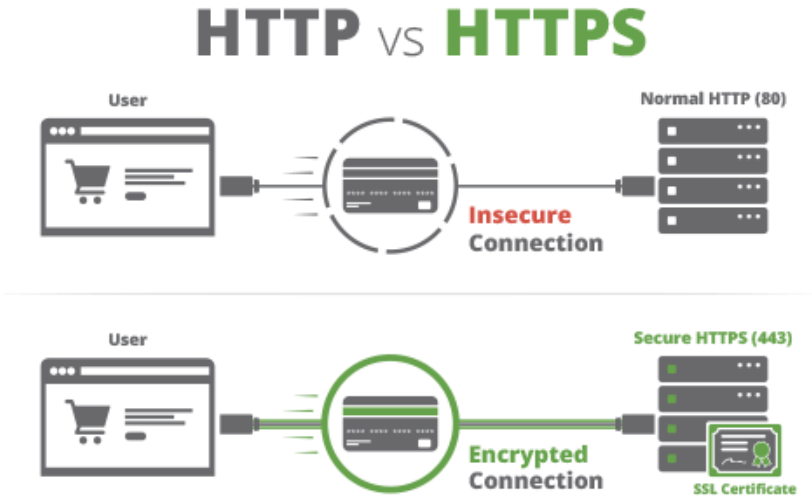
中華資安國際
CHT Security

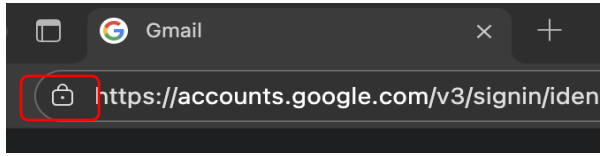
職場與日常生活的資安管理

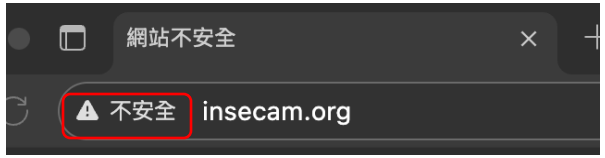
圖片來源：https://finance.technews.tw/2021/09/14/top-10-emerging-hot-jobs/

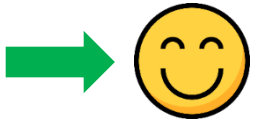
瀏覽網頁時 HTTP/HTTPS 有什麼差別

- 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

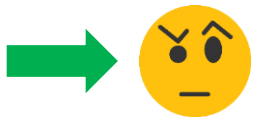




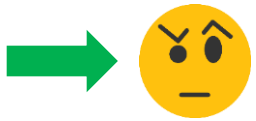




安全!



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

如何辨別網址的主網域

網址首段是「gov.tw」結尾的，才是政府專用網址！

最近網路上有傳出民眾收到未繳交通罰款的詐騙簡訊，簡訊上用偽造的監理服務網，並且刻意混淆，以民間商業縮網址服務加上不屬於政府網站的網址結尾改為「gov.tw」，意圖冒充政府專用網域 https://gov.tw/ 。

網址是網路上完整的地址，而在網址首段的「網域」在使用時是需要進行申請的 因此網址首段為 gov.tw 結尾的才是政府網站（例如 https://moda.gov.tw），其他出現在任何地方都有可能是偽冒（例如 https://xxx/mvdis.gov.tw），切勿點擊來源不明的簡訊或訊息連結，避免上當受騙。

