

資安風險與

個人資料保護案例研析

# 報告大綱

個資現況案例

個資外洩風險

個資相關法條異動

個資外洩防護方案

# 個資現況案例

---

# DBIR報告

- 68%人為因素
- 32%勒索病毒
- 28%設定錯誤
- 15%第三方影響

verizon  
business

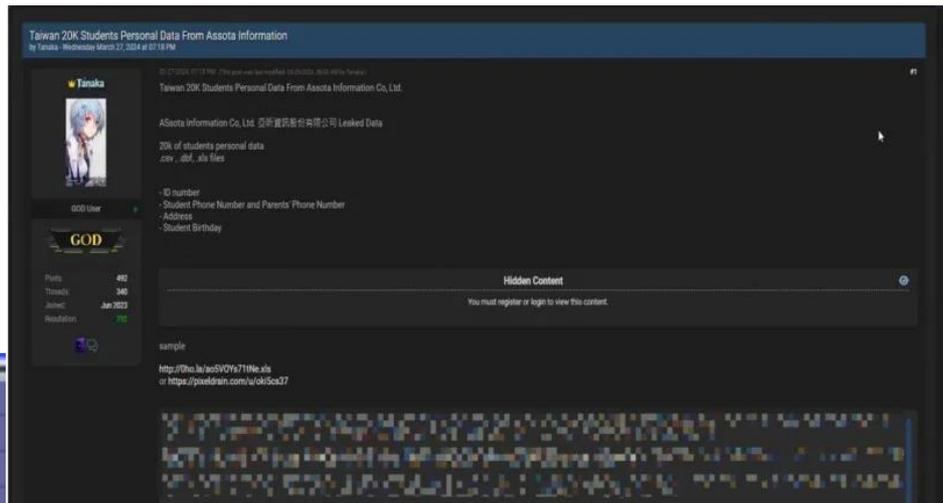
2024 Data Breach  
Investigations Report



Figure 3. Select key enumerations in breaches

# 弱密碼、漏洞

校務系統遭「駭」！  
7所學校學生個資外洩



**駭客** 學生個資遭駭客散布

- 取得個資
- 勒索贖款
- 地址多分布在中、彰、投
- 1988、1989年出生者
- 家長姓名、電話

**外洩個資多達2萬筆**

韓國綜合 8.29 2754.92

7所高中校務系統遭駭 多達2萬筆個資外洩

# 攻擊路徑

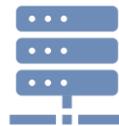


駭客利用  
IP:191.185.XX.114  
(巴西)於112年11月  
初對第一間學校發  
起攻擊。



利用前述方式  
於11月底取得  
○○公司使用  
高權限帳密。

- 1.弱密碼=>(暴力破解)
- 2.系統漏洞=>(上傳惡意程式)
- 3.高權限帳號、明文密碼=>(擴展)



於112年11  
月至113年3  
月初對使用  
相同型號系  
統發起攻擊，  
取得其上完  
整個資。

# 密碼噴射攻擊

微軟遭俄羅斯駭客竊取程式碼、存取內部系統

## Microsoft says state-sponsored Russian hacking group accessed email accounts of senior leaders



By Catherine Thorbecke, CNN

2 minute read · Updated 9:52 PM EST, Fri January 19, 2024



密碼噴射攻擊：利用少量強度較弱的密碼去配對多個帳號來攻破內部系統。

(CNN) — A Russian hacking group gained access to some email accounts of Microsoft senior leaders, the software giant disclosed in a regulatory filing Friday afternoon.

“The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access,” the Microsoft Security Response Center said in a [blog post](#). “Microsoft has identified the threat actor as [Midnight Blizzard](#), the Russian state-sponsored actor also known as Nobelium.”

Nobelium, notably, is the same group responsible [for the infamous SolarWinds breach](#) back in 2020.

Hackers were able to gain access to “a very small percentage of Microsoft corporate email accounts,” the blog post added, including accounts belonging to members of its senior leadership team and employees in its cybersecurity and legal departments.

The company said that hackers were able to exfiltrate some emails and attached documents, though the preliminary investigation indicates that the attackers seemed to be seeking information related to Midnight Blizzard itself. That mirrors what the same group did when it used tampered software made by SolarWinds to infiltrate US agencies in 2020 — and then [sought to track how the US government was responding](#) to its intrusions.

Microsoft said it is in the process of notifying employees whose email was accessed. There is currently no evidence that the hackers had any access to customer environments or AI systems, Microsoft said.

The attack began in late November 2023, the company said, and hackers gained an initial foothold using a so-called [“password spray attack.”](#) Password spraying refers to the attempt to access a large number of accounts using commonly known passwords.

# => 變臉詐騙

透過假冒成內部員工、高階主管或外部合作夥伴來欺騙員工進行電匯付款或洩漏機密資料。

## 俄駭客再出手 微軟信箱又被駭



工商時報 余葳芸

2024年6月28日



微軟 (Microsoft) 27日向客戶發布通知，表示俄羅斯駭客組織午夜暴雪 (Midnight Blizzard) 竊盜其電子郵件資料。



微軟發言人以電子郵件聲明中表示：「本周我們將繼續向與遭受到午夜暴雪 (Midnight Blizzard) 竊取的微軟電子郵件帳戶通信的客戶發出通知。」並表示駭客正針對客戶發送商務郵件詐騙 (BEC, 變臉詐騙)，但沒有透露具體有多少客戶或電子郵件受到影響。



微軟在今年1月首次披露相關入侵事件，當時為公司郵件系統及員工信件遭入侵。微軟表示，駭客的目標是網路安全研究人員，而該部門正持續調查俄羅斯駭客組織行為。

微軟表示，它還在與客戶分享受損的電子郵件，但沒有透露有多少客戶受到影響，也沒有透露有多少電子郵件可能被盜。微軟發言人表示：「隨著調查持續進行，我們會與客戶分享資訊。」



# 撞庫攻擊

利用其他漏洞竊取或地下網站購買個使用者帳號密碼，不斷嘗試登入用戶的其他網站或服務。



# 社交工程

教會 ... ×

贊助 · 🌐

❤️ 歡迎有愛心的你/妳一起為弱勢團體 身心障礙者 遲緩兒代禱…… 顯示更多



**為孩童代禱**  
**為戰爭代禱**  
**為傷患代禱**

詳情內洽 薪酬內洽  
年滿20 不限地區

表單 [立即申請](#)

👍 33 9則留言 1次分享

5:43 5G 90%

台灣基督長老教會

facebook 登入

10 按讚數 · 17 位追蹤者

追蹤 ...

