

# 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



# 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

## 為何企業難以抵抗資安攻擊 (2023 資安弱點排名)

5成多企業員工資安意識不足，3成企業缺乏資安老手



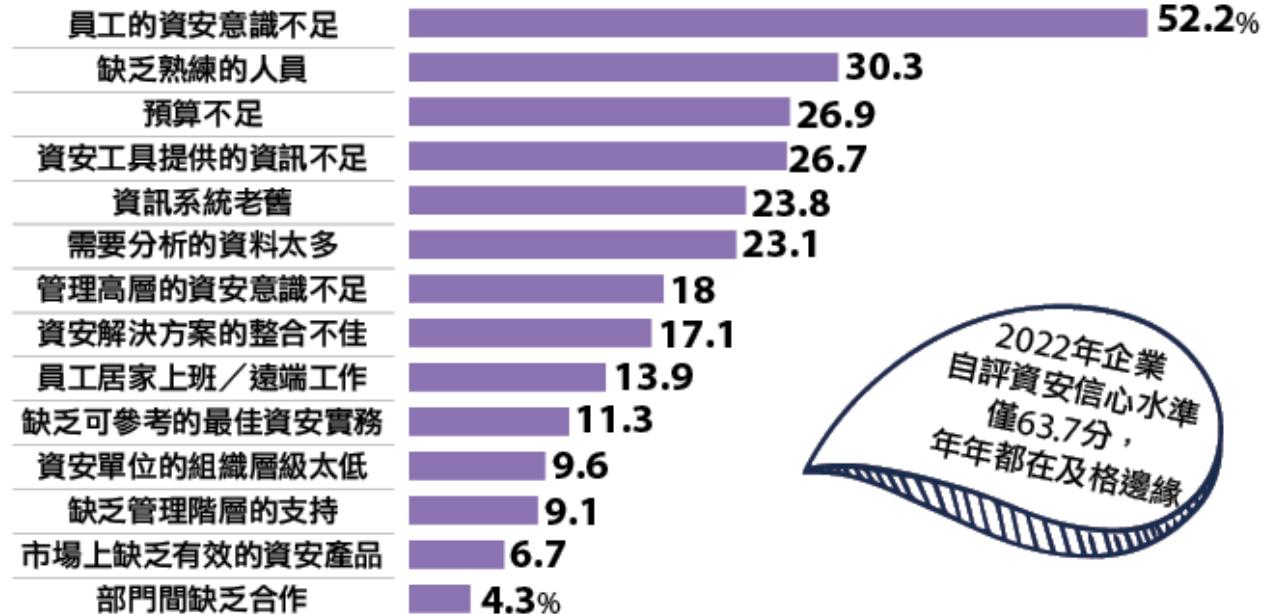
資料來源：2023 iThome CIO大調查，2023年7月



- 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

## 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



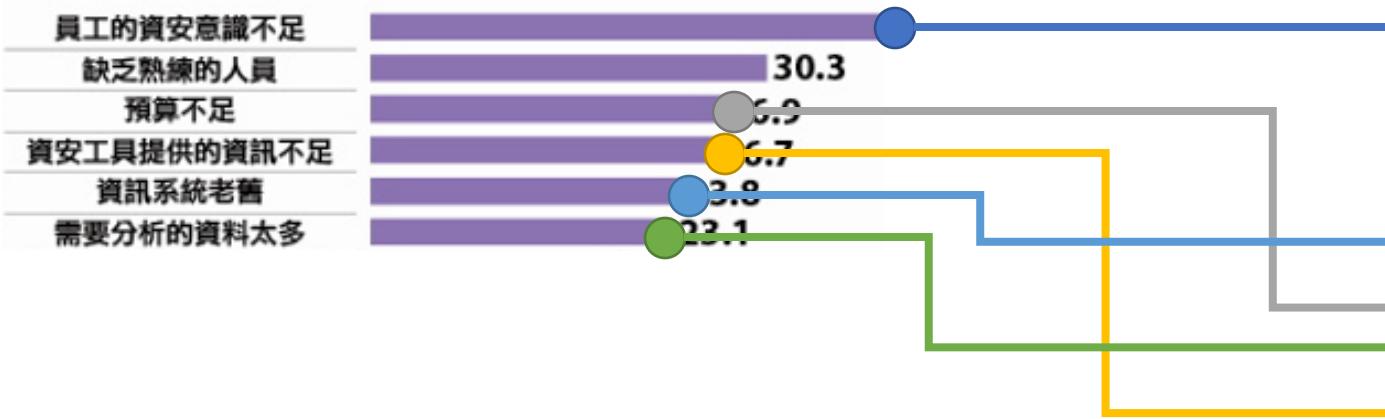
2022年企業  
自評資安信心水準  
僅63.7分，  
年年都在及格邊緣

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

# 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



男子僅用一發弓箭  
就逃脫了棕熊的襲擊



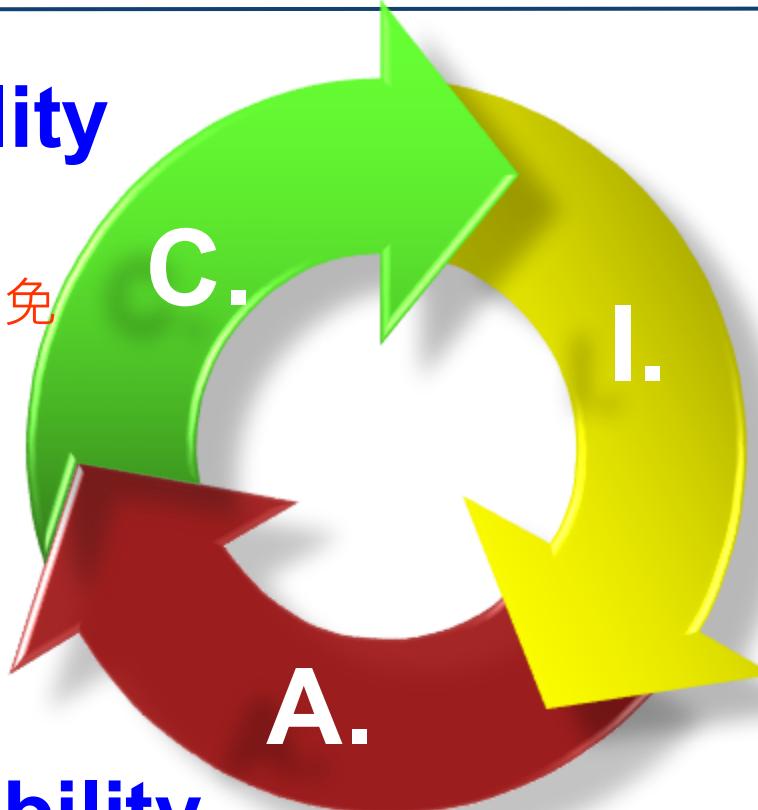
# 資訊安全三大要素

## Confidentiality (機密性)

確保資訊隱密性並避免  
遭到非法存取

## Availability (可用性)

確保可適時提供可用  
及正確之資訊



## Integrity (完整性)

確保可提供正確與完  
整的資訊

## 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**





# 資安新聞事件

---



## 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

The screenshot shows a news article from Coupang's newsroom. The header includes the Coupang logo and navigation links for Company Profile, Coupang News, Blog, Download, Search, and a share icon. The main title is "Coupang酷澎台灣就近期酷澎韓國資安事件之內部調查進度說明". Below it, it says "By Coupang Taiwan • 2025-11-29". There are social sharing icons for Facebook, Twitter, LinkedIn, and a link icon. A "PDF DOWNLOAD" button is also present. The text states: "根據目前的調查結果，沒有證據顯示Coupang酷澎台灣的消費者資料外洩。我們持續調查此事件，並與頂尖獨立資安公司的專家進行合作。" Another paragraph below discusses the Korean incident: "在韓國，調查顯示客戶帳號遭外洩的規模約為 3,370 萬筆。遭外洩的韓國消費者資料僅限於姓名、電話號碼、電子郵件地址、寄送地址及部分訂單紀錄，不包含任何支付資訊、信用卡號碼或登入密碼；相關重要資訊仍受到安全保護。"

## 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

The screenshot shows the KoiDEX analysis interface for the 'Urban VPN Proxy' extension. At the top, there's a navigation bar with 'KOIDEX', 'Blog', 'Enterprise', and 'Shai Hulud'. Below that is a sign-up button and a 'Check out Koi' button. The main content area displays the extension's name, 'Urban VPN Proxy', with a small icon of a shield with a 'U'. A brief description follows: 'Get the best secured Free VPN access to any website, and unblock content with Urban VPN'. It shows a risk level indicator with 'High' highlighted in orange. Below this, there are tabs for 'Analysis summary', 'Findings' (which is selected), 'Code Analysis', 'API Calls', 'Secrets', 'Vulnerabilities', 'External communication', 'Dependencies', and 'Licenses & compliance'. The 'Findings' tab shows a list of findings, with the first one being 'make\_chrome\_yours/privacy'. To the right, under 'Listing details', it says 'Publisher: Urban VPN'. At the bottom, there's a large 'Findings' button.