- https://moda.gov.tw/press/clarification/4791

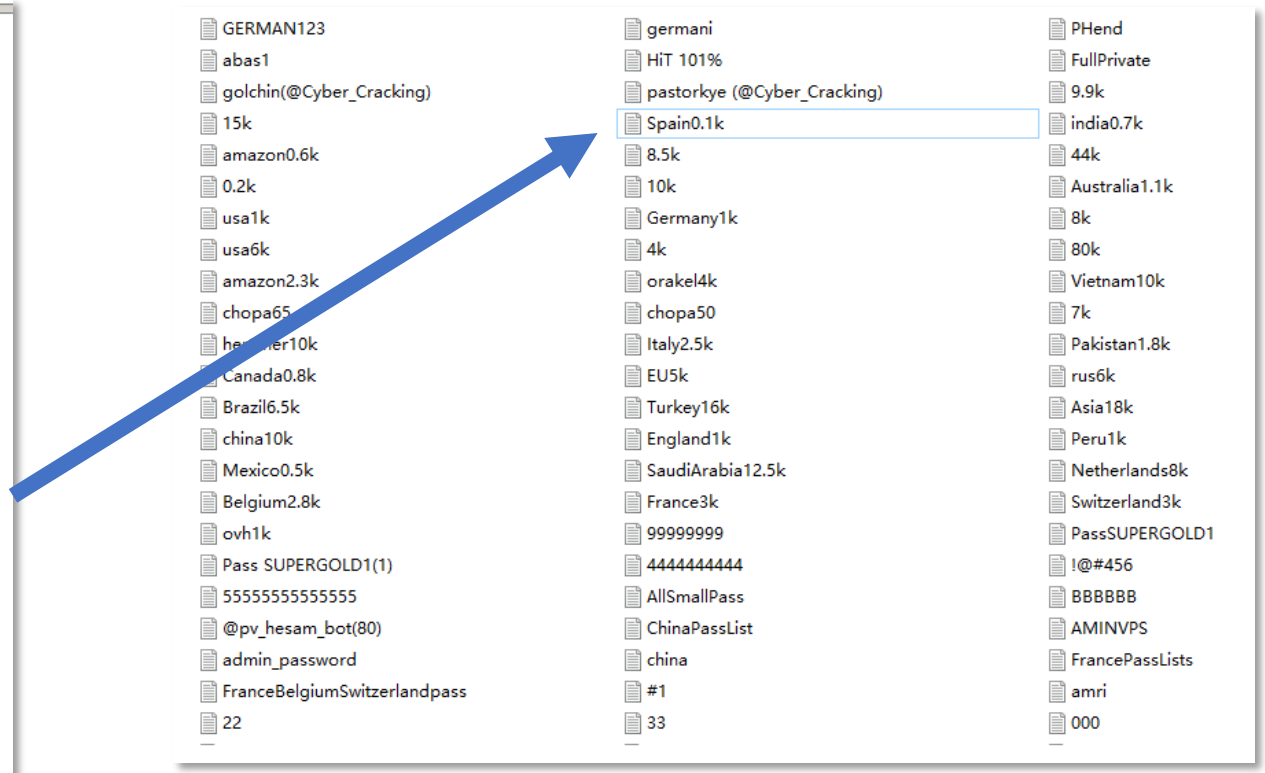
https://mvdis-gov-twyv.net/tw
https://6000-mof-tw.net/tw
https://mofy-gov.net/tw

勿再使用弱密碼

- 網路存在眾多常見且非常弱的密碼清單，可供駭客使用字典檔做暴力破解

Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]	2018[10]
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321
20	123123	football	12345	michael	login	sunshine	master	!@#$%^&*
21	654321	jesus	password1	superman	princess	master	hello	charlie