貼文 關於 相片 提及

詳細資料

- 粉絲專頁 · 非營利組織
- ★ 尚無評分 (0 則評論)

粉絲專頁資訊透明度 [查看全部](#)

Facebook  
將顯示資訊，讓你更瞭解這個粉絲專頁的目的。

建立 - [redacted] 教會  
6月18日

管理員資料  
這個粉絲專頁可能有多位管理員，且他們可能有權以粉絲專頁的身分發佈貼文、留言或傳送訊息。

此粉絲專頁目前並未刊登廣告。

[顯示「關於」的完整內容](#)



**錄製聖經  
經文章節**

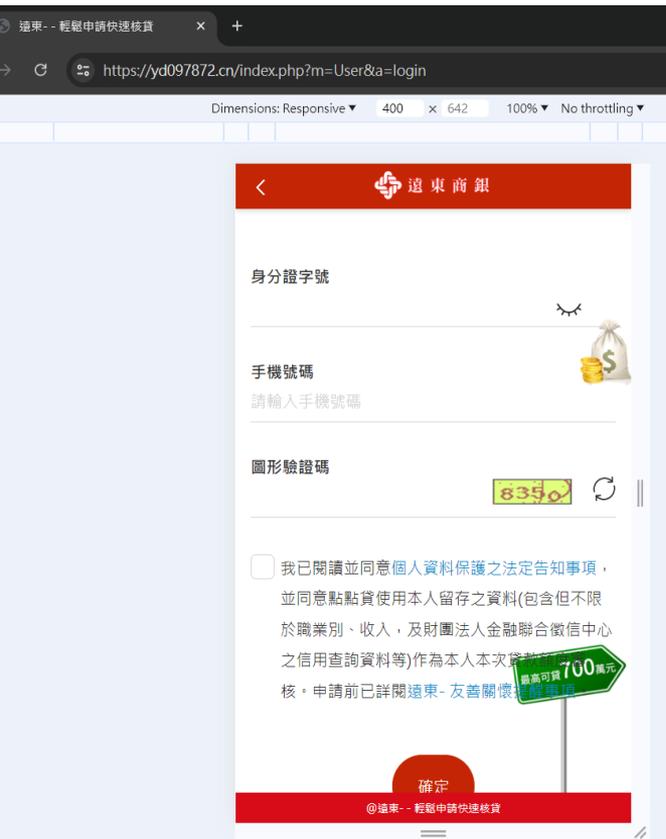
年滿二十 全台召募  
線上作業 研讀詳談

**誠徵聖經有聲書複讀員**

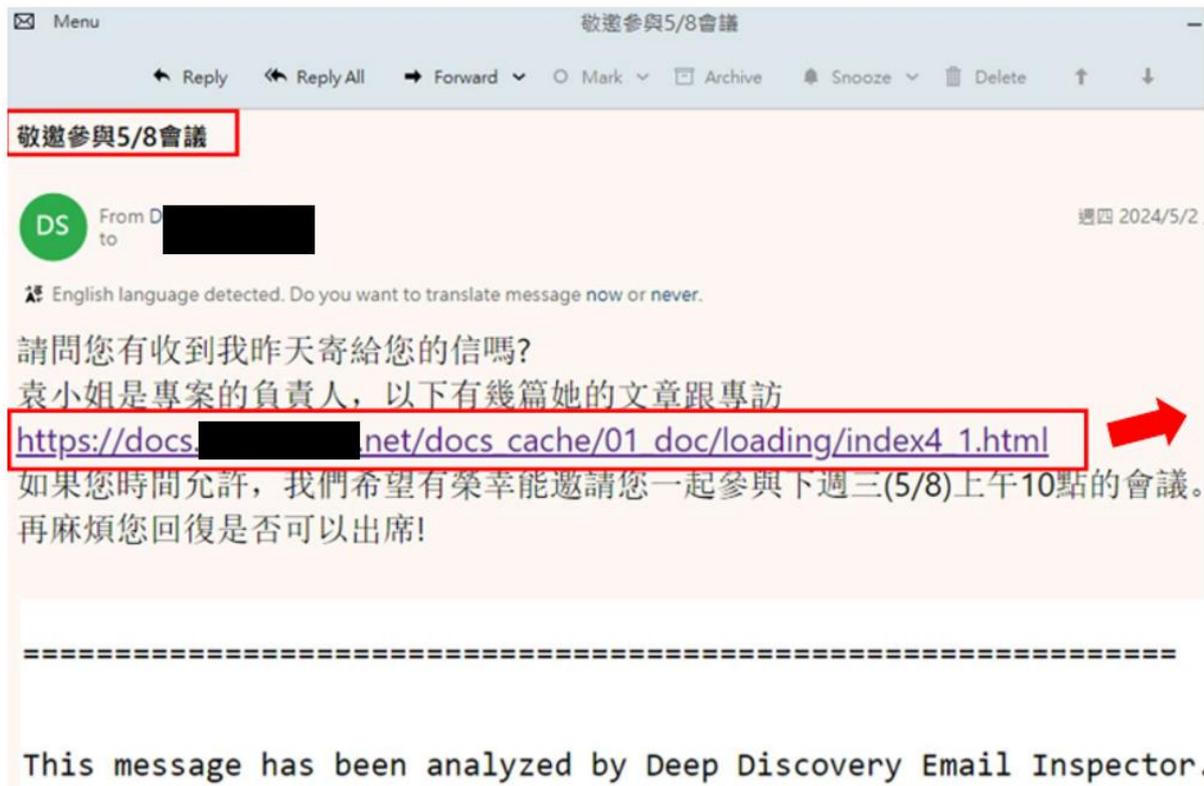
- 誠徵聖經有聲書複讀員
- 只需要照著聖經朗誦
- 語速自然 真誠朗讀 歡迎試試~
- 可自行安排時間...

# 社交郵件

# 偽冒網址 偷個資



# 社交郵件





# 多重認證轟炸

X 用戶 Parth Patel 也分享了他近期成為攻擊目標的經歷

 **Parth** ✓ · 2024年3月24日  
@parth220\_ · 跟隨  
回覆 @parth220\_

The attackers made a led high effort focused attack on me, using OSINT data from People Data Labs and caller ID spoofing.

First, around 6:36pm yesterday all of my Apple devices started blowing up with Reset Password notifications.

Because these are Apple system level alerts,...

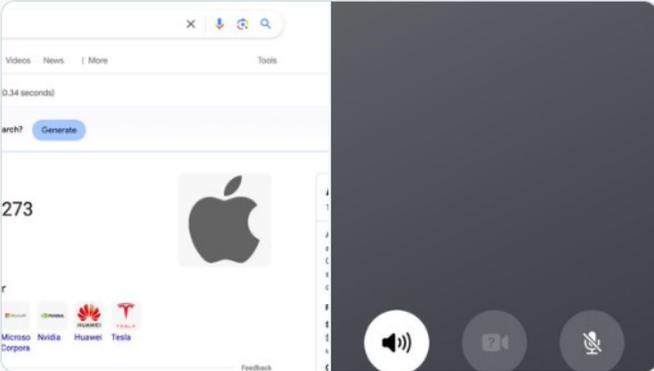


 **Parth** ✓  
@parth220\_ · 跟隨

About 15 minutes later, they call me on my number, using Caller ID spoofing of the official Apple Support phone line (1 (800) 275-2273).