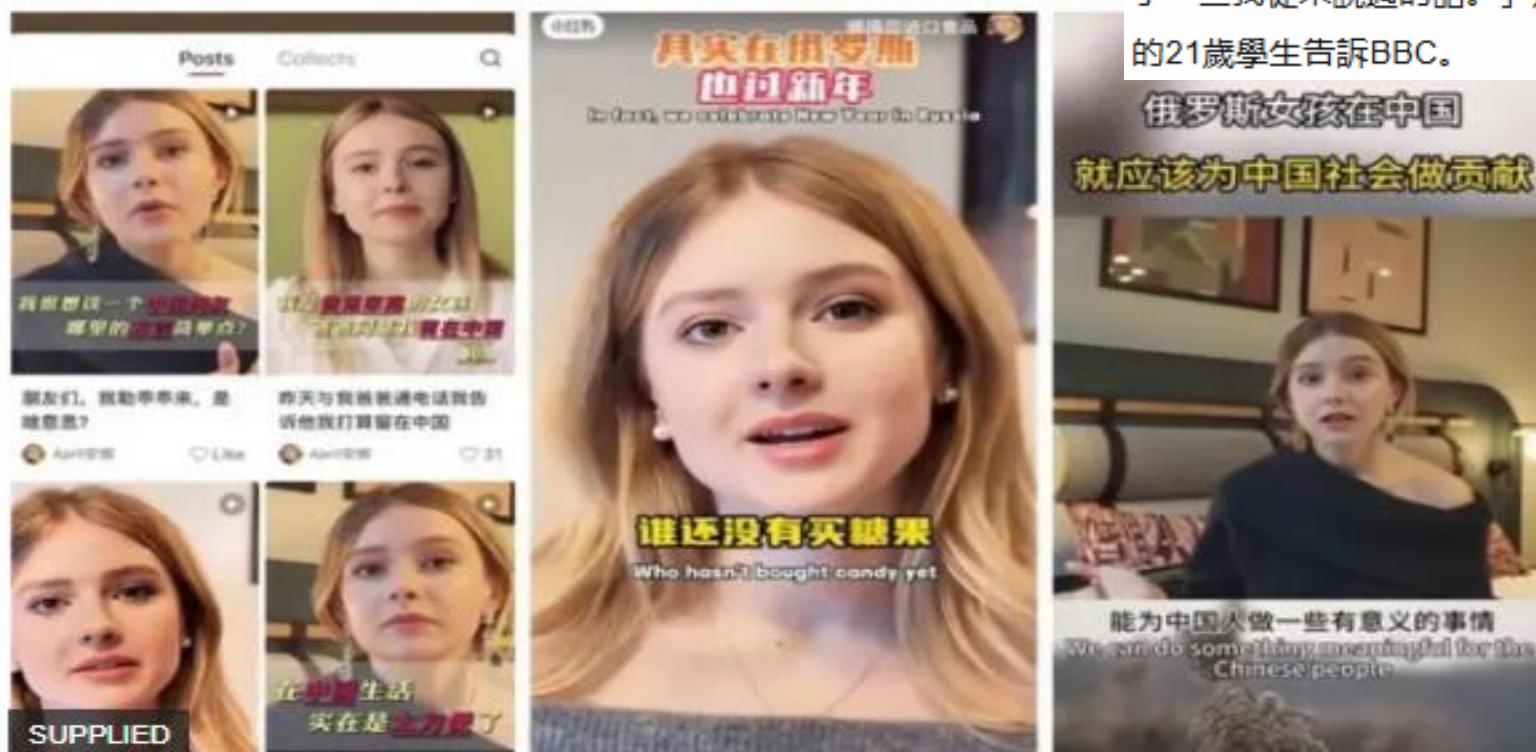
- Urban VPN Proxy
- 1ClickVPN Proxy
- Urban Browser Guard
- Urban Ad Blocker

# 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。

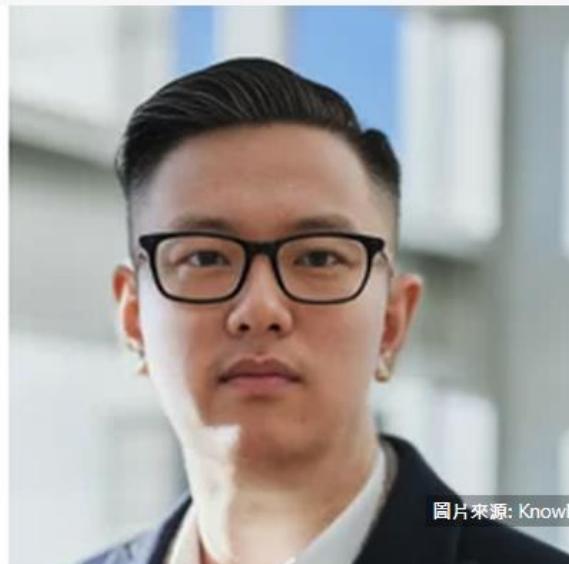
<https://www.bbc.com/zhongwen/trad/world-69014941>

## 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

↑ 讀 47 分享



圖片來源: KnowBe4

Hello World Dev Conference  
Organized by iThome  
連線！台灣 Line 特別專題議程  
揭露 LLM Ops 讓 LLM 服

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



## 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!

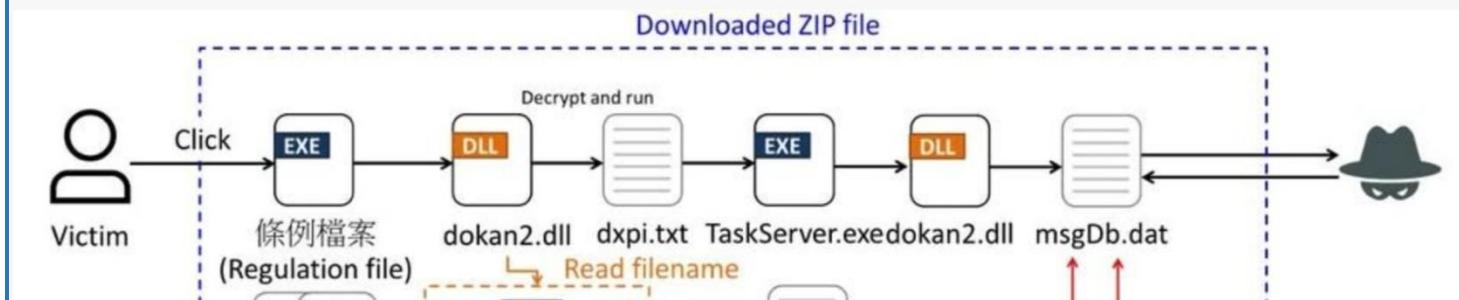


## 駭客假冒政府機關與商業夥伴，在臺灣散布惡意軟體HoldingHands RAT、Gh0stCringe

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。

# 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/>



## 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」？

**Screenshot 1:公路總局公告 | 案件辦理時效通知**  
請於24小時內完成，逾期將影響其他作業（郵件代碼 [REDACTED]）

**Screenshot 2:交通違規案件緊急通知**  
請於 114 年 9 月 9 日 23:59 前完成繳款與核銷！逾期將登錄駕照扣點 2 點，並每日累計滯納金，影響駕照後續申辦及審查流程

**Screenshot 3:結果備註**  
[X1N8K-R2G6JPYQ]辦理-函件 ☆  
查閱 收件匣  
1Z17/中華民國... 15:37 🌟 ← :  
寄給我  
核定件-  
編號: [REDACTED]  
親愛的駕駛人您好：  
依資料檢核結果，您的名下目前有一份正式函件待查閱。該函件關係到行車權益與管理事項，請務必於期限內完成相關處理，以免衍生額外負擔或影響後續作業。  
如已完成，紀錄將於 3-5 個工作天內更新，無需重複操作。請妥善保存相關憑證，以利後續查詢。  
祝您行車平安。

# 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](#)

監理服務管理處  
do\_not\_reply@on24event.com

收件者：您 tatusaku@hotmail.com

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：

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-twv.net/tw>

如有任何疑問，請於辦公時間洽詢：

- 服務專線：[\(02\) 2763-0153](tel:(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-twv.net/tw>



# 資安新聞-實例

## 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月06 日	在禁止臨時停車處所停車	900	114年09月21 日

線上繳費

APP 監理服務網-首頁

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！

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  
VISA MasterCard American Express JCB  
有效日期: 11/29 安全碼CVV: 225

此字段有誤，請檢查

確定金融帳號資訊

黏貼隔熱紙

交通罰鍰查詢及繳納注意事項

中華資安國際 CHT Security

## 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[.]000
  - line-chinese[.]000
  - line-tw[.]000
  - windows-line[.]000

# 資安新聞(續 )

https://www.google.com/search?q=line+電腦版+下載&sca\_esv=0b6cd31ca70c40ac&sxsrf=AE3TifMVa2LFIXB\_rkLrIDFt3LpnW6x5-s

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 ... 不安全 https://www.linerpc.com

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. 發現新鮮事 ...



