永遠走在最前面
Always Ahead

基隆市政府
112年度資通安全通識教育訓練
多因子身份驗證(MFA)新時代

中華電信
Chunghwa Telecom

課程大綱

- **多因子認證(MFA)簡介**
  身份驗證(Authentication)與授權(Authorization)
  、安全的密碼設定、密碼強度檢驗、 密碼外洩檢查 、Password 認證問題、密碼替代方案、一次性密碼OTP、無密碼新時代PassKey
- **常見應用場景**
  Google MFA介紹
  Binance 加密貨幣交易所 MFA介紹
- **實際攻擊案例分享**
  VPN多因素認證繞過、WebMail多因素認證繞過、假網站釣魚信件多因素認證繞過及社交工程資料庫成熟應用(多因素認證繞過)
- **防護策略與日常應注意事項**

永遠走在最前面
Always Ahead

多因子認證(MFA)簡介

中華電信
Chunghwa Telecom

身份驗證(Authentication)與授權(Authorization)

身份驗證(**Authentication**)是用於驗證用戶身份的過程

授權(**Authorization**)是一種向用戶提供訪問特定資源的權限的方法

Source: https://cybermeteoroid.com/authentication-and-authorization-what-comes-first-in-security/

身份驗證(Authentication)與授權(Authorization)

登入系統輸入用戶名和密碼。
用戶名表明你是誰，但本身不足以授予你訪問權限。
只有該用戶應該知道的密碼結合使用時，才允許連線進入你的系統。

Source: https://cybermeteoroid.com/authentication-and-authorization-what-comes-first-in-security/

身份驗證(Authentication)與授權(Authorization)

5 個身份驗證因素

- 你知道的事情：
  在此身份驗證中，用戶通過輸入他們的用戶 ID、密碼或個人識別碼來驗證自己。
- 你擁有的東西：
  在這種類型的身份驗證中，用戶可以使用一些東西來對自己進行身份驗證。
- Somewhere You Are：
  特定位置或特定坐標以驗證自己。
- Something You Are：
  生物特徵來驗證自己，例如指紋、虹膜辨識等。
- 你做的事情：
  為了登錄網站，用戶需要在屏幕上執行一些步驟來驗證自己。

Source: https://cybermeteoroid.com/authentication-and-authorization-what-comes-first-in-security/

身份驗證(Authentication)與授權(Authorization)

單因素認證模型：

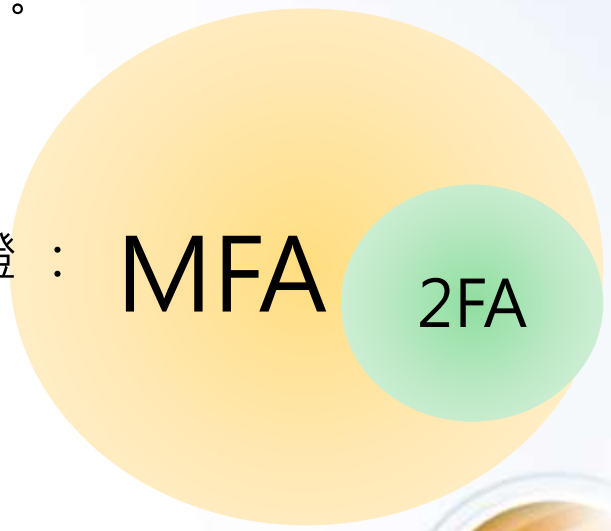
- 「 5 個身份驗證因素」只採用一個因素進行驗證，最常見的是密碼。
- 「單因素身份驗證模型」是所有身份驗證模型中最弱的。
- 密碼很容易被駭客破解、猜測或竊取。
- 盡可能避免單因素身份驗證，以強化身分驗證安全。

Source: https://cybermeteoroid.com/authentication-and-authorization-what-comes-first-in-security/

身份驗證(Authentication)與授權(Authorization)

Multi-factor Authentication (MFA)多因素身份驗證：
是一種需要兩個或更多身份驗證因素的身份驗證。

Two-factor authentication (2FA)雙因素身份驗證 ：
恰好需要兩個身份驗證因素。



身份驗證(Authentication)與授權(Authorization)

多因素身份驗證 (MFA) 模型

- 用戶使用兩個或多個以上身份驗證因素來驗證自己，例如用戶名/密碼和指紋來驗證自己。
- MFA 比任何其他單因素身份驗證都更好，提供更好的安全性，但登錄過程更長。
- 多因素身份驗證 (MFA) 模型可提升身分驗證強度，但非100%安全。

ATM提款機提款機制MFA：
用戶持有銀行核發的提款卡，並且要輸入密碼，才能進行提款動作。

Source: https://cybermeteoroid.com/authentication-and-authorization-what-comes-first-in-security/

身份驗證(Authentication)與授權(Authorization)

ATM提款-台新銀行為例

無卡提款(手機)

密碼

多因素身份驗證 (MFA)

身份驗證(Authentication)與授權(Authorization)

ATM提款-中國信託為例

無卡提款(指靜脈/臉部辨識)

密碼

多因素身份驗證 (MFA)

身份驗證(Authentication)與授權(Authorization)

身份驗證(Authentication)和授權(Authorization)之間的區別

驗證Authentication	授權Authorization
身份驗證過程驗證用戶是誰。	授權過程決定了用戶可以訪問哪些資源。
身份驗證在授權之前完成。	而授權是在身份驗證之後完成的。
過程需要用戶的資訊，例如：用戶名和密碼等。	此過程需要用戶的權限或安全級別。
用戶可以更改身份驗證憑據(密碼)。	授權權限不能由用戶更改，權限由組織授予用戶。
情境： 員工在訪問公司內部系統之前需要進行身份驗證。	情境： 權限決定了員工在認證成功後，可使用系統上哪些資源。

Source: https://cybermeteoroid.com/authentication-and-authorization-what-comes-first-in-security/

安全的密碼設定

風傳媒

祖克柏帳號的密碼是dadada，難怪被盜

臉書CEO祖克柏的帳號6日傳出被駭客所盜，最新的消息則是他使用的是一個駭客只要花25秒就能破解的「菜市場密碼」─dadada，顯然祖克柏的安全意識也明顯...