They really emphasized this detail to win trust from the victim.

I was obviously still on guard, so I asked them to validate a ton of... [顯示更多](#)



上午1:28 · 2024年3月24日

# 多重認證轟炸

iPhone 收到 Apple ID 驗證通知要小心 | 昨日 (4月11日) 大量 iPhone 用家，突然收到 Apple ID 驗證通知，如有多個 Apple ID 帳戶，更一次過同時彈出驗證要求，甚至出現陌生的 Apple ID 驗證，令一眾 iPhone 用家擔心手機安全問題。事後 Apple 亦緊急向全球 92 個國家用家，發出緊急威脅郵件通知，警告有機會成為「傭兵間諜軟體」攻擊對象。

外媒《TechChurch》指出，Apple 向 92 個國家的 iPhone 用戶發送「威脅通知」，向用家警告有機會成為傭兵間諜軟體攻擊目標。Apple 發現國家等級的黑客攻擊事件，利用 iPhone 的漏洞遠端入侵 iPhone 系統。這次的攻擊比起一般的惡意軟體攻擊複雜，估計是針對政治人物、政府官員、名人等作出攻擊。

檢測是否受駭客攻擊方法：

1. 登入 [AppleID.apple.com](https://appleid.apple.com) : 登入 Apple ID 後，頁面上出現「Threat Notification」(威脅通知)，就代表當前的 Apple ID 已受到黑客攻擊。
2. Apple 會向受影響的用家，透過郵件和 iMessage 通知當前 Apple ID 處於不安全狀態，而且會附上官方的詳細解決方法，可按照來保護 Apple 裝置的安全。

# 多重認證繞過

Cookie theft技術：透過竊取或從暗網上購買了用戶被盜的憑證，攻擊者只需重複輸入這些憑證即可。

Google Updates from Threat Analysis Group (TAG)

THREAT ANALYSIS GROUP

## Phishing campaign targets YouTube creators with cookie theft malware

Oct 20, 2021 · 6 min read

Share



Ashley Shen  
Threat Analysis Group

Google's Threat Analysis Group tracks actors involved in disinformation campaigns, government backed hacking, and financially motivated abuse. Since late 2019, our team has disrupted financially motivated phishing campaigns targeting YouTubers with Cookie Theft malware.

The actors behind this campaign, which we attribute to a group of hackers recruited in a Russian-speaking forum, lure their target with fake collaboration opportunities (typically a demo for anti-virus software, VPN, music players, photo editing or online games), hijack their channel, then either sell it to the highest bidder or use it to broadcast cryptocurrency scams.

In collaboration with YouTube, Gmail, Trust & Safety, CyberCrime Investigation Group and Safe Browsing teams, our protections have decreased the volume of related phishing emails on Gmail by 99.6% since May 2021. We blocked 1.6M messages to targets, displayed ~62K Safe



Microsoft

Microsoft Security

Solutions

Products

More

Start free trial

All Microsoft



July 12, 2022 · 13 min read

## From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud

Microsoft 365 Defender Research Team

Microsoft Threat Intelligence Center (MSTIC)

Share

A large-scale phishing campaign that used adversary-in-the-middle (AiTM) phishing sites stole passwords, hijacked a user's sign-in session, and skipped the authentication process even if the user had enabled multifactor authentication (MFA). The attackers then used the stolen credentials and session cookies to access affected users' mailboxes and perform follow-on [business email compromise \(BEC\)](#) campaigns against other targets. Based on our threat data, the AiTM phishing campaign attempted to target more than 10,000 organizations since September 2021.

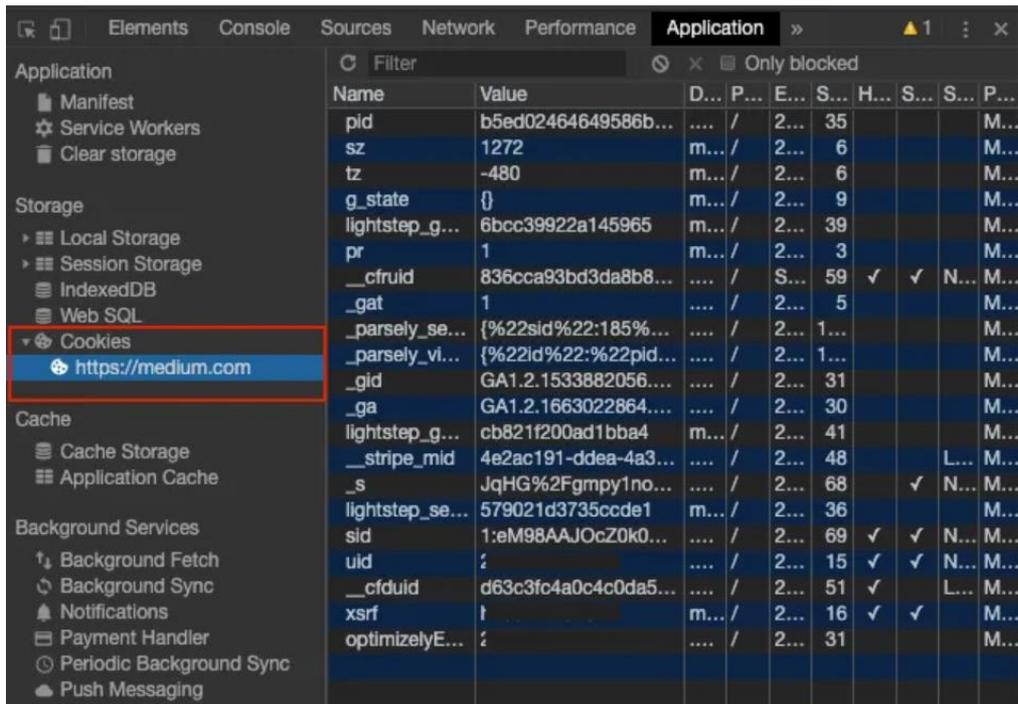
# Cookie?

小型文字檔案：

網站為了辨識使用者身分

而儲存在本地端

目的：記住使用者



The screenshot shows the Chrome DevTools Application tab with the 'Application' panel open. The 'Storage' section is expanded to show 'Cookies' for the domain 'https://medium.com'. The cookies are listed in a table with columns for Name, Value, Domain, Path, Expires, Size, HttpOnly, Secure, and SameSite.