此網域已經遭到  
m d 數位發展部  
Ministry of Digital Affairs 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/>

## 釣魚網站通報

通報人 email \*

請輸入通報人email

釣魚網站 \*

請輸入釣魚網站網址

模仿對象名稱 \*

請輸入模仿對象名稱

模仿對象網址 \*

請輸入模仿對象網址

釣魚網址行業類型 \*

請選擇釣魚網站類型

上傳釣魚網站截圖(圖片大小限制為5MB) \*

請選擇檔案 尚未選擇檔案

尚未選擇檔案

通報人公司統編

請輸入通報人公司統編

通報人公司抬頭

請輸入通報人公司抬頭

請說明您判斷為釣魚網站之原因 \*

 我已閱讀並同意 個人資料保護法應告知事項 (版次編號：C-G-20250616-000003) 及使用規範

Console

# 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)

網站

- 1 Apple
- 2 mobile01
- 3 Yahoo
- 4 Yahoo
- 5 Facebook
- 6 Facebook
- 7 8591
- 8 5285
- 9 Yam
- 10 Emailcash
- 11 www.hk199.com
- 12 Mu空間
- 13 MyFreeCams
- 14 玩運彩
- 15 玩運彩
- 16 開誠購
- 17 博客來
- 18 富邦銀行
- 19 Google
- 20 Gash
- 21 CD70799A4A
- 22 PayPal
- 23 bet365
- 24 EC2電子錢包
- 25 fileserve免空下載
- 26 九州
- 27 九州
- 28 mux dj

# 資安新聞

英國14歲少女自殺 法院判社群平台「殺人」



- 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负面影响的內容
- 因為演算法的關係，推送並未主動查詢的內容
- Meta與Pinterest

# 2024企業資安風險圖-政府與學校

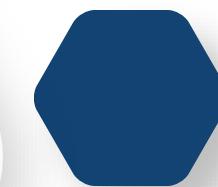
【政府與學校】2024企業資安風險圖（2024~2025）





# 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



# 攻擊手法介紹：APT

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

一般駭客



個人或駭客結盟

亂槍打鳥，速戰速決

無差別攻擊

目標



APT

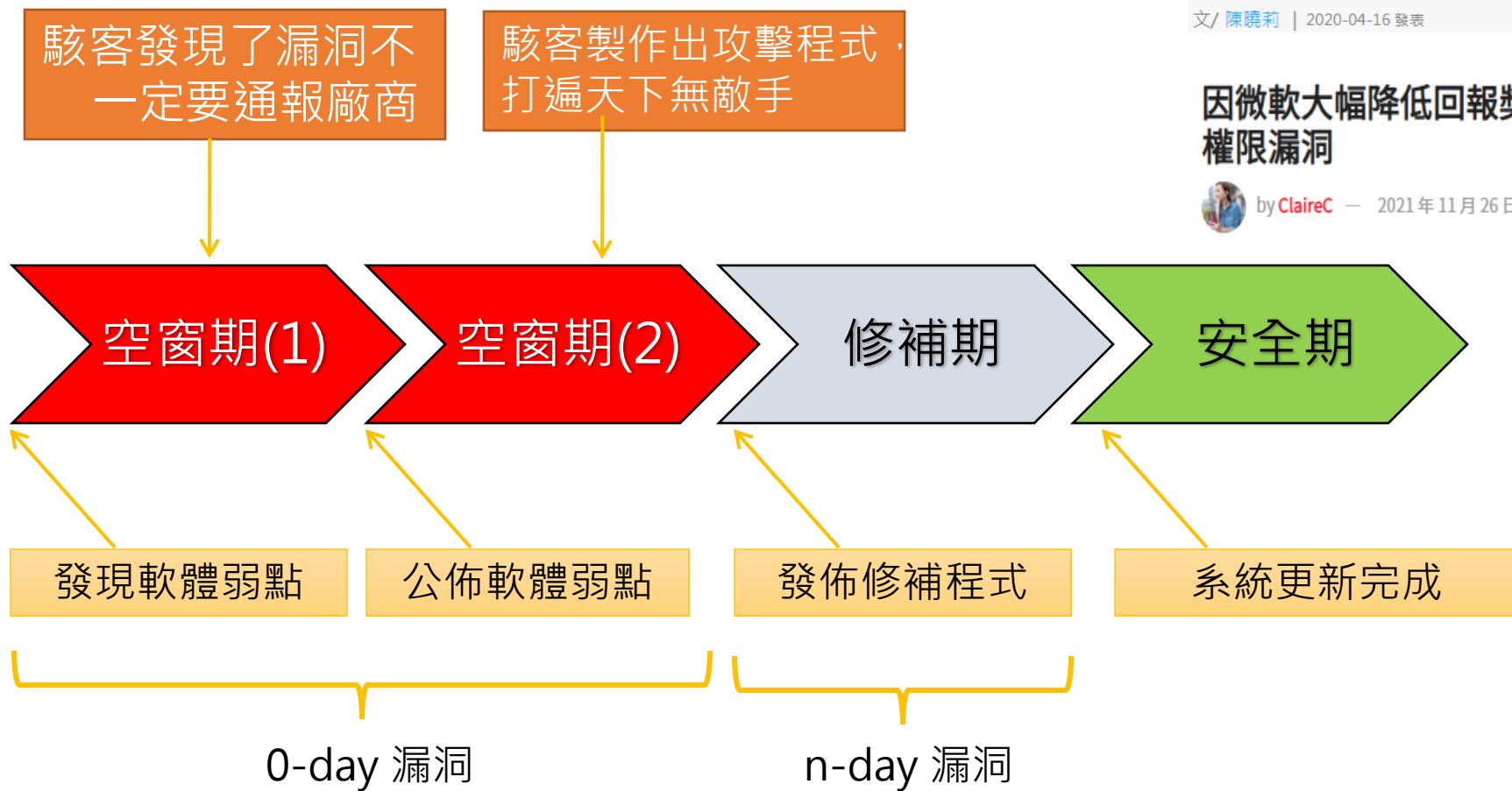
針對性



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



## 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

首頁 信箱 新聞 股市 氣象 運動 影音 娛樂 Flickr 購物中心 商城 拍賣 更多 ▾ 設定 Yahoo 為首頁 台北 sunnyboyccc 信箱

YAHOO!  
奇摩

設為首頁 新聞 股市 理財 運動 中華職棒 名人娛樂 電影 TV 音樂 遊戲 電競 Flickr 字典 知識+ 信箱

6月初開始，只要用IE上雅虎奇摩網頁：[tw.yahoo.com](http://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！

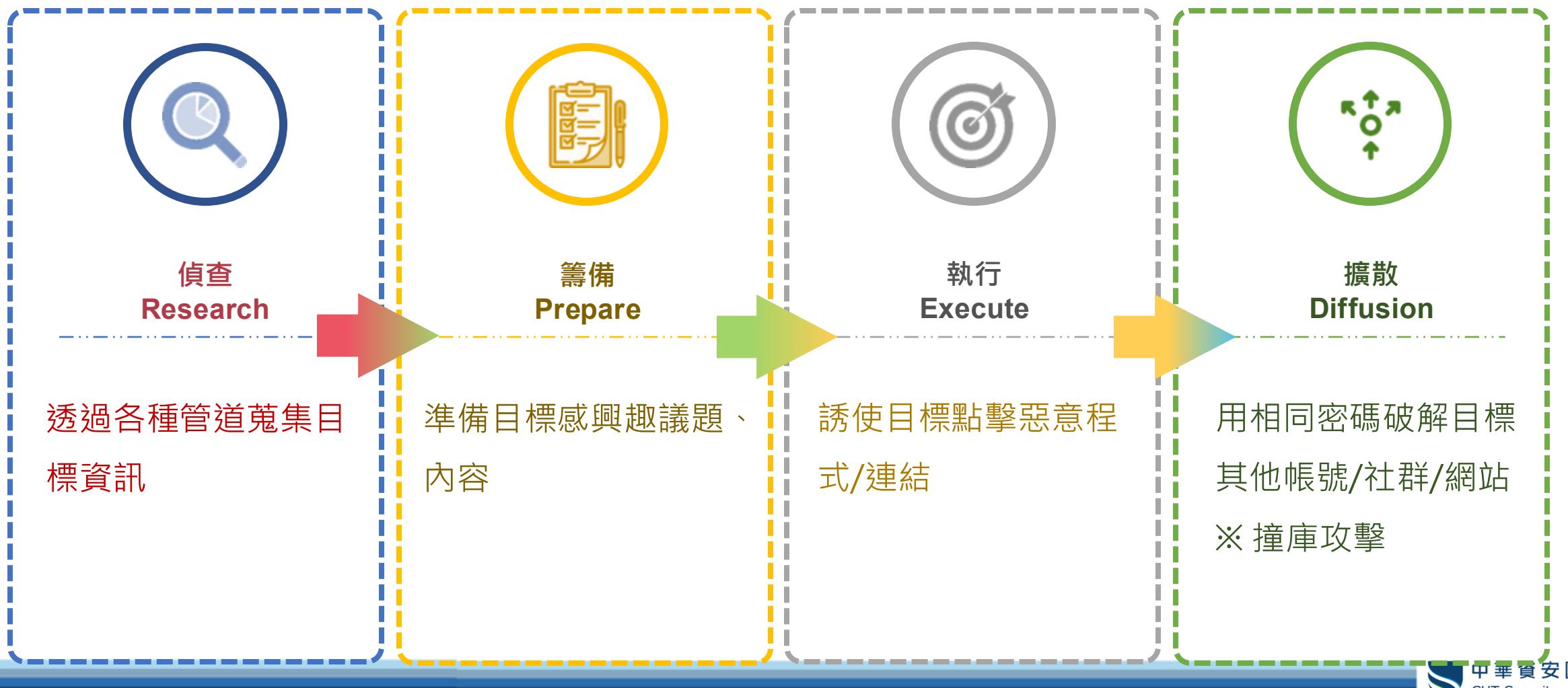
參考來源文章  
<https://blog.malwarebytes.com/cybercrime/2016/06/neutrino-exploit-kit-fills-in-for-angler-ek-in-recent-malvertising-campaigns/>

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Malvertising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...