駭客從社交網路LinkedIn竊取了1.17億個電子郵件帳號和密碼。並在黑市上進行交易。在被售賣的電子郵件列表中，發現了祖克柏的電子郵件帳號密碼。

密碼居然是極其簡單的「dadada」

安全的密碼設定

他LinkedIn的密碼「dadada」用到了他的Twitter 和Pinterest帳戶中。駭客輕鬆破解其他兩個帳戶了~

密碼「dadada」

密碼共用

密碼「dadada」

安全的密碼設定

杰弗斯表示，川普一直以來都不喜歡使用「兩段式驗證」，而且使用的密碼都過於簡單，2016年時，他就發現川普的推特密碼是「你被開除（yourefired）」，這句話是川普在美國實境節目《誰是接班人》中的經典名言。

安全的密碼設定

	2019		2020		2021	
	Password	Number of users	Password	Number of users	Password	Number of users
1	**12345**	2,812,220	**123456**	2,543,285	**123456**	103,170,552
2	**123456**	2,485,216	**123456789**	961,435	**123456789**	46,027,530
3	**123456789**	1,052,268	**picture1**	371,612	**12345**	32,955,431
4	**test1**	993,756	**password**	360,467	**qwerty**	22,317,280
5	**password**	830,846	**12345678**	322,187	**password**	20,958,297
6	**12345678**	512,560	**111111**	230,507	**12345678**	14,745,771
7	**zinch**	483,443	**123123**	189,327	**111111**	13,354,149
8	**g_czechout**	372,278	**12345**	188,268	**123123**	10,244,398
9	**asdf**	359,520	**1234567890**	171,724	**1234567890**	9,646,621
10	**qwerty**	348,762	**senha**	167,728	**1234567**	9,396,813

安全的密碼設定

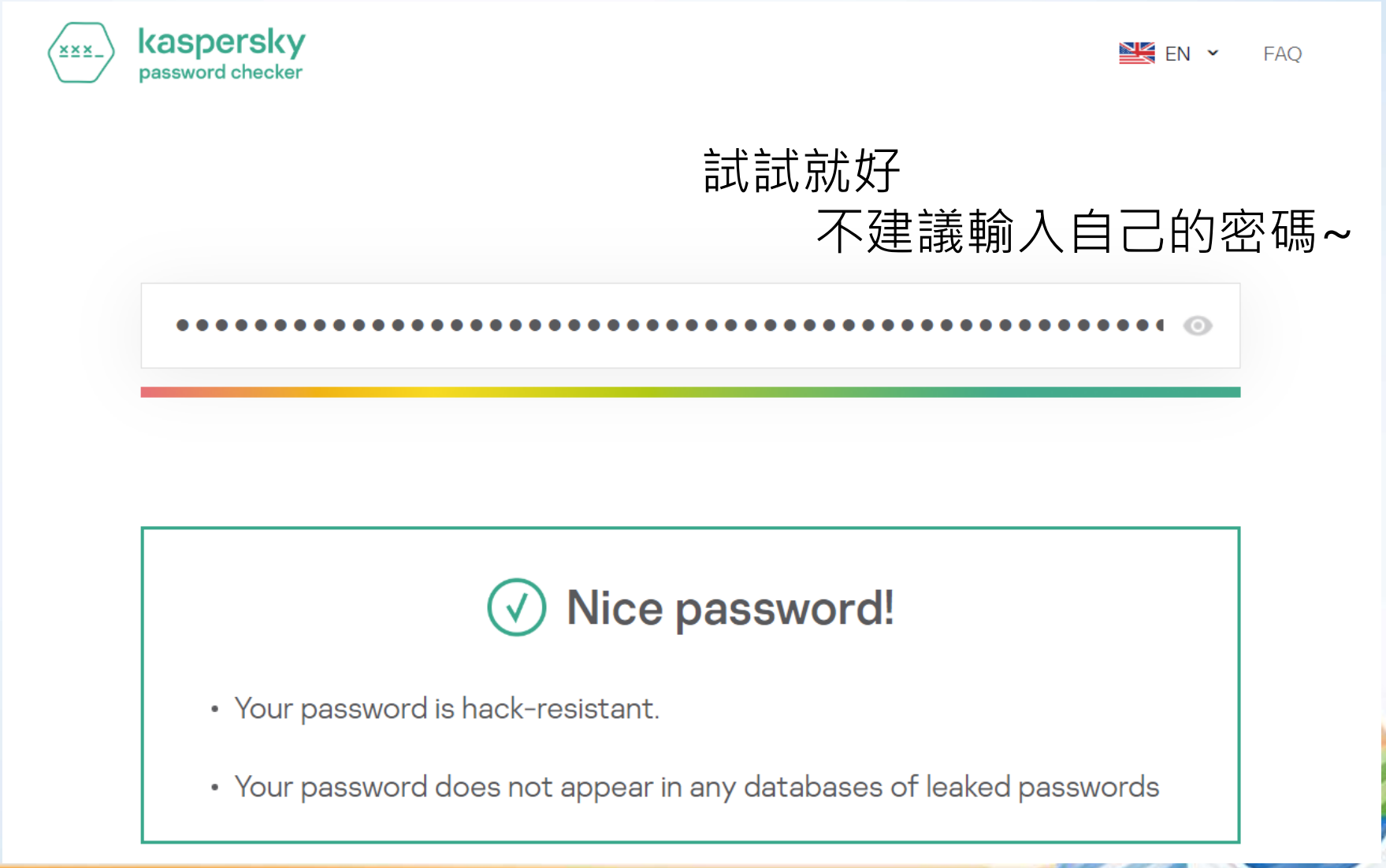

TOP 10 MOST COMMON PASSWORDS IN 2022
Rank
Password
Time to crack it
1
password
< 1 Second
2
123456
< 1 Second
3
123456789
< 1 Second
4
guest
10 Seconds
5
qwerty
< 1 Second
6
12345678
< 1 Second
7
111111
< 1 Second
8
12345
< 1 Second
9
col123456
11 Seconds
10
123123
< 1 Second

安全的密碼設定

The top 10 most common passwords list in 2023:

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

密碼強度檢驗



Source: https://password.kaspersky.com/

密碼外洩檢查

';--have i been pwned?