Name	Value	D...	P...	E...	S...	H...	S...	S...	P...
pid	b5ed02464649586b...	...	/	2...	35				M...
sz	1272	m...	/	2...	6				M...
tz	-480	m...	/	2...	6				M...
g_state	{}	m...	/	2...	9				M...
lightstep_g...	6bcc39922a145965	m...	/	2...	39				M...
pr	1	m...	/	2...	3				M...
__cfuid	836cca93bd3da8b8...	...	/	S...	59	✓	✓	N...	M...
__gat	1	...	/	2...	5				M...
__parsely_se...	{%22sid%22:185%...	...	/	2...	1...				M...
__parsely_vi...	{%22id%22:%22pid...	...	/	2...	1...				M...
__gid	GA1.2.1533882056...	...	/	2...	31				M...
__ga	GA1.2.1663022864...	...	/	2...	30				M...
lightstep_g...	cb821f200ad1bba4	m...	/	2...	41				M...
__stripe_mid	4e2ac191-ddea-4a3...	...	/	2...	48			L...	M...
__s	JqHG%2Fgmpy1no...	...	/	2...	68		✓	N...	M...
lightstep_se...	579021d3735ccde1	m...	/	2...	36				M...
sid	1:eM98AAJ0cZ0k0...	...	/	2...	69	✓	✓	N...	M...
uid	;	...	/	2...	15	✓	✓	N...	M...
__cfduid	d63c3fc4a0c4c0da5...	...	/	2...	51	✓		L...	M...
xsrftoken	;	m...	/	2...	16	✓	✓		M...
optimizelyE...	;	...	/	2...	31				M...

# IOT設備配置不當

- IOT設備面臨的資安問題:
  - 1.設備管控不易，落在校園各角落。
  - 2.系統更新不易，當設備數量多時可能有疏漏。
  - 3.設定配置不當，使任何人都有存取權限。
  - 4.購買品牌不甚，造成設備有後門漏洞。





OK  
Q1  
--  
[ ]  
[ ]  
[ ]  
[ ]

Insecam



Live camera in Taipei, Taiwan, Province Of

網路摘要

組態

IPv4 組態

IPv6 組態

網路識別碼

進階

Google 雲端列印

設定

Proxy 設定

AirPrint

狀態

安全性

# 設定

## 網路設定

功能/服務名稱	目前值
驗證	
管理員密碼	關閉
PJL 安全性	停用
印表機憑證	已安裝
CA 憑證	未安裝
存取控制清單	停用
防火牆	停用

# SHARP MX-2010U

## 位址目錄

更新(R)

☐ 頁面上方

▶ 狀態

▶ 位址目錄

☐ 自訂索引

▶ 工作記憶

▶ 用戶控制

▶ 系統設定

▶ 網路設定

▶ 應用程式設定

▶ E-mail 警示及狀態

☐ 儲存備份

☐ 裝置複製

▶ 機密保護設定

☐ 自訂連接

檢索:

全部名單 ▾

顯示項目:

10 ▾

位址名稱 ▲ ▾	型式 ▲ ▾	位址 ▲ ▾	No. ▲ ▾
<input type="checkbox"/> 許 [redacted]	桌面	192.168.1.134	1
<input type="checkbox"/> 表演藝術科主任	桌面	192.168.1.144	2
<input type="checkbox"/> 林 [redacted]	桌面	192.168.1.111	3
<input type="checkbox"/> 實習主任	FTP	192.168.1.172	4
<input type="checkbox"/> 輔導室	桌面	192.168.1.14	6
<input type="checkbox"/> 吳 [redacted]	桌面	192.168.1.96	7
<input type="checkbox"/> 實習組	桌面	192.168.1.155	10
<input type="checkbox"/> Micky	桌面	192.168.1.84	11
<input type="checkbox"/> user-FOLDER	桌面	192.168.1.197	12
<input type="checkbox"/> 運 [redacted]	桌面	192.168.1.108	14

全部位址: 16

先前的(M) 1 / 2 下一個(N)

選擇全部(S) 選擇解除(Z)

# 個資管理不當

- 校園公告專區，可能因業務需要須公布學生個人資訊。
- 建議以去識別化操作，防止身分遭他人識別並加以利用。
- 個資法中有規範公務機關因故意或過失洩漏個資之相關罰則，須注意單位是否有違規事項。

site:edu.tw 身分證字號 陳 ext:xls OR xlsx

全部 新聞 圖片 地圖 影片 更多

共約 1,310 項結果，這是第 5 頁 (搜尋時間：0.26 秒)

<https://www.tsgn.ndmctsgn.edu.tw> > web > file\_up > XLS  
**未領 - 三軍總醫院**  
12, 11, 111, 0408-, 01, 4月8日, 12:00, 急診, 民眾, 健保卡(陳...), ... 43, 50, 111, 0422-, 02, 4月22日, 10:45, 門診, 民眾, 身分證(陳...).

<http://ptac.npust.edu.tw> > ezfiles > attach > pta\_14... > PDF  
**班別**  
身分證字號(後4碼). 錄取. 基礎班. 003. 黃○楠. T12... 1835. 錄取01. 基礎班. 112. 潘○輝. T12... 2770. 錄取02. 基礎班. 088. 陳○中. A12... 5269.

<https://www.npu.edu.tw> > df\_ufiles > 中華民國11... > XLS  
**學校名單 - 國立澎湖科技大學**  
12, NO, 職稱, 姓名, 性別, 單位, 職稱, 身分證字號, 備註. 13, 1, 領隊, 郭校長, 男, 教育學院, 校長 ... 17, 5, 隊員1, 陳一二, 女, 國貿系, 助理教授, E200000004.

# 個資管理不當

學術倫理相關網相及手冊，請轉知所屬系所學生，謝謝。

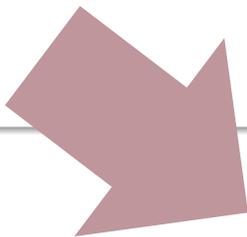
網址：[https://\[redacted\].edu.tw](https://[redacted].edu.tw)

登入身份請選「必修學生」。

並選擇學校。

帳號為學號，密碼預設學號末 5 碼。

若不確定身分，請選「[查詢身分](#)」。



[http://www.\[redacted\].tw](http://www.[redacted].tw) > portaldoc > news > XLS

## 110-1助學生(第一批)

1, 序號, 學號, 發送簡訊有問題. 2, 1, E10944071. 3, 2, E10761001. 4, 3, B10836060. 5, 4, M10912002. 6, 5, E10764011. 7, 6, B11058088. 8, 7, E10861019.