左邊清單只是駭客眾多字典檔的冰山一角

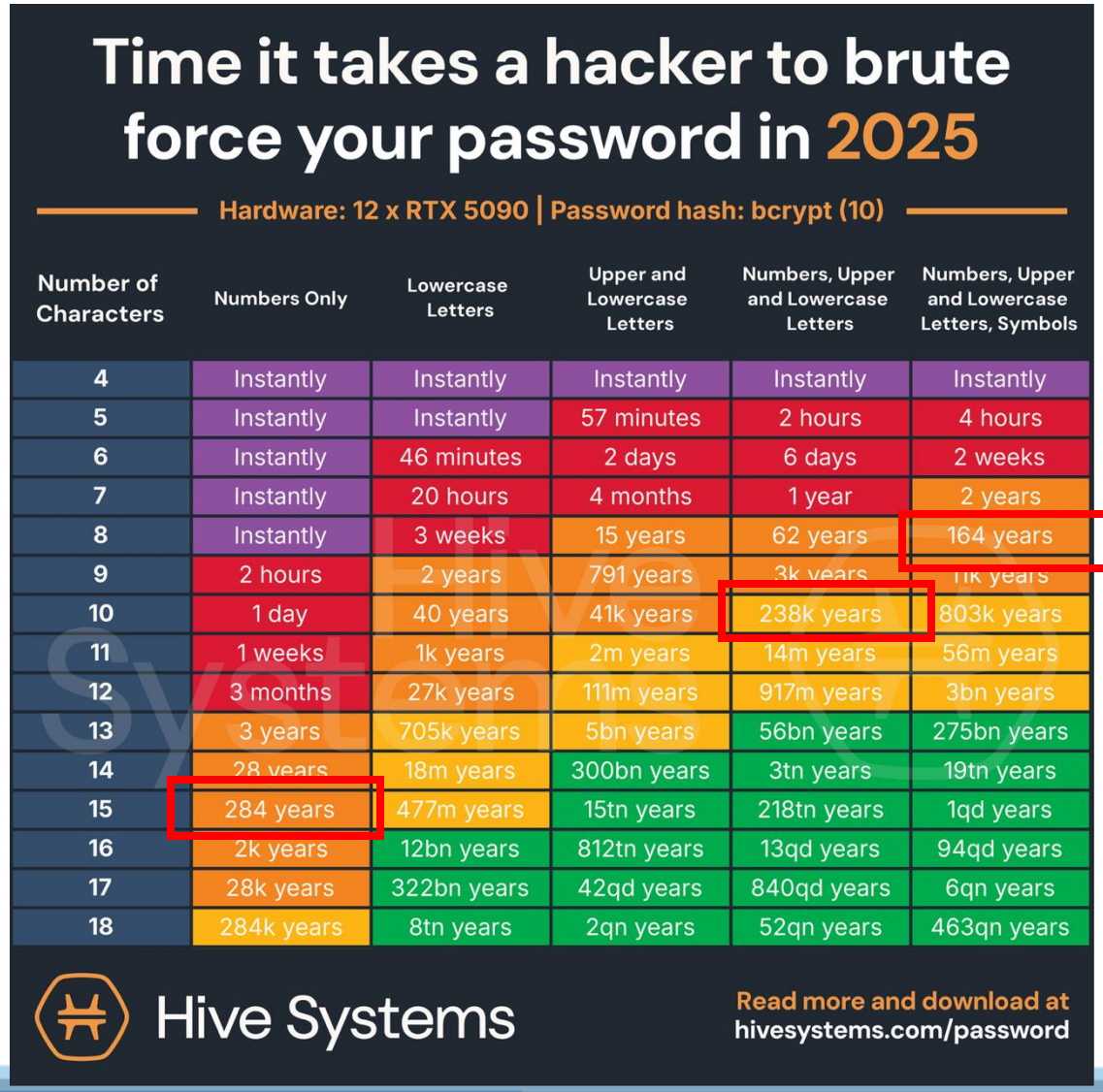
https://web.tainan.gov.tw/houbi/News_Content.aspx?n=7055&s=7705285

NIST改變心意

- NIST(美國國家標準暨技術研究院)文件2025年 SP 800-63B
  - 數位身份指南，拋棄許多傳統上「被認為安全」但實際上對用戶不友善且效果不佳的規則。
  - 廢除「強制定期更換密碼」：不一定要3個月改一次!
  - - 強調「長度」而非「複雜度」： 最好超過12碼, 可有基本複雜度要求，但不一定要非常複雜!
  - - 強制檢查「已洩露密碼黑名單(Blocklist)」: 已洩漏的建議不再用，可用 https://haveibeenpwned.com/ 自我檢查帳號及密碼是否外洩
  - - 多因素驗證(MFA)仍是王道

https://blog.darkthread.net/blog/15-chars-password/ https://pages.nist.gov/800-63-4/sp800-63b.html

密碼更在意的是-長度



Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

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	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