Check if your email or phone is in a data breach

DEHASHED

mypwd
by ///AXUR

BreachDirectory

leakpeek
Is your data safe?

BREACHDIRECTORY.ORG

密碼外洩檢查

英國國家犯罪調查局
（NCA）

美國聯邦調查局
（FBI）

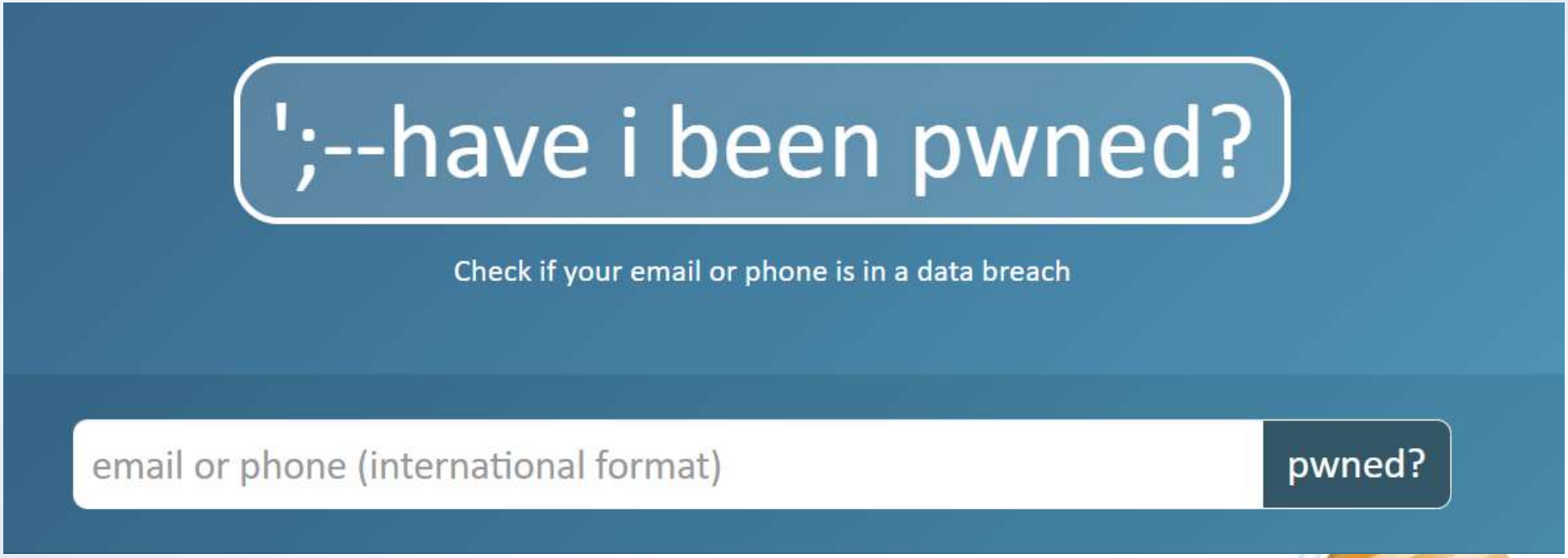
暗網

密碼外洩資料庫

提供全球使用者免費使用
強化Email保護

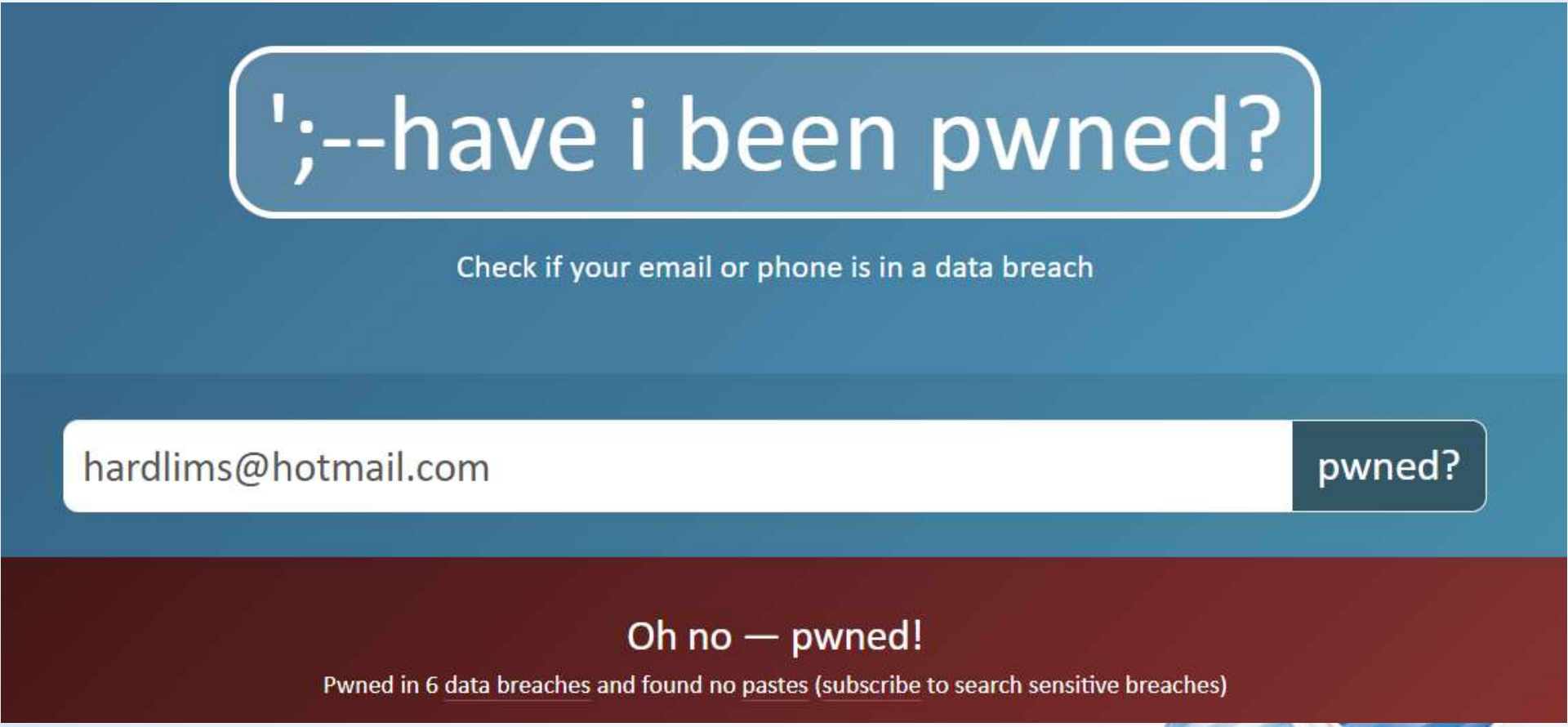
密碼外洩檢查

確認自己的密碼是否外洩