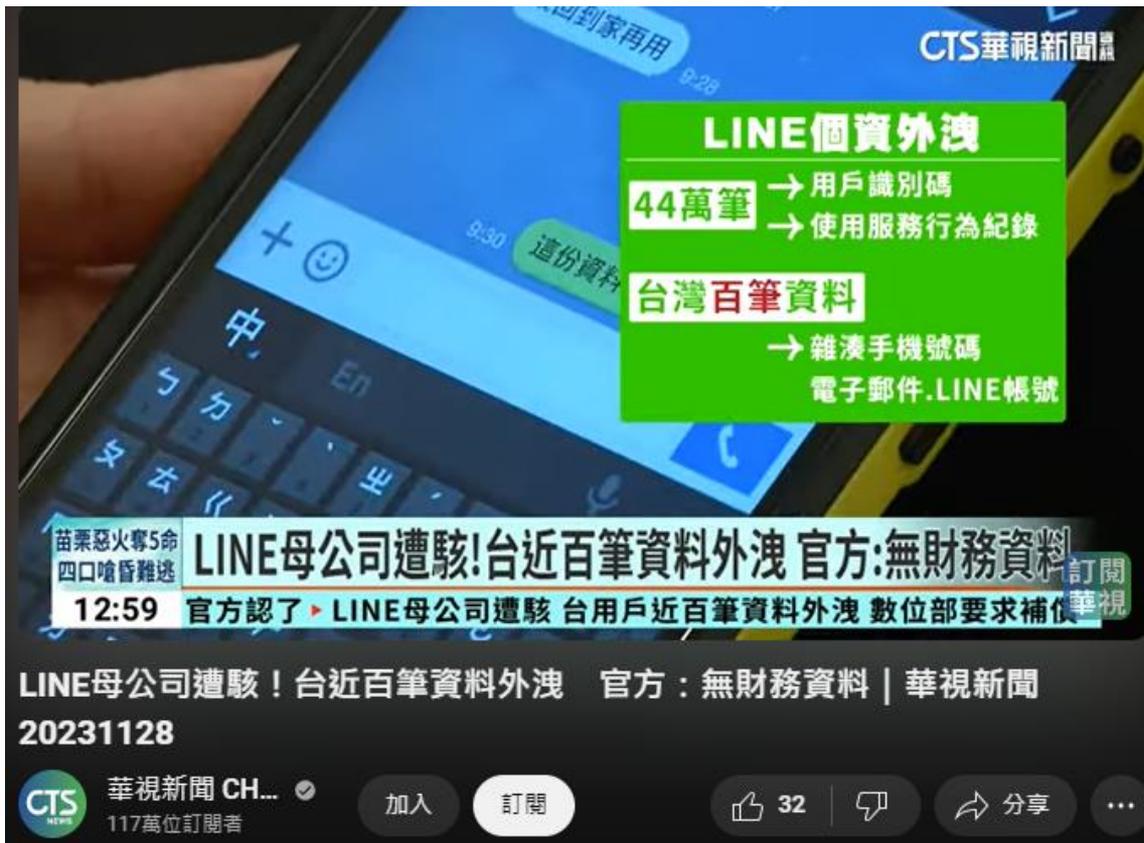
[http://www.\[redacted\].tw](http://www.[redacted].tw) > portaldoc > news > XLS

## Office 2003 XLS Test Document

1, 學號, 姓名, 身分證字號, 金額, 付款方式, 銀行代號, 銀行帳號, 銀行分行. 2, (範例). 3, B10912356, 廖小美, A123456789, 6000, 郵局, 7000021-, 01012345678910- ...

<http://osa.npust.edu.tw> > ezfiles > lma > XLS

# 第三方影響



Line母公司LY Corporation指出他們偵測到未經授權的第三方於10月9日存取該公司系統，而有可能導致使用者、業務合作夥伴、員工等人士的資訊遭到洩露。

# 個資外洩風險

---

# 常見風險

1. 財損：信用卡盜刷、詐騙、勒索、罰款
2. 個資遭濫用、利用
3. 隱私侵害
4. 信譽受損
5. 影響擴及周邊



# 詐騙

## 假冒不同單位名義



### ✓ 網路店家

接到買家電話，聲稱「購物訂單錯誤」，要求解除分期付款，即為電話詐騙！



### ✓ 公家機關

檢警、法院等公家機關不會主動打電話給民眾，要求民眾匯款或監管帳戶！



### ✓ 電信業者

接到假冒電信公司語音催繳電話費，利用「已進入司法程序」、「財產將被查封」、「24小時內停機」製造緊張氣氛，應向電信公司求證，以免受騙！

## 假冒不同情境詐騙



### ✓ 求職陷阱

求職應聘期間，請勿提供存摺正本、提款卡、密碼或代人提款，以免淪為詐欺集團人頭帳戶！



### ✓ 網戀詐騙

網路交友時，若遇對方「自稱外籍人士」、「從事特定職業」、並且「打探薪資收入」或「要求金援」，請提高警覺！



### ✓ 假投資

「假投資、真詐財」，歹徒藉由話術宣稱「利用投資○○管道，高倍快速獲利、穩賺不賠」，可能都是詐騙，請小心查證！

# 個資相關法條異動

---

# 專屬監管機構

## 第 1-1 條

- 1 本法之主管機關為個人資料保護委員會。
  - 2 自個人資料保護委員會成立之日起，本法所列屬中央目的事業主管機關、直轄市、縣（市）政府及第五十三條、第五十五條所列機關之權責事項，由該會管轄。
- **舊：並無設置單一專責主管機關**，個資法之執行係依據非公務機關之事業性質，由各中央目的事業主管機關或各縣市政府分散式管理，並由國家發展委員會擔任個資法解釋機關。
  - **新：第1條之1條增訂「個人資料保護委員會」**作為未來個資法下之專責主管機關，自其成立之日起，整合目前分屬中央目的事業主管機關、地方政府及國家發展委員會的權責。

## 罰則調高

- 舊：規定非公務機關違反個資法先由行政機關命限期改正、屆期未改正者，得按次處新臺幣（下同）2萬元至20萬元之罰鍰。
- 新：修正個資法第48條**非公務機關**違反安全維護義務之裁罰方式及額度，**改為逕行處罰同時命改正**，並提高罰鍰上限，處新臺幣(下同)2萬元以上200萬元以下罰鍰；情節重大者，處15萬元以上**1,500萬元以下罰鍰**。屆期未改正者，**按次處**15萬元以上1,500萬元以下罰鍰。