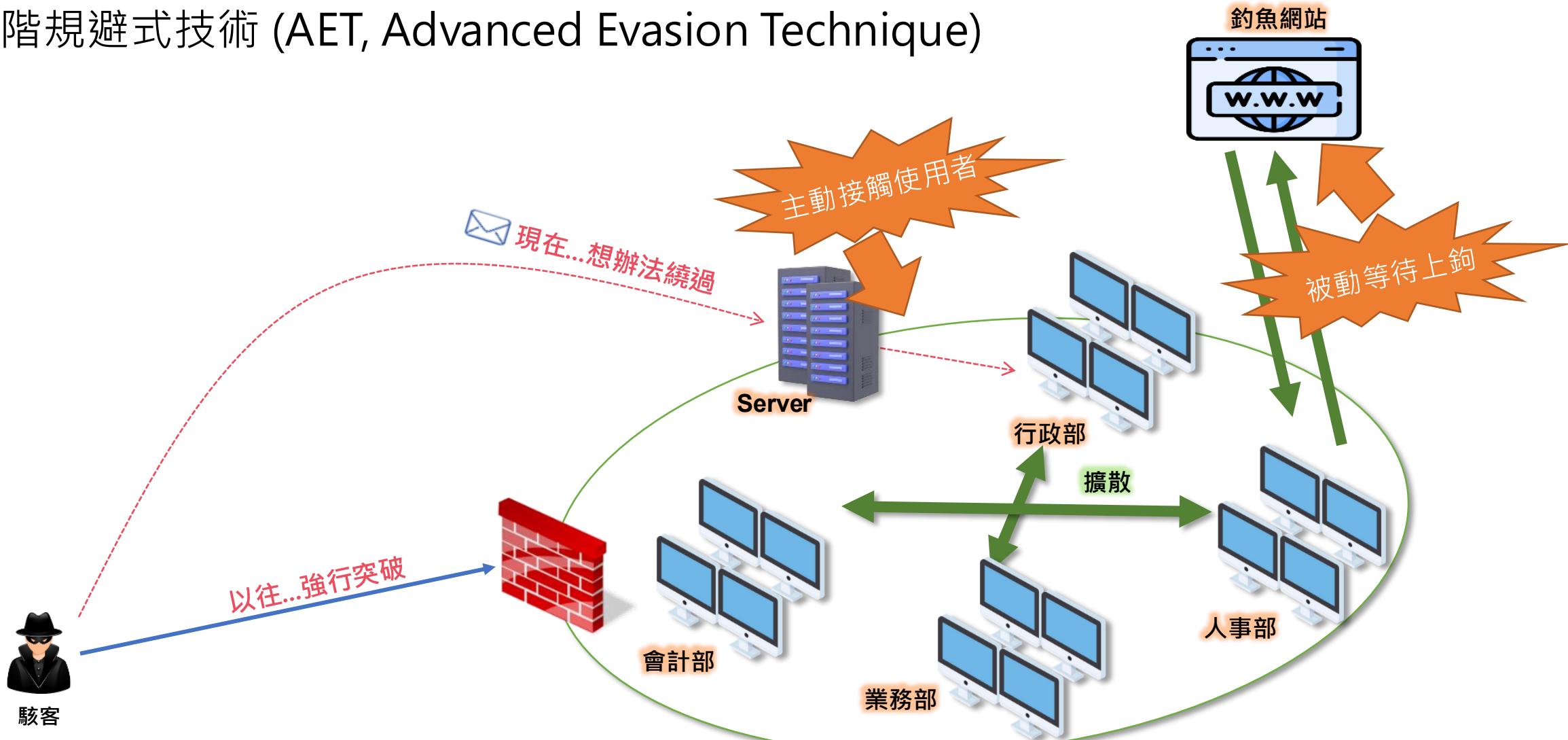
# 影片的啟發

- 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)

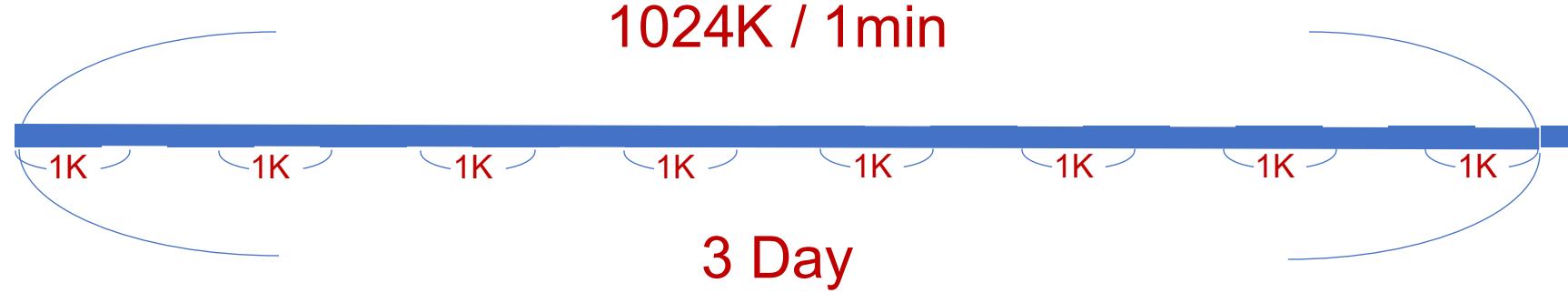
- 進階規避式技術 (AET, Advanced Evasion Technique)

Call Home:

[https://www~~dropbox~~.com/fakefileabc.exe](https://www.dropbox.com/fakefileabc.exe)

[https://~~one~~drive.com/public/infected.exe](https://onedrive.com/public/infected.exe)

[https://~~google~~cloud.com/aabbat](https://googlecloud.com/aabbat)



# 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



# AET 攻擊手法範例：短網址



This diagram shows the process of deconstructing a shortened URL. It starts with a red box labeled "短網址還原網站" (Short URL Reconstruction Website). Inside, there is a form field labeled "短網址：" (Short URL:). Below the form, two arrows point downwards from the text "https://goo.gl/FahH3J" to the resulting long URL "https://www.dropbox.com/s/qfyc2t8hnurzllk/%E5%9B%9E%E5%9F%B7%E5%96%AE.apk". This demonstrates how a shortened URL can be expanded to reveal its original destination.

# 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

[tw.yahoo.com](http://tw.yahoo.com)

## 範例二：說明

[點我抽獎](#)

## 範例三：圖片



## 範例四：檔案



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?!

收件匣 4046

我的最愛

收件匣 寄件備份 寄件匣 O2 ISO制度管理

檔案 常用 傳送 / 接收 資料夾 檢視 說明

新增電子郵件 新項目 從伺服器復原刪除的郵件 清理 垃圾郵件 新增 動作

刪除 封存 回覆 全部回覆 轉寄 IM 其他 共用到 Teams 快速步驟 移動 規則 傳送至 OneNote 指派原則 未讀取/已讀取 分類 待處理 標籤 中文繁簡轉換 簡繁轉換 簡繁轉換 新增群組 搜尋連絡人 通訊錄 瀏覽群組 選擇電子郵件 群組 尋找

全部 未讀取

(i) 復原最近從此資料夾移除的項目

! | 立 | 凸 | ① 寄送者 | 收到日期 | 2022/9/14 (週三) 下午 2:36

! nccst-tw@outlook.com 資通安全協查函-行政院國家資通安全會報技術服務中心

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

信件內容

1. 主旨

2. 各收信單位：

3. 為確保此次資安審查真實性，本次審查採用不提前知會，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。

4. 依循國家資通安全管理法，未按要求完成此次資通安主審查，並因此造成三級及以上資通安事件的（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。