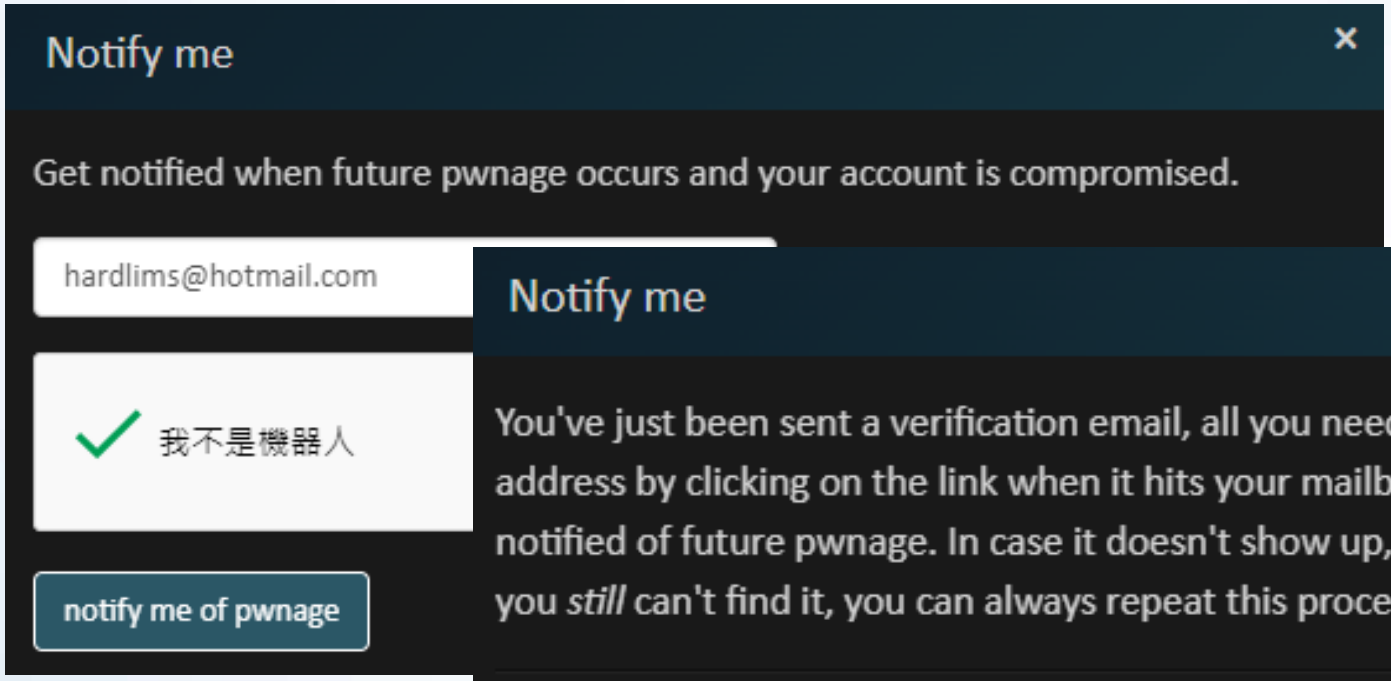
密碼外洩檢查

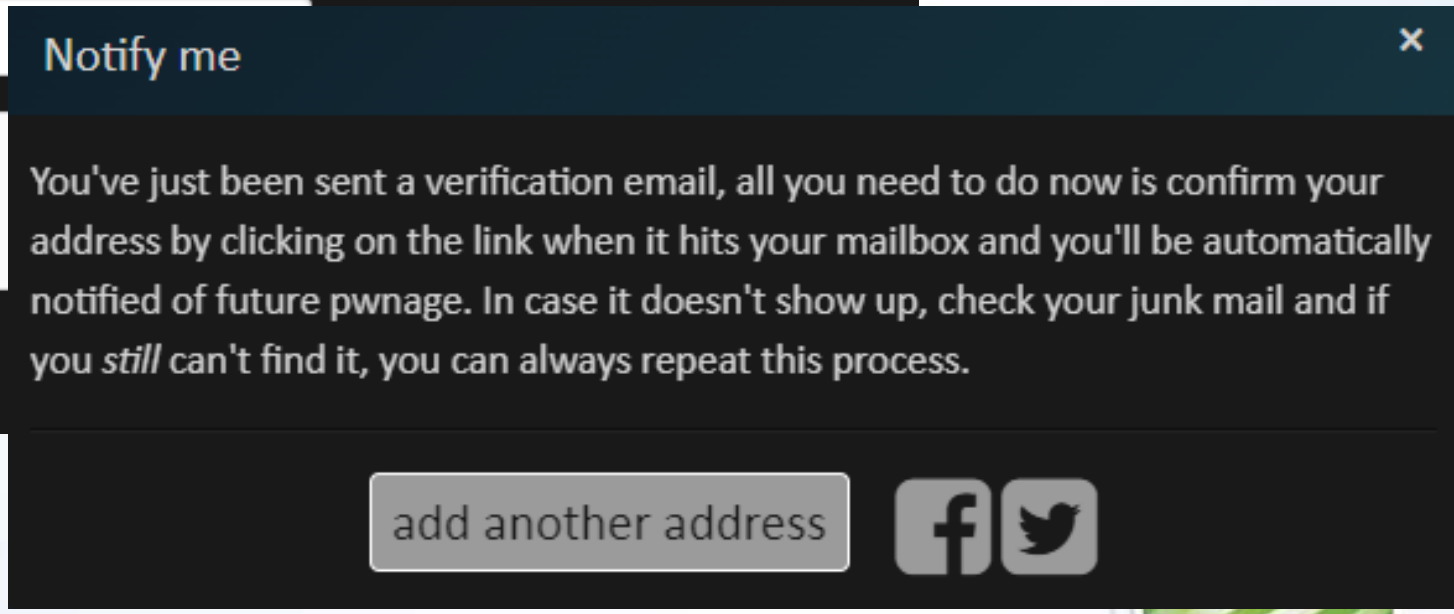
- 定期更換密碼
- 信箱密碼監控機制：密碼已外洩，立即更換密碼



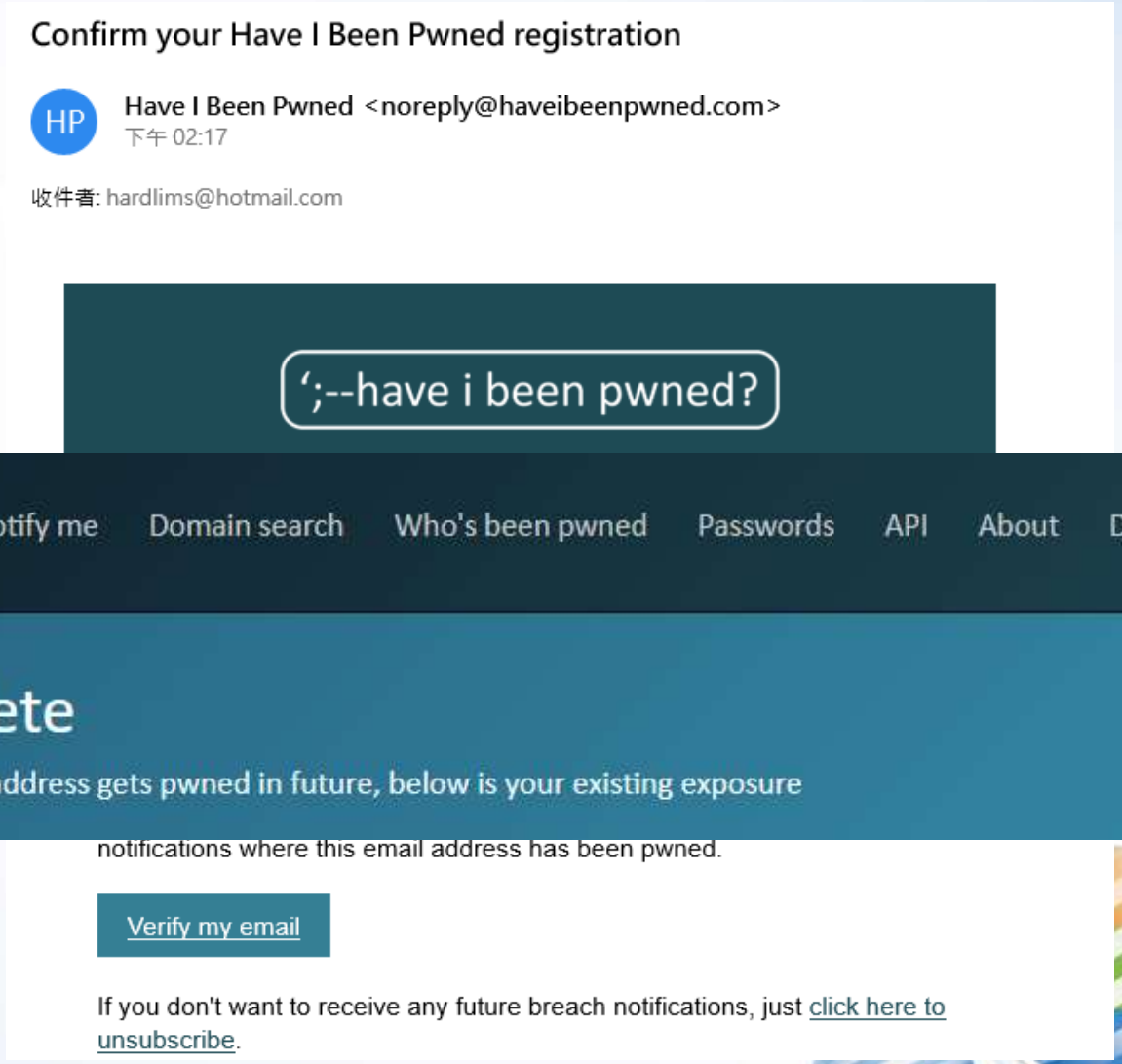
密碼外洩檢查

自己帳戶的密碼外洩時，自動發信件通知





密碼外洩檢查


Confirm your Have I Been Pwned registration
HP
Have I Been Pwned <noreply@haveibeenpwned.com>
下午 02:17
收件者: hardlims@hotmail.com
';--have i been pwned?
';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
Verification complete
All done, you'll be sent an email if this address gets pwned in future, below is your existing exposure
notifications where this email address has been pwned.
Verify my email
If you don't want to receive any future breach notifications, just click here to unsubscribe.