# 案例

本資料由 (上市公司) 2762 世界健身-KY 公司提供

序號	2	發言日期	113/06/21	發言時間	21:14:57
發言人	柯約翰	發言人職稱	董事長兼總經理	發言人電話	04-36010880
主旨	(更正格式)本公司之子公司及子公司代表人接獲 教育部裁處書乙案				
符合條款	第	26	款	事實發生日	113/06/21
說明	1. 事實發生日：113/06/21 2. 事實發生主體：代子公司申報：香港商世界健身事業有限公司 3. 發生緣由(事件說明)：本公司之子公司香港商世界健身事業有限公司，今日收到教育部6月19日發函，以子公司違反個人資料保護法第12條、第27條第1項及個人資料保護法施行細則第12條第2項規定裁處。 4. 處理過程：本公司已針對此事件進行檢討，並已全面加强資訊安全防護，未來將持續強化以確保資通安全。 5. 處分情形：子公司及子公司代表人皆受罰鍰新臺幣140萬元。 6. 是否遭裁處罰鍰：是 7. 裁罰金額(元)：新台幣 1,400,000 元 8. 預計可能損失或影響：罰鍰新臺幣140萬元。 9. 可能獲得保險理賠之金額(元)：不適用 10. 改善情形及未來因應措施：(1) 合作廠商將加強資安管控，確保資料安全。 (2) 未來將持續強化資訊安全防護以確保資通安全。 (3) 針對本次裁罰，本公司將研議行政救濟。 11. 是否前已就同一事件發布重大訊息：113/6/21 12. 其他應述明事項：子公司新台幣140萬元罰鍰，子公司代表人新台幣140萬元罰鍰。				

## 近期3家上市櫃公司因個資外洩裁罰，發布重大訊息

諾貝兒

2023年10月7日 說明本公司遭受網路駭客攻擊事件

2023年10月31日 公告本公司接獲高雄市政府裁處書罰鍰乙案  
(高雄市政府以諾貝兒寶貝違反個人資料保護法第27條規定，依同法第48條規定裁處罰鍰新臺幣15萬元整)

雄獅

2023年11月20日 說明本公司遭受駭客網路攻擊事件

2024年1月17日 公告本公司受交通部裁罰案之說明  
(依據交通部113年1月12日交授觀業字第1133000076號函所論，就雄獅112年11月20日遭受網路駭客攻擊，致發生該次資安事件，違反個人資料保護法第27條第1項。該主管機關核處200萬元。)

上海商銀

2023年11月28日 公告本公司受金管會裁罰案之說明

(公告項目：M26遭受重大損失或資安事件；說明依據金管會官方網站112年11月28日公告，上海商銀有未完善建立及未確實執行內部控制制度之情事，違反銀行法第45條之1第1項及其授權訂定之「金融控股公司及銀行業內部控制及稽核制度實施辦法」第3條、第8條第1項第2款第2目規定，核處1,000萬元。)

資料來源：臺灣證券交易所公開股市觀測站，iThome整理，2024年3月

- <https://www.ithome.com.tw/news/161667>

# 重訊標準

## 證交所規範：

113年1月18日公布的新版「**重大訊息發布應注意事項參考問答集**」第26款內容，首度**明確規範資安事件的「重大性」標準**，包括：公司的核心資通系統、官方網站或機密文件檔案資料等，遭駭客攻擊或入侵（包括遭入侵、破壞、竄改、刪除、加密、竊取、DDoS等），致無法營運或正常提供服務，**或有個資外洩的情事等**。即屬造成公司重大損害或影響。

### ●6月有7起：

#### 第一周（6月3日到6月7日）

- 走著瞧（Gogolook）說明網路資安事件。
- 華邦電子說明因合作廠商遭駭疑似資料外洩事件。
- 藍天電腦在媒體報導疑似遭駭後，說明部份網路系統受駭客攻擊。

#### 第二周（6月11日到6月14日）

- 環球晶說明發生網路資安事件，之後又兩度重訊說明復工情形。

#### 第三周（6月17日到6月21日）

- 永信藥品說明公司部分資訊系統遭受駭客攻擊。

#### 第四周（6月24日到6月28日）

- 華碩說明發生資通安全事件。
- 崑崙精密科技說明公司遭冒名通知客戶更改收款帳戶事件。

# 個資外洩防護方案

---

# 常見密碼排行

-密碼管理公司「NordPass」2023台灣常見密碼排行榜

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	admin	< 1 Second	8,430
2	123456	< 1 Second	8,035
3	a123456	< 1 Second	6,843
4	12345678	< 1 Second	3,730
5	1qaz2wsx	< 1 Second	3,542
6	123456a	< 1 Second	3,378
7	janejane123	2 Minutes	2,768
8	password	< 1 Second	2,092
9	a123456789	< 1 Second	2,057
10	abc123	< 1 Second	1,857

RANK	PASSWORD	TIME TO CRACK IT	COUNT
11	123456789	< 1 Second	1,593
12	88888888	< 1 Second	1,465
13	888888	< 1 Second	1,408
14	000000	< 1 Second	1,348
15	q123456	< 1 Second	1,111
16	111111	< 1 Second	1,094
17	asdasd	< 1 Second	1,025
18	Aladdin66	9 Hours	1,005
19	david221	59 Seconds	1,000
20	qq123456	2 Seconds	963

# RockYou字典檔



hashcat  
advanced  
password  
recovery

## RockYou2021: largest password compilation of all time leaked online with 8.4 billion entries

Updated on: February 24, 2023 2:28 PM 35



Edvardas Mikalauskas, Senior Researcher



What seems to be the largest password collection of all time has been leaked on a popular hacker forum. A forum user posted a massive 100GB TXT file that contains 8.4 billion entries of passwords, which have presumably been combined from previous data leaks and breaches.

10 Billion Rockyou2024 Password Compilation Cloud Mix  
ObamaCare · 4 minutes ago

Quick search...

Cloud Mix 10 Billion Rockyou2024 Password Compilation Jump to new Watch

4 minutes ago New 1

Hi,

Xmas came early this year. I present you a new rockyou2024 password list with over 9.9 billion passwords!

I updated rockyou21 with collected new data from recent leaked databases in various forums over this and last years.

Also cracked some old ones with my new 4090. This contains actual new real passwords from users.

You must either reply or click 'Like' to see the hidden information contained here.

Joined: May 24, 2024  
Messages: 5  
Reaction score: 25  
#CR: 32

Worked hard on this fellas, enjoy!