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

6. 附註：壓縮檔案之解壓密碼統一為nccst@2022

National Center for Cyber Security Technology

附件：附件1-NCCST 資通安主審查[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

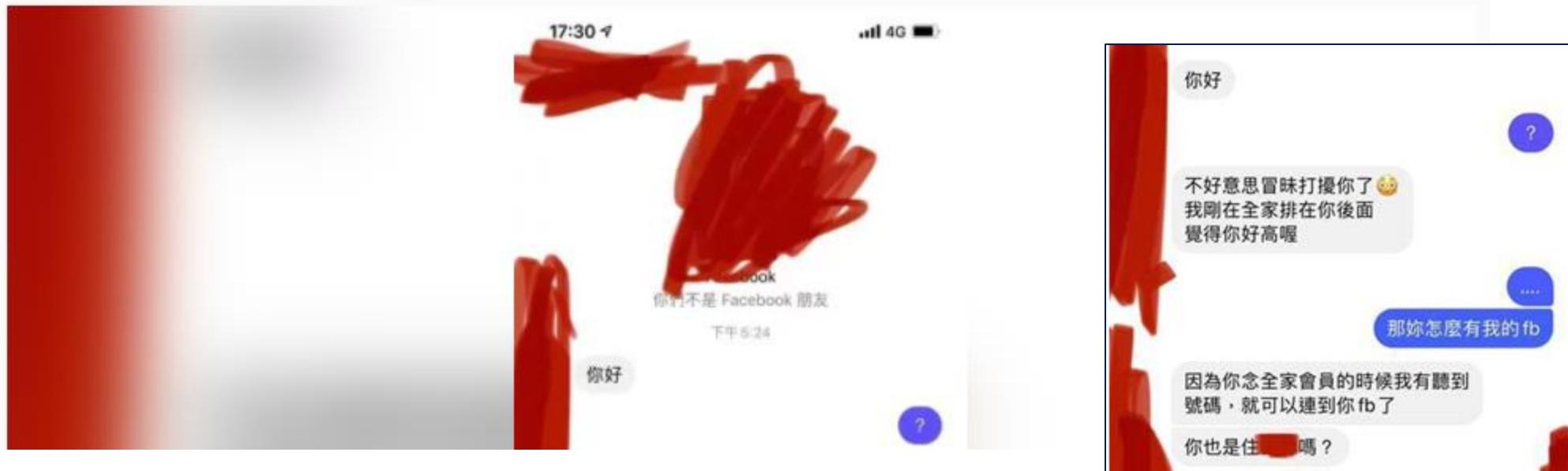
- 報會員電話被找到FB

他去超商結帳報電話累積點數 回家收到陌生男「恐怖訊息」

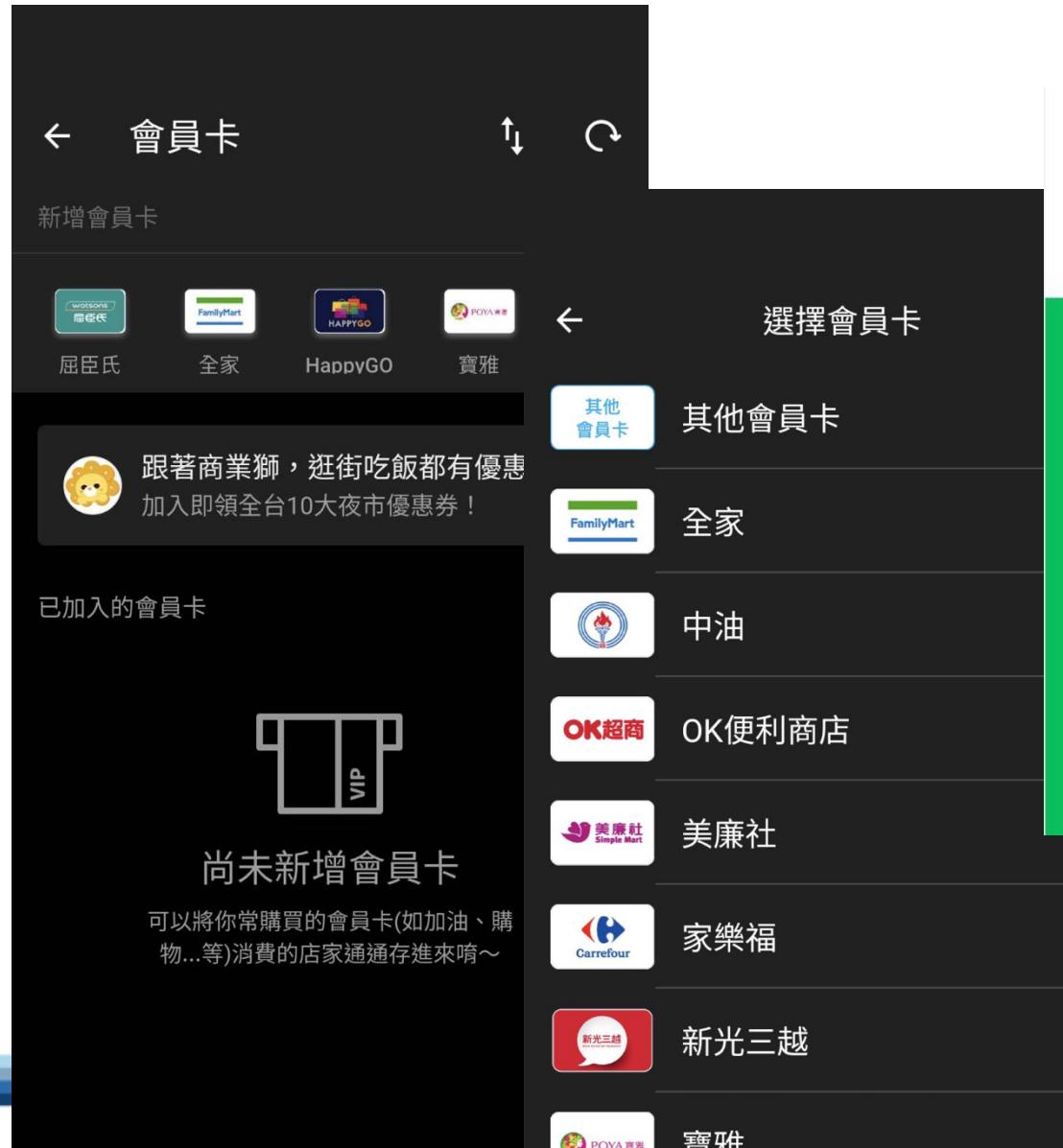
那身分證呢？

2020-12-14 11:53 聯合新聞網 / 綜合報導

+ 超商



# 手機APP-會員卡功能



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



AA

119





# 電影賞析-原本以為只是手機掉了

---

<https://www.youtube.com/watch?v=kbmnr3JzU0Pk>

<https://www.youtube.com/watch?v=U5KkTCYR-ls>



# 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。



# 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

▲ 論 6.1 萬 按讚加入iThome粉絲團

▲ 論 549 分享

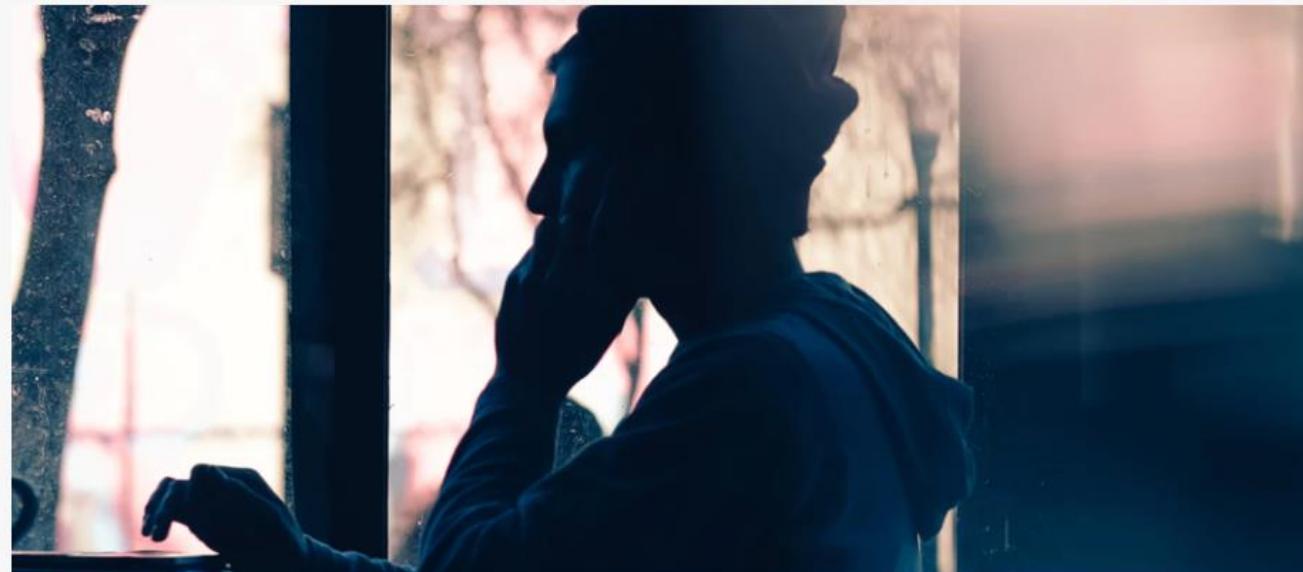


Photo by Hannah Wei on Unsplash

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



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/>



資訊局稱個資項目僅預列  
局處依實際業務需要使用

## 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. 大稻埕戲臺
- 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、出入證許可證、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種族或血緣來源(例如：原住民身分)。