密碼外洩檢查

2 Steps to Better Password Security

Monitoring Have I Been Pwned for data breaches is a great start, now try these next 2 steps to protect all your accounts:

Step 1: Protect yourself with strong, unique passwords for each website with the 1Password password manager

Step 2: Enable 2 factor authentication and store the codes inside your 1Password account

每個網站密碼都不能一樣

MFA多因子認證方式登入

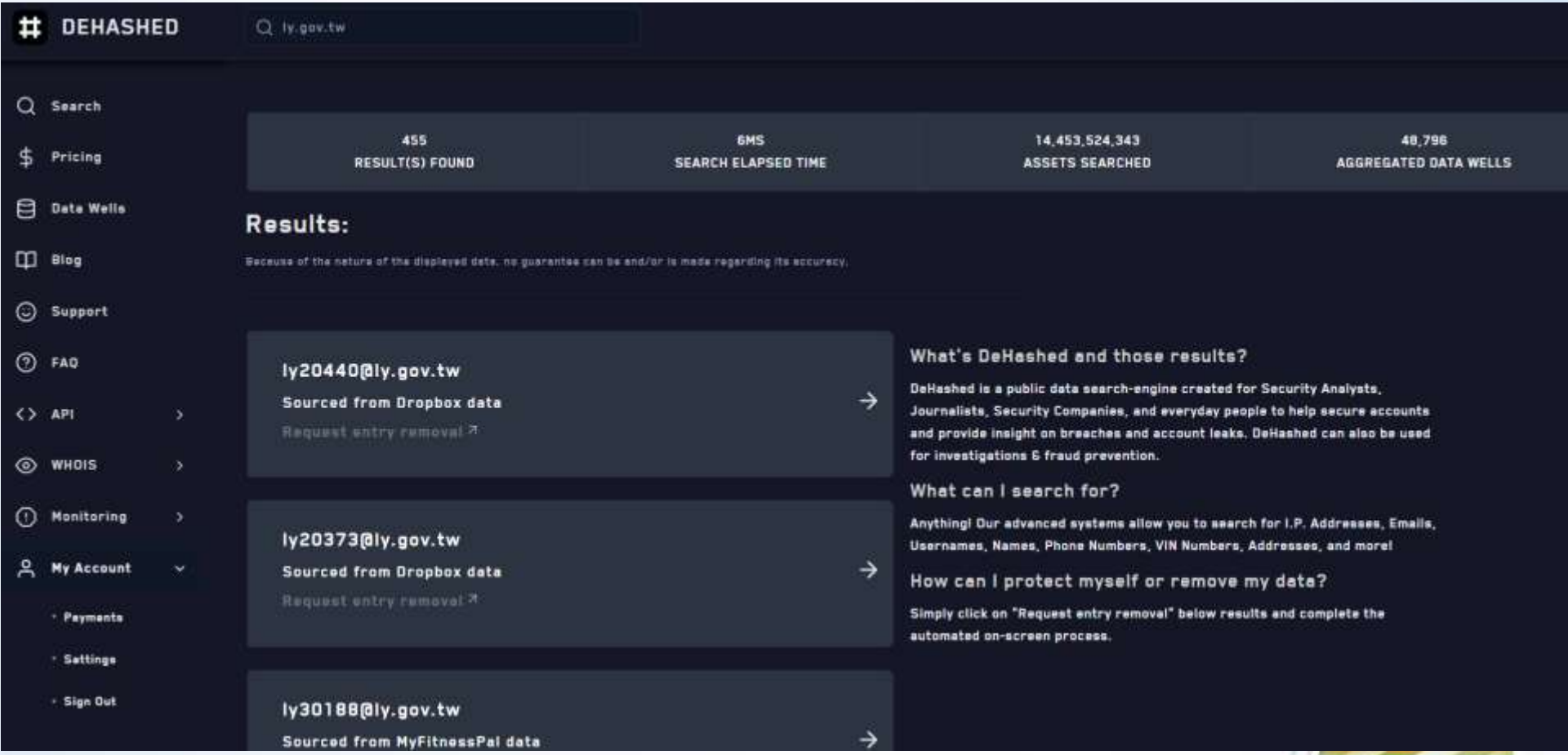
密碼外洩檢查

DEHASHED

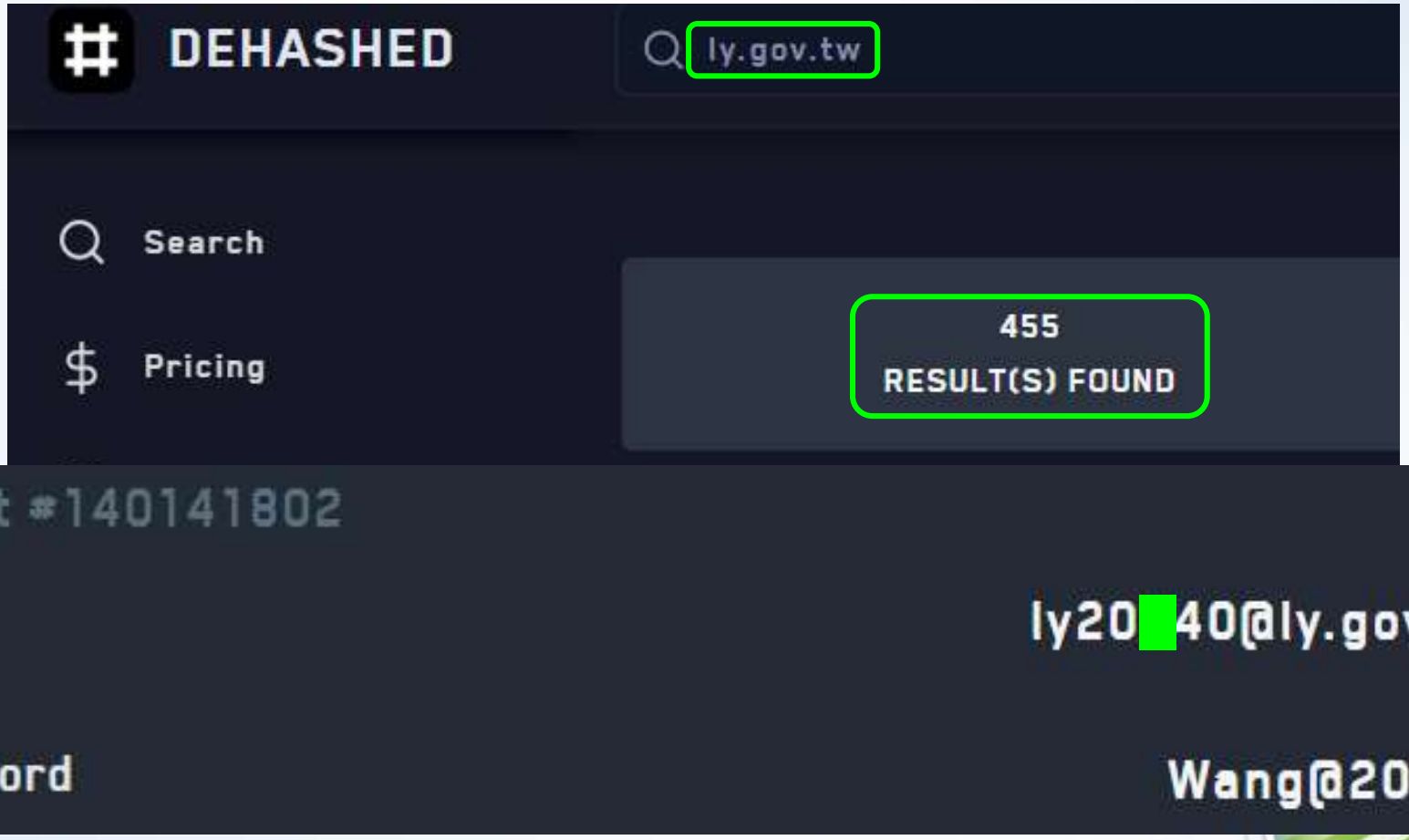
檢查自己的帳戶密碼是否外洩~

還可以查詢
別人的!!

密碼外洩檢查


DEHASHED
ly.gov.tw
Search
Pricing
Data Wells
Blog
Support
FAQ
API
WHOIS
Monitoring
My Account
Payments
Settings
Sign Out
455
RESULT(S) FOUND
6MS
SEARCH ELAPSED TIME
14,453,524,343
ASSETS SEARCHED
48,796
AGGREGATED DATA WELLS
Results:
ly20440@ly.gov.tw
Sourced from Dropbox data
Request entry removal
ly20373@ly.gov.tw
Sourced from Dropbox data
Request entry removal
ly30188@ly.gov.tw
Sourced from MyFitnessPal data
What's DeHashed and those results?
DeHashed is a public data search-engine created for Security Analysts, Journalists, Security Companies, and everyday people to help secure accounts and provide insight on breaches and account leaks. DeHashed can also be used for investigations & fraud prevention.
What can I search for?
Anything! Our advanced systems allow you to search for I.P. Addresses, Emails, Usernames, Names, Phone Numbers, VIN Numbers, Addresses, and more!
How can I protect myself or remove my data?
Simply click on "Request entry removal" below results and complete the automated on-screen process.

密碼外洩檢查


DEHASHED
ly.gov.tw
Search
Pricing
455
RESULT(S) FOUND
Result #140141802
Email
ly20 40@ly.gov.tw
Password
Wang@20 40

密碼外洩檢查

公司規定密碼複雜度，英文數字大小寫~

員工為了方便記憶

不同系統都使用同一組密碼?

駭客取得一組密碼=成功取得所有系統密碼

Password 認證問題

弱密碼易被暴力破解

```
root@kali:/home/kali/Desktop# hydra -L user.txt -P pass.txt -t 2 -vV -e ns 192.168.124.10 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-22 00:02:58
[DATA] max 2 tasks per 1 server, overall 2 tasks, 40 login tries (l:5/p:8), ~20 tries per task
[DATA] attacking ssh://192.168.124.10:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://admin@192.168.124.10:22
[INFO] Successful, password authentication is supported by ssh://192.168.124.10:22
[ATTEMPT] target 192.168.124.10 - login "admin" - pass "admin" - 1 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "admin" - pass "" - 2 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "admin" - pass "admin123" - 4 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "admin" - pass "abc123" - 5 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "admin" - pass "root" - 6 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "admin" - pass "password" - 7 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "admin" - pass "123456" - 8 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "123456" - pass "123456" - 9 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "123456" - pass "" - 10 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "123456" - pass "admin" - 11 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "123456" - pass "admin123" - 12 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "123456" - pass "abc123" - 13 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "123456" - pass "root" - 14 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "123456" - pass "password" - 15 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "1234" - pass "1234" - 17 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "1234" - pass "" - 18 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "1234" - pass "admin" - 19 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "1234" - pass "admin123" - 20 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "1234" - pass "abc123" - 21 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "1234" - pass "root" - 22 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "1234" - pass "password" - 23 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "1234" - pass "123456" - 24 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "root" - pass "root" - 25 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.124.10 - login "root" - pass "" - 26 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.124.10 - login "root" - pass "admin" - 27 of 40 [child 0] (0/0)
```

Password 認證問題

WiFi密碼勿使用市話或行動電話號碼....