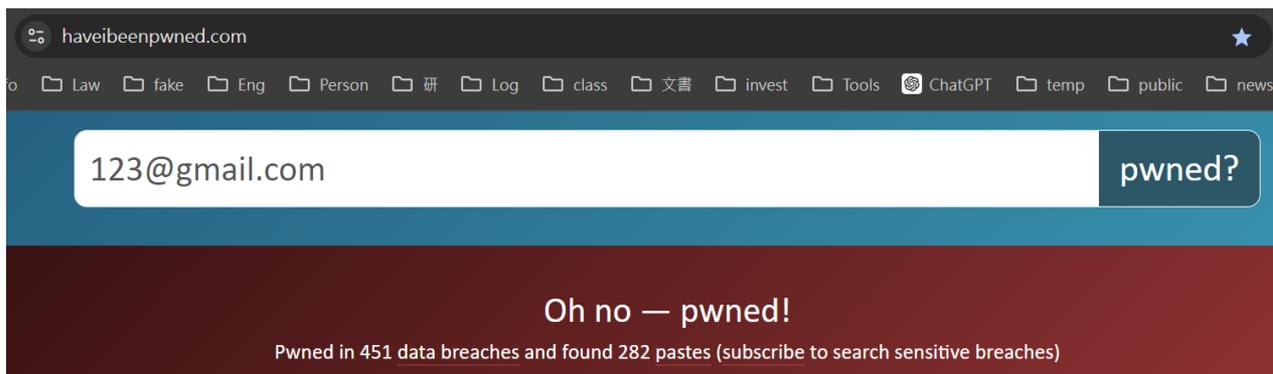
Report

Лайк! + Quote ObamaCare Reply to ObamaCare



# 防護-密碼保護

1. 使用密碼管理器。
2. 更改預設密碼、增加密碼複雜性、嘗試次數限制。
3. 限制密碼暴露、VPN連線、僅受信任可存取RDP。
4. 驗證：多因子、二階段。



# 安全檢查、更新

## 1. 安全檢查

## 2. 更新

設定

你與 Google

自動填入和密碼

隱私權和安全性

效能

外觀

搜尋引擎

預設瀏覽器

起始畫面

語言

下載

搜尋設定

安全檢查

安全資訊一覽



2 組重複使用的密碼  
設定不同的密碼



Chrome 目前是最新版本  
版本 127.0.6533.100 (正式版本) (64 位元)



已啟用安全瀏覽強化防護功能  
目前採用 Chrome 最強大的安全防護機制

安全建議



目前沒有需要處理的事項  
如有任何需要檢查的事項，Chrome 會通知你



瞭解 Chrome 如何保護資料安全

密碼安全檢查

已檢查 11 個網站和應用程式的密碼  
剛剛

- ✓ 沒有任何密碼外洩  
如果密碼外洩，我們會通知你。
- ! 2 組重複使用的密碼  
設定不同的密碼
- ! 1 組密碼的強度太低  
建立高強度密碼

關於 Chrome



Google Chrome



Chrome 目前是最新版本  
版本 127.0.6533.100 (正式版本) (64 位元)

# 瀏覽安全性



## 強化防護

系統會根據你傳送到 Google 的瀏覽資料，即時、主動防範危險的網站、下載內容和擴充功能



### 開啟時

-  這項防護機制分析的網站資料比標準防護來得多，因此即使是 Google 不知道的網站，這項防護機制也能提供危險網站警告。你可以選擇略過 Chrome 的警告。
-  提供深入掃描功能，檢查是否有可疑的下載內容。
-  當你登入帳戶後，保護你在各項 Google 服務中的安全。
-  可為你 and 所有網路使用者提供更完善的安全防護。
-  如果你使用的密碼因資料侵害事件而外洩，系統會顯示警告訊息。

### 注意事項

-  將你造訪的網址和網頁內容、下載內容、擴充功能活動和系統資訊的少許樣本傳送給 Google 安全瀏覽服務，檢查是否有害。
-  當你登入後，這類資料會連結到 Google 帳戶，保護你在各項 Google 服務中的安全，例如在安全事件發生後強化 Gmail 的防護機制。
-  不會大幅降低瀏覽器或裝置運作速度。

進一步瞭解 [Chrome 如何保護你的資料隱私](#)



## 標準防護

防範已知的危險網站、下載內容和擴充功能。當你造訪網站時，Chrome 會透過隱私權伺服器隱藏你的 IP 位址，再傳送經模糊處理的部分網址傳送給 Google。如果網站有可疑行為，系統也會傳送整個網址和部分網頁內容。



## 無防護 (不建議)

無法防範危險的網站、下載內容和擴充功能。其他 Google 產品的安全瀏覽設定不會受到影響。

# 資料管理安全性

## -建議措施

1. 落實個資資料分類存放、管控。
2. 有個資電腦，資料移交後格式化。
3. 公開資料適當去識別化，避免遭認出利用。
4. BitLocker磁碟加密。
5. 敏感資料加密傳送。
6. 敏感資料遮罩。
7. 離線儲存密碼。
8. 開啟系統稽核紀錄，定期監控帳戶是否異常。

# IOT設備防護

## -建議措施

- 1. 設備管控不易，落在校園各角落：**  
落實資產管理，掌握各設備之位置，造冊列管。
- 1. 系統更新不易，可能有疏漏：**  
掌握設備型號、版本，制定更新管理制度，定時更新，避免資安破口。
- 2. 設定配置不當：**  
設備啟用第一時間更改預設帳密、進行相關認證，原則上保守開放權限，開啟稽核紀錄。
- 3. 購買品牌不慎，產生後門漏洞：**  
不購買信譽不佳、中國製品牌，確認供應商來源無中國開發。

# 社交工程郵件

## -建議措施

1. 注意網址正確性(拼字、短網址)
2. 網站是否有**Copyright**資訊
3. 網站內**聯絡資訊**真偽集資訊露出多寡
4. 網站**憑證鎖頭**資訊是否正確
5. 難以記憶、沒有意義、**辨識度差**的網名
6. 未提供**常見付款方法**
7. 無完整的**商家資訊**或**客服系統**

The image shows a browser window with a search result for 'mygopen.com/2021/08/fake-line.html'. The search results list several items, with red boxes highlighting the '假冒' (Fake) and '正確' (Correct) entries. The '假冒' entry is for 'https://www.line.kimi/' and the '正確' entry is for 'https://line.me/zh-hant/'. Below the search results, there is a certificate viewer for 'mygopen.com'.

mygopen.com/2021/08/fake-line.html

約有 8,750,000,000 項結果 (搜尋時間: 0.43 秒)

假冒 - https://www.line.kimi/ -  
最新版本 - LINE Windows版  
Life On Line. LINE始終陪伴在你身旁。現在下載立即何地，都能輕鬆地聊天，以及免費的語音和視頻。

正確 - https://line.me/zh-hant/ -  
LINE | 始終陪伴在你身旁。  
超越通訊軟體，LINE為用戶建構全新的溝通型態與平台。

憑證檢視者: mygopen.com

一般(G) 詳細資訊(D)

核發對象

一般名稱 (CN)	mygopen.com
組織 (O)	<不是憑證的一部分>
組織單位 (OU)	<不是憑證的一部分>

發行者

一般名稱 (CN)	WE1
組織 (O)	Google Trust Services
組織單位 (OU)	<不是憑證的一部分>

有效期間

發行日期	2024年6月14日 星期五 下午1:30:35
到期日	2024年9月12日 星期四 下午1:30:34

SHA-256 指紋

憑證	b75d5110e031f1b84cc89f95b481df38e62e0d76d666952afd78c756fe9b48cb
公開金鑰	9b789dad7ea51db8af2f76f3ca828a15090a8da212f24d123707801beffa0e0