# 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、...



# FACEBOOK-隱私設定檢查

- 帳號
  - 設定和隱私
    - 隱私設定檢查

The screenshot shows the Facebook Privacy Checkup interface. At the top, there's a search bar with '搜尋 Facebook' and several navigation icons. On the right, there's a user profile icon with a red notification badge containing the number '7'. Below the header, the main content area is titled '隱私設定檢查' (Privacy Settings Checkup) with the sub-instruction: 'We'll guide you through some settings so you can make the right choices for your account. 想先從哪個主題開始呢?' (We'll guide you through some settings so you can make the right choices for your account. Which theme would you like to start with?). There are six cards arranged in two rows of three, each representing a different privacy topic:

- 第一行左側：你分享內容的對象 (Today)
- 第一行右側：其他人可以在 Facebook 上找到你的方式 (Today)
- 第二行左側：你在 Facebook 上的資料設定 (Today)
- 第二行中間：如何保障帳號安全 (Today)
- 第二行右側：你的 Facebook 廣告偏好 (Today)

At the bottom left, a note says: 'You can check more privacy settings on Facebook in 設定' (You can check more privacy settings on Facebook in Settings). On the right side, there's a sidebar with a blurred profile picture at the top, followed by a button labeled '查看所有個人檔案' (View all personal files). Below that are five links with icons:

- 設定和隱私 (Settings and Privacy)
- 協助和支持 (Help and Support)
- 顯示方式和無障礙環境 (Display and accessibility)
- 提供意見回饋 (Provide feedback)
- 登出 (Logout)

At the very bottom right, there's a small circular logo for 'PRADA' (PRADA) and the text '隐私政策 · 服務條款 · 廣告 · Ad Choices · Cookie · 更多 · Meta © 2025'.

# 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

安全性  
協助您確保帳戶安全的設定和建議

登入 Google

上次變更時間：2018年6月12日

密碼

使用您的手機登入帳戶

兩步驟驗證

您的第三方連結項目

Clash of Clans  
可以存取下列服務：Google Drive、Google Play

移除存取權

CookieRun: Tower of Adventures  
可以存取下列服務：Google Drive、Google Play

移除存取權



安全檢查  
您有安全性提示

您的裝置  
建議採取 2 項行動

近期的安全性活動  
過去 28 天沒有任何活動

登入和救援選項  
兩步驟驗證已啟用

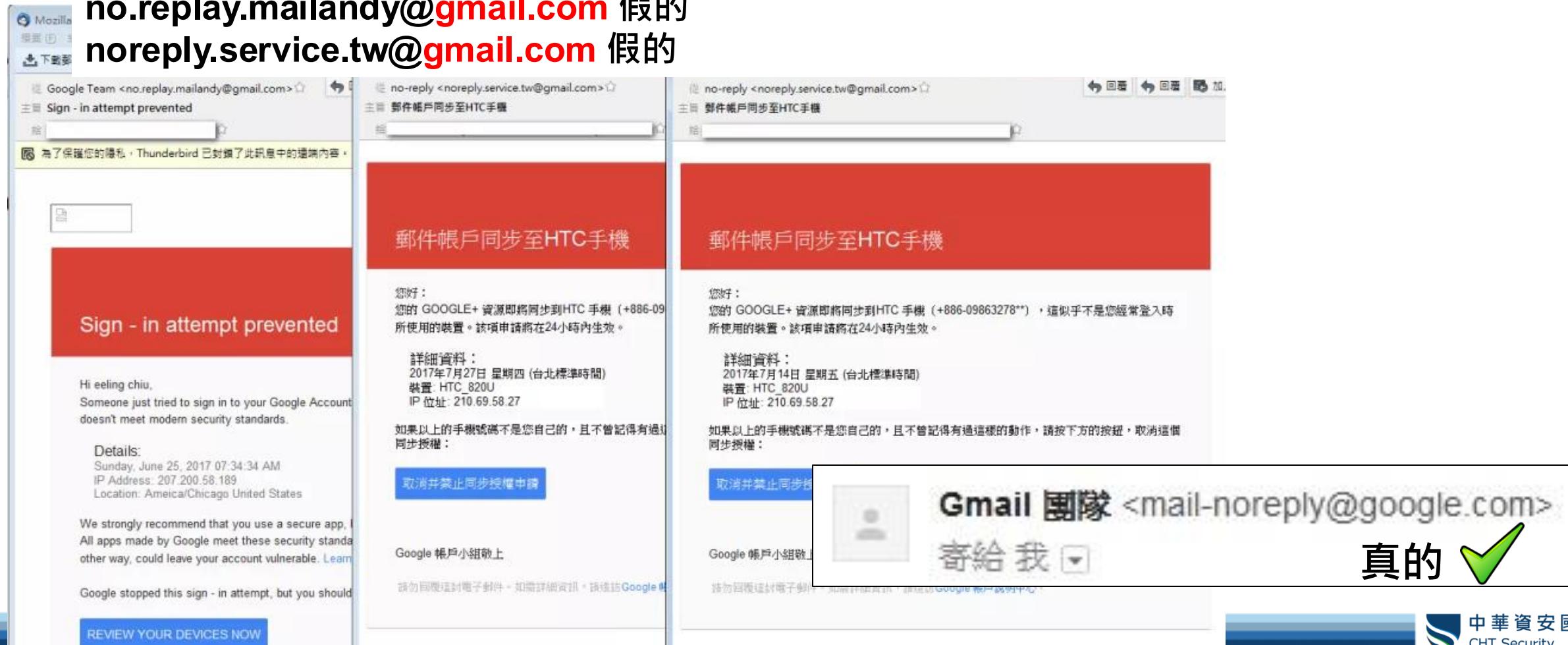
您的第三方連結項目  
1 個應用程式或服務有權存取您 Google 帳戶中的部分資料

你已儲存的密碼  
14 個網站和應用程式的密碼

# 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.reply.mailandy@gmail.com** 假的  
**noreply.service.tw@gmail.com** 假的



The image shows three side-by-side screenshots of email messages. The first message is from 'Google Team <no.reply.mailandy@gmail.com>' with the subject 'Sign - in attempt prevented'. It contains a red banner with 'Sign - in attempt prevented' and details about a failed sign-in attempt by someone from America/Chicago United States on June 25, 2017. The second message is from 'no-reply <noreply.service.tw@gmail.com>' with the subject '郵件帳戶同步至HTC手機'. It has a red banner with '郵件帳戶同步至HTC手機' and details about account synchronization to an HTC 820U device. The third message is also from 'no-reply <noreply.service.tw@gmail.com>' with the same subject. It has a red banner with '郵件帳戶同步至HTC手機' and similar synchronization details. At the bottom right, there is a large green checkmark icon with the text '真的'.

Mozilla 標題 下載 Mozilla 標題 下載 Mozilla 標題 下載

Google Team <no.reply.mailandy@gmail.com>

主題: Sign - in attempt prevented

为了保護您的隱私，Thunderbird 已封鎖了此訊息中的遠端內容。

Sign - in attempt prevented

Hi eeling chiu,  
Someone just tried to sign in to your Google Account doesn't meet modern security standards.

Details:  
Sunday, June 25, 2017 07:34:34 AM  
IP Address: 207.200.58.189  
Location: America/Chicago United States

We strongly recommend that you use a secure app. All apps made by Google meet these security standards other way, could leave your account vulnerable. Learn more

Google stopped this sign - in attempt, but you should

REVIEW YOUR DEVICES NOW

no-reply <noreply.service.tw@gmail.com>

主題: 郵件帳戶同步至HTC手機

郵件帳戶同步至HTC手機

您好：  
您的 GOOGLE+ 資源即將同步到 HTC 手機 (+886-09863278\*\*)，這似乎不是您經常登入時所使用的裝置。該項申請將在24小時內生效。

詳細資料：  
2017年7月27日 星期四 (台北標準時間)  
裝置: HTC\_820U  
IP 位址: 210.69.58.27

如果以上的手機號碼不是您自己的，且不曾記得有過這同步授權：

取消並禁止同步授權申請

Google 帳戶小組啟上

請勿回覆這封電子郵件。如需詳細資訊，請造訪 Google 帳戶小組。

no-reply <noreply.service.tw@gmail.com>

主題: 郵件帳戶同步至HTC手機

郵件帳戶同步至HTC手機

您好：  
您的 GOOGLE+ 資源即將同步到 HTC 手機 (+886-09863278\*\*)，這似乎不是您經常登入時所使用的裝置。該項申請將在24小時內生效。