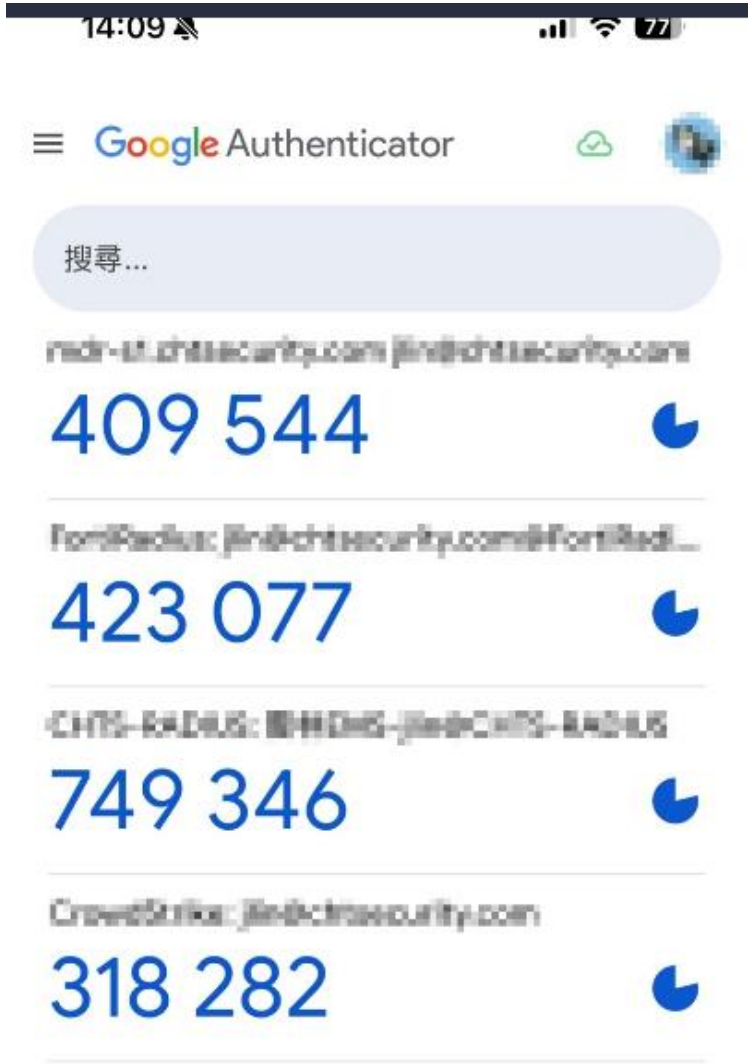
Hive Systems

Read more and download at hivesystems.com/password

- １５個純數字 ＞ 8個字元符合複雜度

https://www.hivesystems.com/blog/are-your-passwords-in-the-green

開啟多因子認證，強化安全性

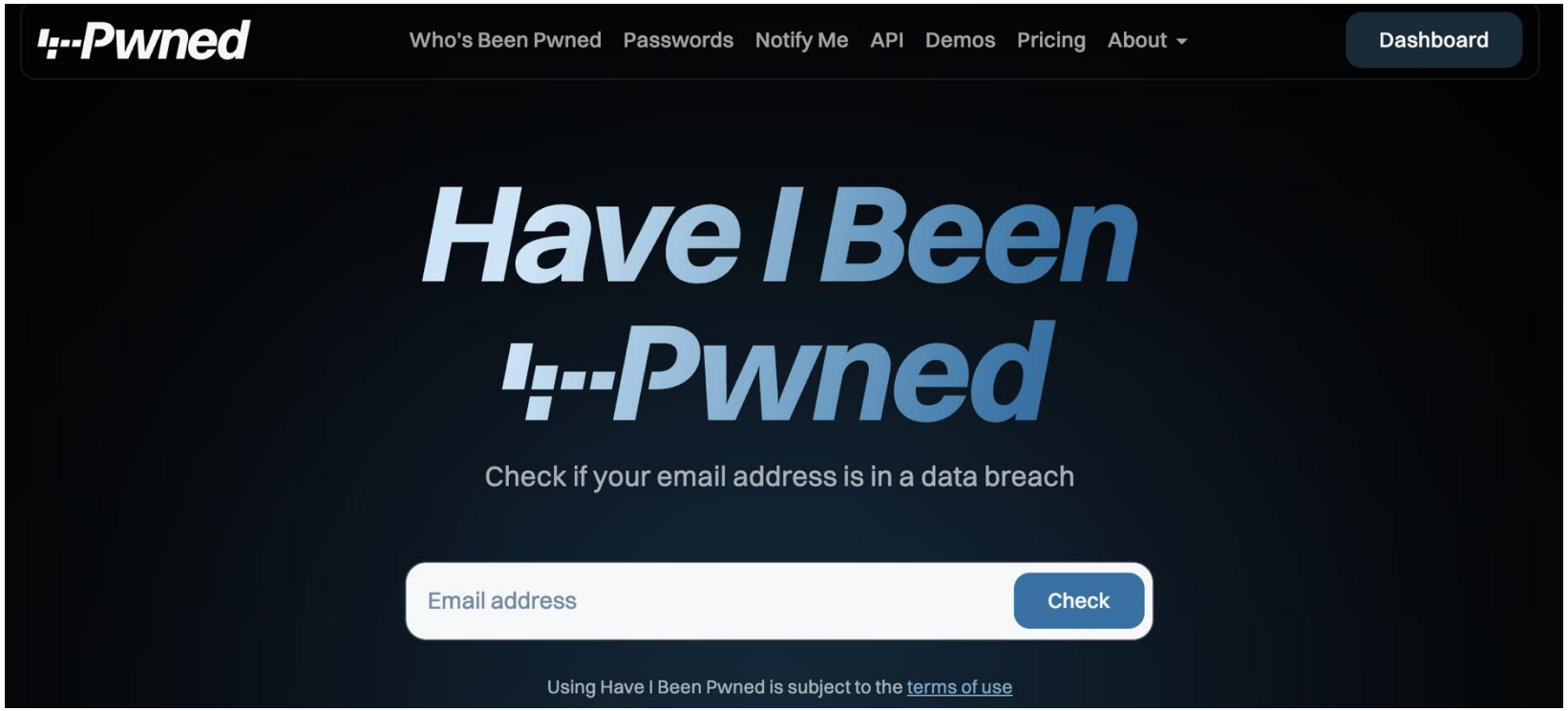


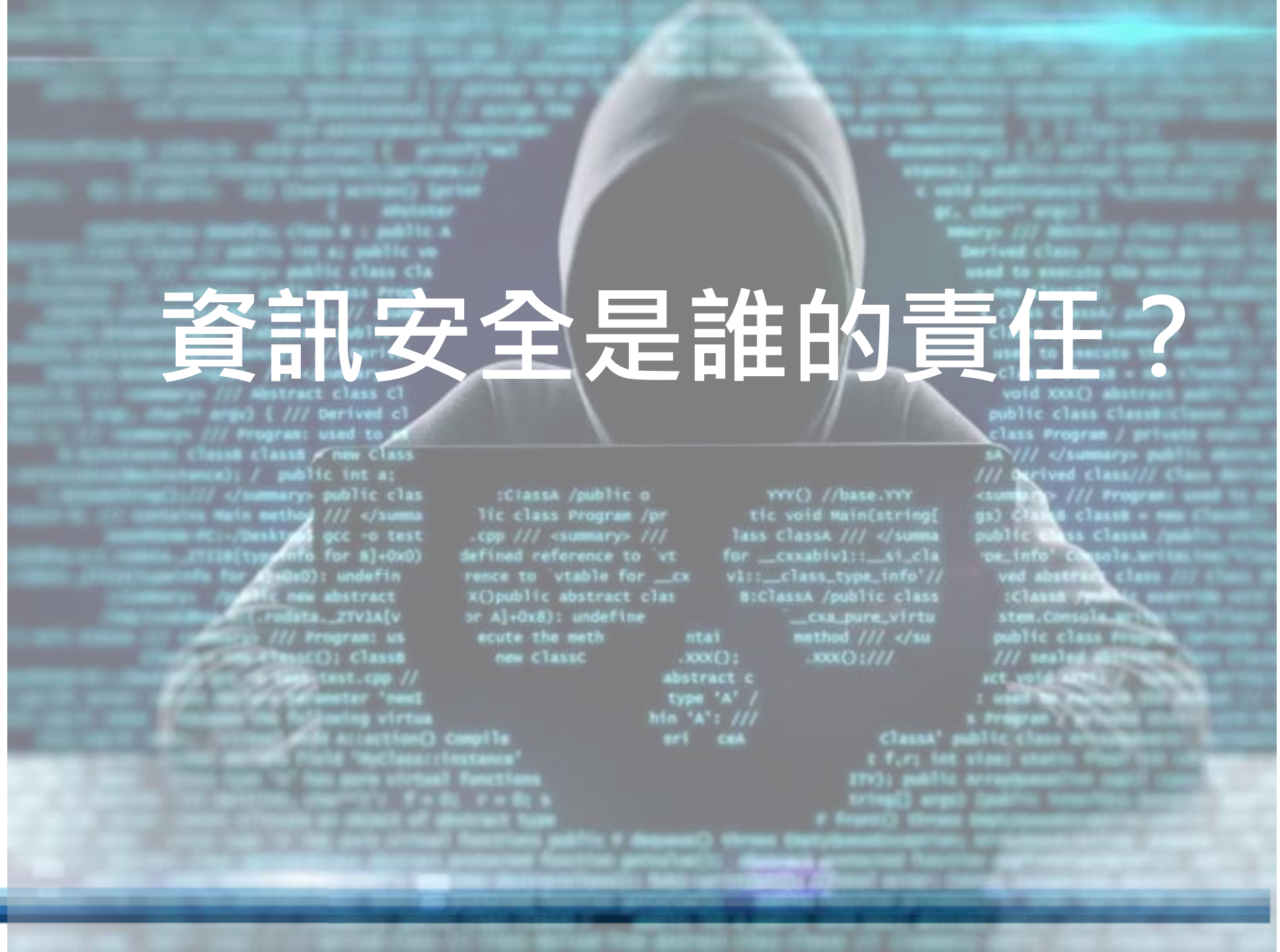
多因子認證是甚麼?

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

檢查自己的 Email 是否在外流名單

- 網站名稱：Have I Been pwned
- 網站鏈結： https://haveibeenpwned.com/





資訊安全是誰的責任？

資訊安全是誰的責任？

- 老闆？
- 資安長？長官？
- 資訊部門？
- 稽核人員？資安窗口？
- 資訊開發/維護廠商？
- …或是…新來的菜鳥？

中華資安國際
CHT Security

課後問券

Thank you.