此網站頁面都設計得跟 LINE 官方圖案。

# 查詢驗證

# -Whois

Whois mygopen.com

whois.com/whois/mygopen.com

.COM @ \$8.98 Register a .COM domain for only \$8.98! While stocks last! BUY

Whois Identity for everyone Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

## mygopen.com

Updated 1 second ago

Interested in similar domain

Domain Information	
Domain:	mygopen.com
Registrar:	Squarespace Domains II LLC
Registered On:	2017-05-24
Expires On:	2031-05-24
Updated On:	2024-06-17
Status:	clientDeleteProhibited clientTransferProhibited
Name Servers:	hank.ns.cloudflare.com kara.ns.cloudflare.com

- my-g-open.com
- myvopen.com
- mygopenhouse.com
- findmygopen.com
- mygopen.net
- myvopen.net

# 查詢驗證

## -趨勢科技Site Safety Center 網站安全檢測

The screenshot displays the Trend Micro Site Safety Center website. At the top, the browser address bar shows the URL `global.sitesafety.trendmicro.com`. The navigation menu includes links for `Products`, `Solutions`, `Why Trend Micro`, `Research`, `Support`, `Partners`, and `Company`. A secondary navigation bar features `Home` and `Site Safety Center`. The main content area is titled "Is it safe?" and contains a search input field and a red `CHECK NOW` button. Below the search area, there is a section titled "About Our Safety Ratings" which explains that scores are based on website age, historical locations, and suspicious activities. At the bottom, four safety rating categories are listed: **Safe** (green checkmark), **Dangerous** (grey X), **Suspicious** (orange exclamation mark), and **Untested** (blue question mark).

global.sitesafety.trendmicro.com

Region Language Contact Us

TREND MICRO Business For Home

Products Solutions Why Trend Micro Research Support Partners Company

Home Site Safety Center

### Is it safe?

[CHECK NOW](#)

Please type the URL that you want to check.

#### About Our Safety Ratings

Scores are assigned based on factors such as a website's age, historical locations, changes, and indications of suspicious activities discovered through malware behavior analysis. We've advanced how we apply web reputation to keep pace with new types of criminal attacks that can come and go very quickly, or try to stay hidden.

<b>Safe</b> The latest tests indicate that this URL contains no malicious software and shows no signs of phishing.	<b>Dangerous</b> The latest tests indicate that this URL contains malicious software or phishing.	<b>Suspicious</b> This URL has been compromised before, or has some association with spam email messages.	<b>Untested</b> Because you were curious about this URL, Trend Micro will now check it for the first time. Thanks for mentioning it!
---	--	--	---

# 清除瀏覽資料

## 刪除瀏覽資料

基本

進階

時間範圍

過去 1 小時



瀏覽記錄

從所有已同步裝置上刪除歷史記錄



Cookie 和其他網站資料

你會從大多數網站登出，但不會因此登出 Google 帳戶，所以仍可刪除同步資料。



快取圖片和檔案

釋出不到 8.2 MB。下次造訪部分網站時，載入速度可能會變慢。



在你登入後，[搜尋記錄](#)和[其他形式的活動](#)可能會儲存至你的 Google 帳戶。你隨時可以刪除這些內容。

取消

刪除資料

## 刪除瀏覽資料

基本

進階

時間範圍

過去 1 小時



瀏覽記錄

無



下載記錄

無



Cookie 和其他網站資料

28 個網站 (Google 帳戶會保持登入狀態)



快取圖片和檔案

不到 8.2 MB



密碼和其他登入資料

無



自動填入表單資料

# Cookie設定

← 第三方 Cookie ?



管理網站可在你瀏覽時用來追蹤的資訊類型。

- 允許第三方 Cookie ▼
- 在無痕模式中封鎖第三方 Cookie ▲

 網站可使用 Cookie 改善瀏覽體驗，例如讓你保持登入狀態，或記住購物車中的商品

在無痕模式下，網站無法使用 Cookie 瞭解你的跨網站瀏覽活動 (即使是相關網站)，因此無法根據瀏覽活動提供個人化廣告等服務。某些網站的功能可能無法運作。

- 封鎖第三方 Cookie ▼

# 廣告隱私權設定

## ← 廣告隱私權設定



### 廣告主題

以你的瀏覽記錄做為依據。這項設定已關閉。



### 網站建議廣告

以你的網站活動做為依據。這項設定已關閉。



### 廣告評估功能

網站和廣告主可以瞭解廣告成效。這項設定已關閉。

## ← 廣告主題 ?

### 廣告主題

Chrome 會根據你最近的瀏覽記錄推測主題，做為網站放送個人化廣告的依據，同時保護你的身分資料

廣告主題只是網站在放送個人化廣告時的其中一項依據。即使沒有廣告主題，網站仍可放送廣告，但廣告內容可能較不貼近你的需求。進一步瞭解如何[管理廣告隱私權](#)。

## ← 網站建議廣告 ?

### 網站建議廣告

你造訪的網站可以判斷你喜愛的內容，並在接下來的瀏覽過程中顯示建議廣告

網站建議廣告功能只是網站在放送個人化廣告時的其中一項依據。即使你未開啟這項功能，網站仍可放送廣告，但廣告內容可能較不貼近你的需求。

## ← 廣告評估功能 ?

### 廣告評估功能

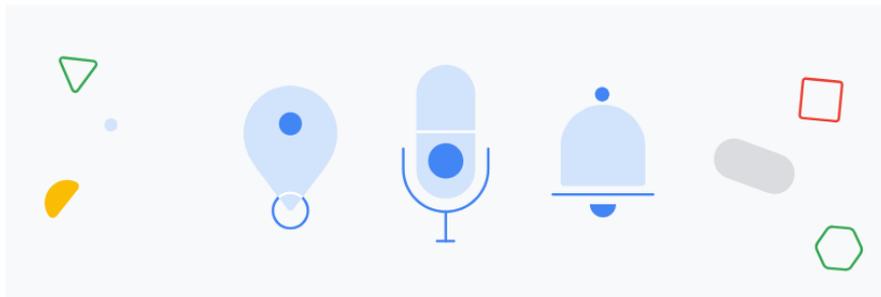
網站和廣告主可評估廣告成效

[開啟時](#)

[注意事項](#)

# 個別網站設定

← 網站設定



## 近期活動

- community.cellebrite.com  
已允許使用彈出式視窗與重新導向
- discord.com  
已封鎖麥克風

← discord.com

## 用量

36.2 KB · 5 個 Cookie

刪除資料

## 權限

重設權限

- 位置
- 攝影機
- 麥克風
- 動作感應器
- 通知
- JavaScript

詢問 (預設)

詢問 (預設)

封鎖

允許 (預設)

詢問 (預設)

允許 (預設)



**The End~**