詳細資料：  
2017年7月14日 星期五 (台北標準時間)  
裝置: HTC\_820U  
IP 位址: 210.69.58.27

如果以上的手機號碼不是您自己的，且不曾記得有過這樣的動作，請按下方的按鈕，取消這個同步授權：

取消並禁止同步授權

Gmail 團隊 <mail-noreply@google.com>

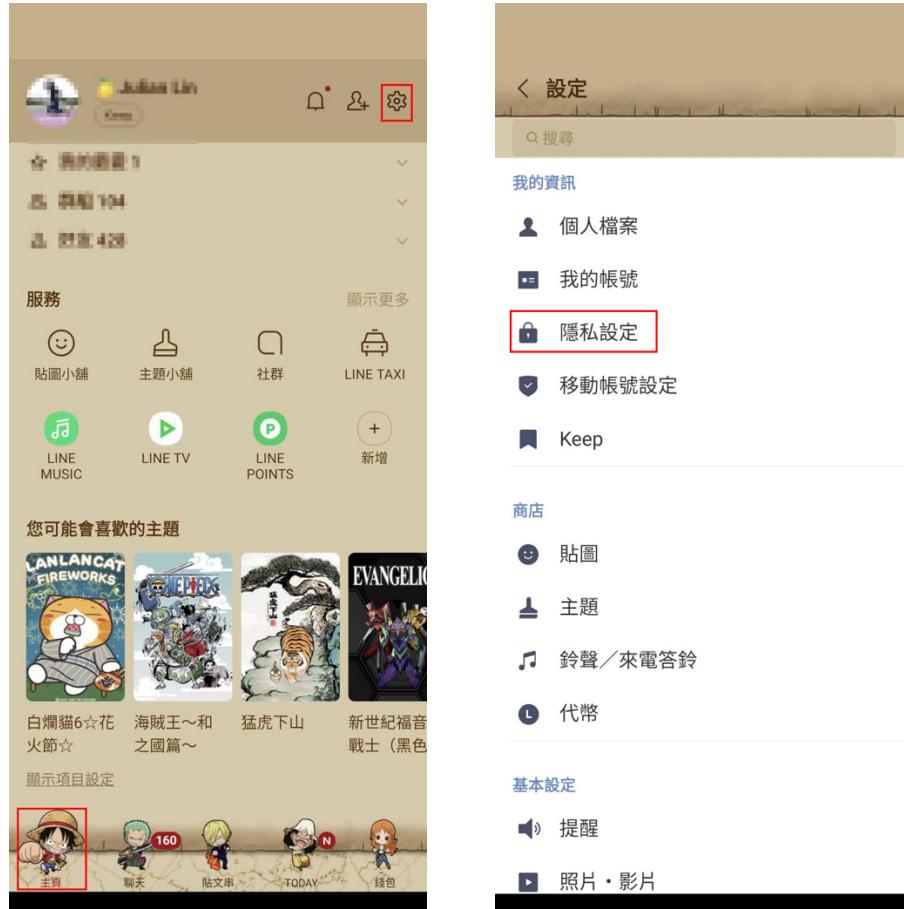
寄給我

真的 

中華資安國際 CHT Security

# LINE 安全設定

## • Letter Sealing 設定位置



## • 確認是否開啟



## 其他設定

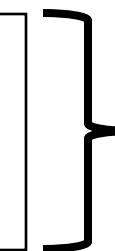
# LINE 安全設定

## • 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。

# 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**

**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。

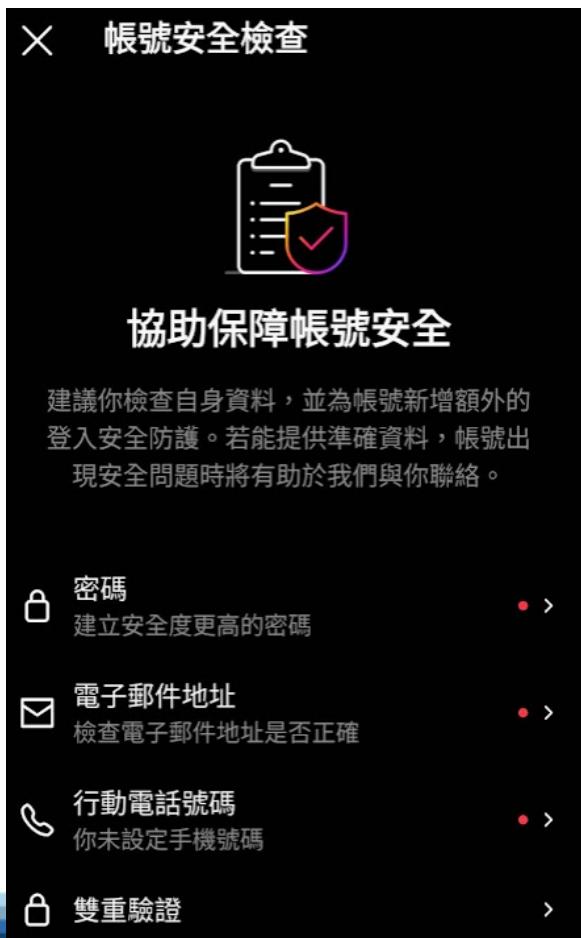
**使用密碼登入**   
若您已啟用生物辨識登入，建議可關閉此設定，以便您管理登入安全性。關閉此設定後，仍可使用其他方式登入。

**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

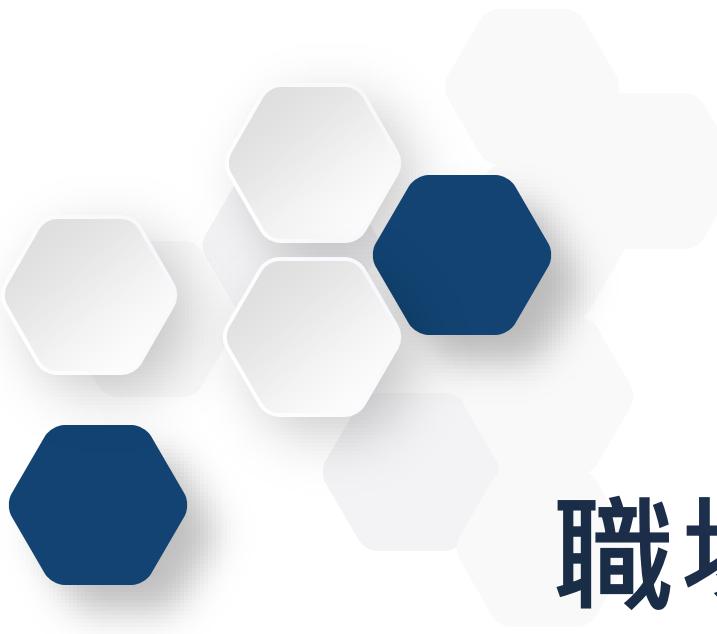


- 登入警告



- 最近的電子郵件





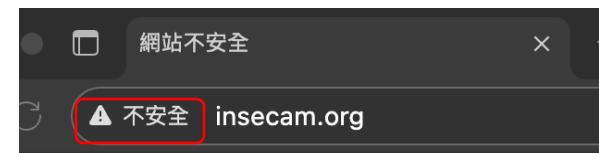
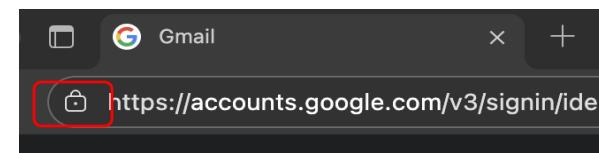
# 職場與日常生活的資安管理

---



# 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



你的連線不是私人連線

攻擊者可能會試圖從 [www.hchst.gov.tw](http://www.hchst.gov.tw) 篫取你的資訊 (例如密碼、郵件或信用卡資料)。  
[瞭解詳情](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

## HTTP vs HTTPS



# 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-tw.yv.net/tw>

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

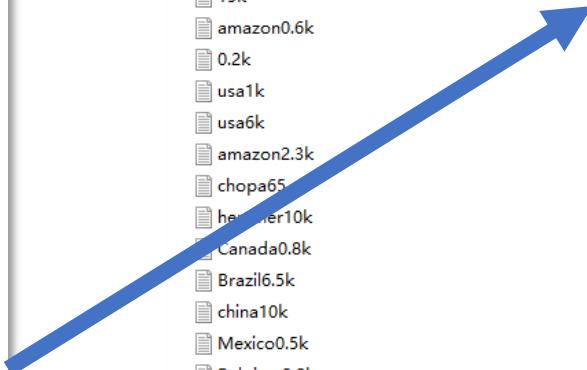
<https://mofy-gov.net/tw>

# 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 <sup>[4]</sup>	2012 <sup>[5]</sup>	2013 <sup>[6]</sup>	2014 <sup>[7]</sup>	2015 <sup>[8]</sup>	2016 <sup>[3]</sup>	2017 <sup>[9]</sup>	2018 <sup>[10]</sup>
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 <sup>[a]</sup>	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 <sup>[a]</sup>	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



GERMAN123	germani
abas1	HiT 101%
golchin(@Cyber_Cracking)	pastorkye (@Cyber_Cracking)
15k	Spain0.1k
amazon0.6k	8.5k
0.2k	10k
usa1k	Germany1k
usa6k	4k
amazon2.3k	orakel4k
chopa65	chopa50
hacker10k	Italy2.5k
Canada0.8k	EU5k
Brazil6.5k	Turkey16k
china10k	England1k
Mexico0.5k	SaudiArabia12.5k
Belgium2.8k	France3k
ovh1k	99999999
Pass SUPERGOLD1(1)	4444444444
5555555555555	AllSmallPass
@pv_hesam_bot(80)	ChinaPassList
admin_password	china
FranceBelgiumSwitzerlandpass	#1
22	33
—	—

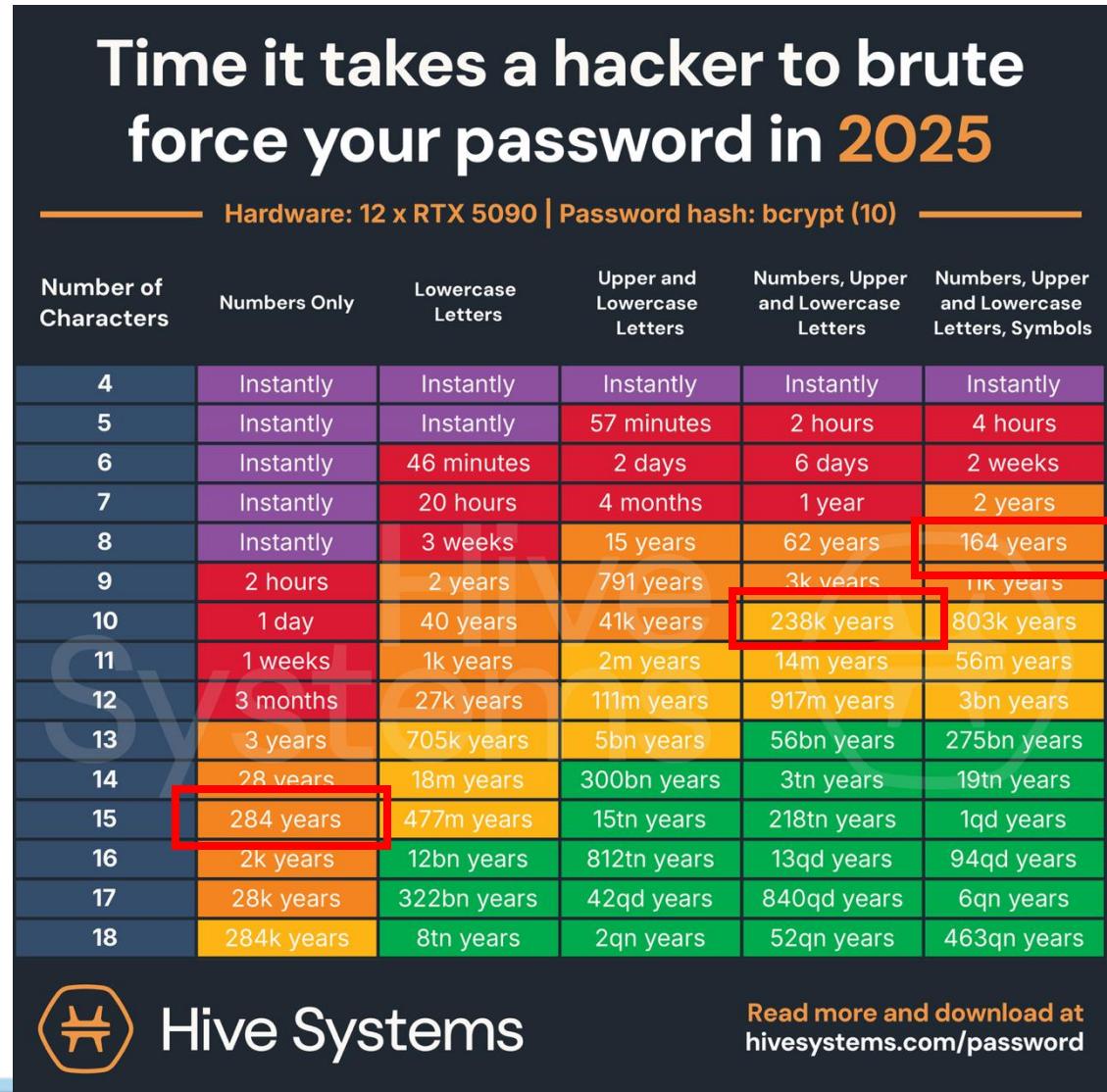
左邊清單只是駭客眾多字典檔的冰山一角

# 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

# 密碼更在意的是-長度



1 5 個純數字 > 8個字元符合複雜度

# 開啟多因子認證，強化安全性

14:09



Microsoft Authenticator 4+

Microsoft Corporation

在「生產力工具」類中排名第 13

★★★★★ 4.8 • 1.1萬 則評分

免費

## Google Authenticator

Google LLC

3.7★

59.7 萬則評論

1億+

次下載

3+

3 歲以上



安裝在更多裝置上

分享

≡ Google Authenticator



搜尋...

mdr-cttsecurity.com jinchtsecurity.com

409 544



FortiRadius: jinchtsecurity.com@FortiRadi...

423 077



CHTS-後端名: 雷神DMS-jinchtsecurity.com

749 346



CrowdStrike: jinchtsecurity.com

318 282



# 多因子認證是甚麼？

身分證字號

使用者代號

使用者密碼

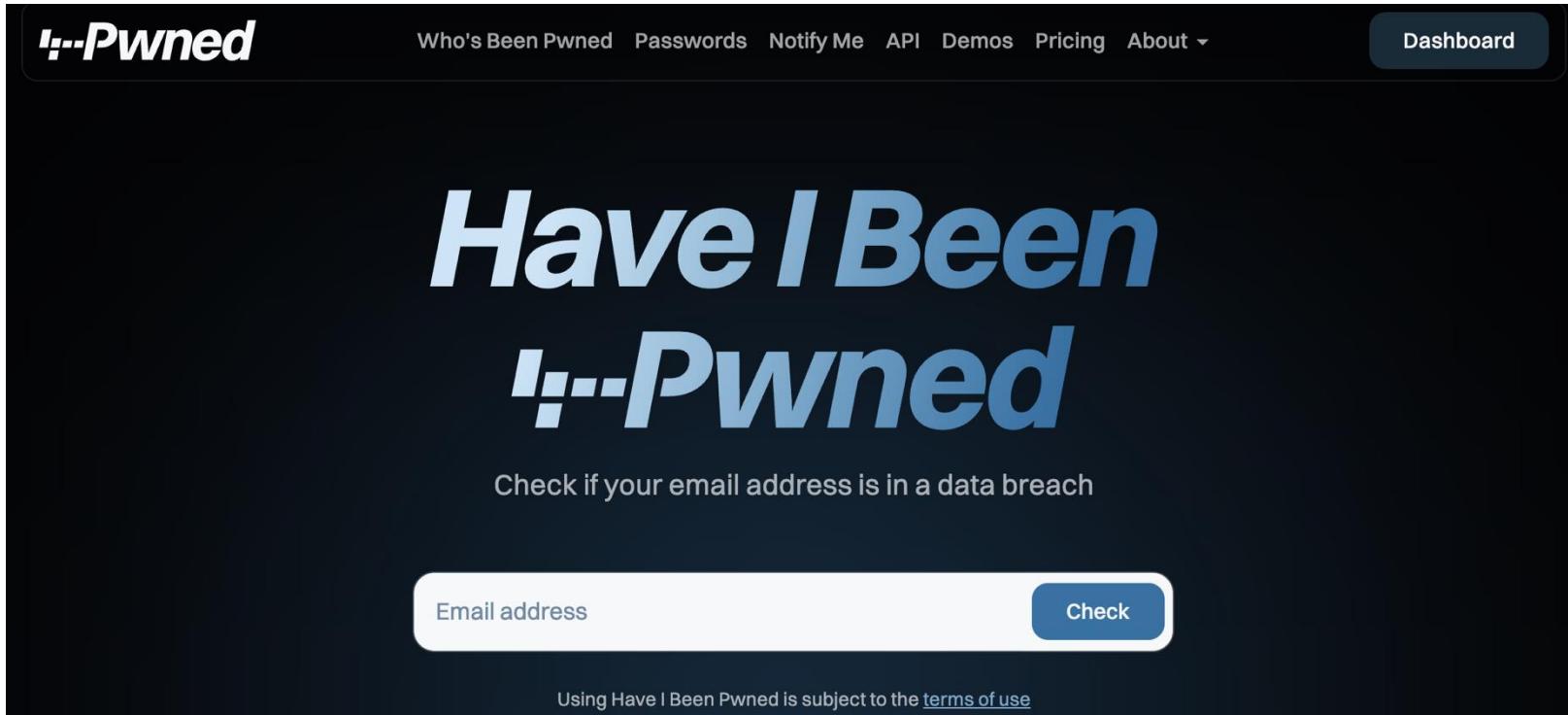
驗證碼

登入網銀



# 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/>



The screenshot shows the homepage of the Have I Been Pwned website. The page has a dark background with large, light blue text that reads "Have I Been Pwned". Below the main title, there is a subtitle "Check if your email address is in a data breach". A white input field labeled "Email address" is centered at the bottom, with a blue "Check" button to its right. At the very bottom of the page, there is a small note: "Using Have I Been Pwned is subject to the [terms of use](#)".



# 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

# 課後問券



**Thank you.**