弱密碼易被暴力破解

```
                    Aircrack-ng 1.6

[00:23:10] 3666028/10000000 keys tested (2681.33 k/s)

Time left: 39 minutes, 22 seconds                          36.66%

                    KEY FOUND! [ 0[redacted]11578 ]


Master Key     : 0C 0B 80 72 03 29 94 C5 FE A3 8D 89 AD AE 15 2A
                 90 6B 3A C4 E1 25 6D 5D 45 19 79 2E C2 17 87 AE

Transient Key  : 9C 9A C9 E7 61 24 5E 5E BB 38 7E 38 21 B8 70 C7
                 31 4C 8E AB E8 17 0C D2 30 FE 37 E1 58 68 30 94
                 90 7A E6 34 99 43 7D 53 FB 4B 95 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 49 C1 00 AC D4 14 0E 56 8E F7 15 56 8E 2F 2B F3
```

Password 認證問題

肩窺攻擊

Password 認證問題

密碼具有可轉移性
任何取得有效密碼的人，都能在任何地方，以任何裝置登入

密碼替代方案

Android unlock pattern

密碼替代方案

生物辨識(身體就是密碼)

密碼替代方案

yam.com
https://dq.yam.com › 文章列表

照片也能複製指紋德部長指紋遭駭客盜走 - 地球圖輯隊

2014年12月30日 — 歐洲最大駭客聯盟搗亂電腦俱樂部(CCC)的駭客宣稱，他已經用照片和一個軟體成功複製了德國國防部長的指紋。 這位駭客名叫克里斯勒(Jan Krissler)，他身上並 ...

ettoday.net
https://www.ettoday.net › 生活

拍照別再比YA！「駭客100%還原指紋、秒解鎖手機」 專家教2 ...

2020年6月2日 — 拍照別再比YA了，因可能讓個資外洩！上海資安專家最新實驗發現，如果您拍照比YA，駭客能夠藉由放大照片、AI增強技術，取得您的指紋，進一步解鎖您的 ...

cnews.com.tw
https://cnews.com.tw › 拍照比ya真會導致指紋外流、...

拍照比YA真會導致指紋外流、資安外洩？中日專家這麼說！

2022年4月13日 — 專家詳細說明表示，原則上，只要在1.5公尺內拍攝YA的照片，就可以100%還原出被拍照者的指紋；而在1.5到3公尺距離內拍攝的照片，指紋還原度大約50%，如果是 ...

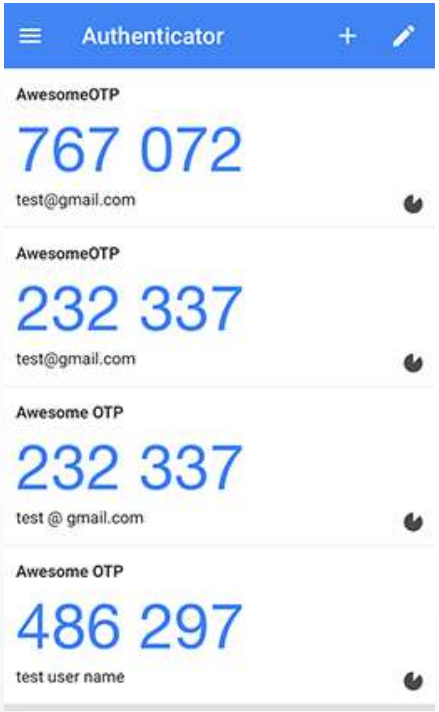

Kraken Security Labs Bypasses Biometric Security With $5 In Materials
kraken SECURITY LABS
0:00 / 1:02
HD

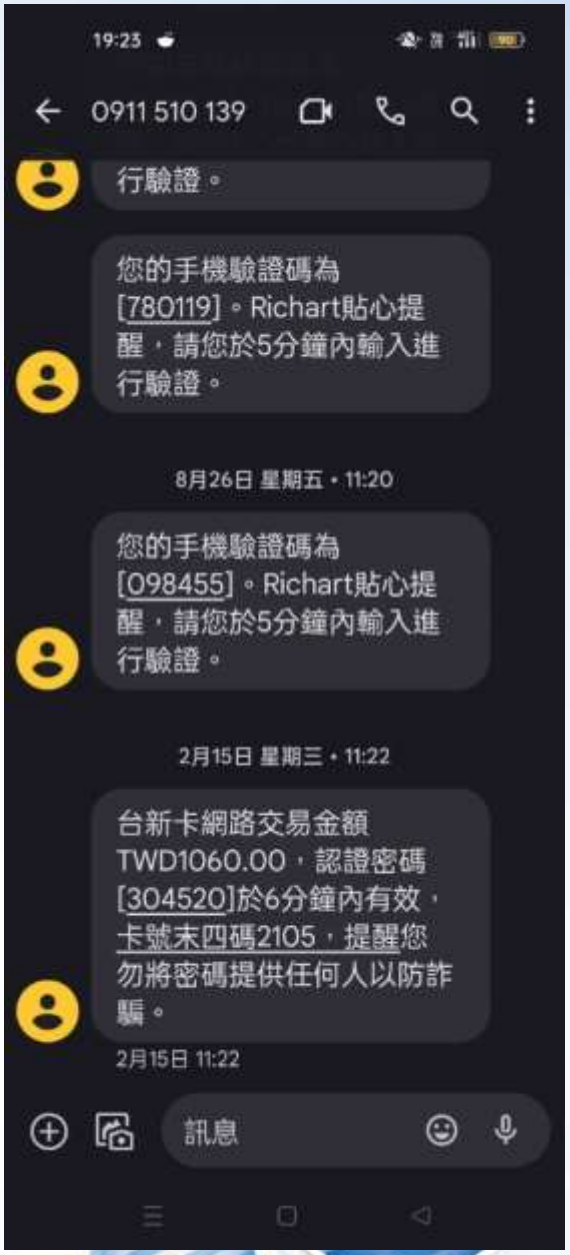
一次性密碼OTP

透過手機簡訊或APP(Google Authenticator)

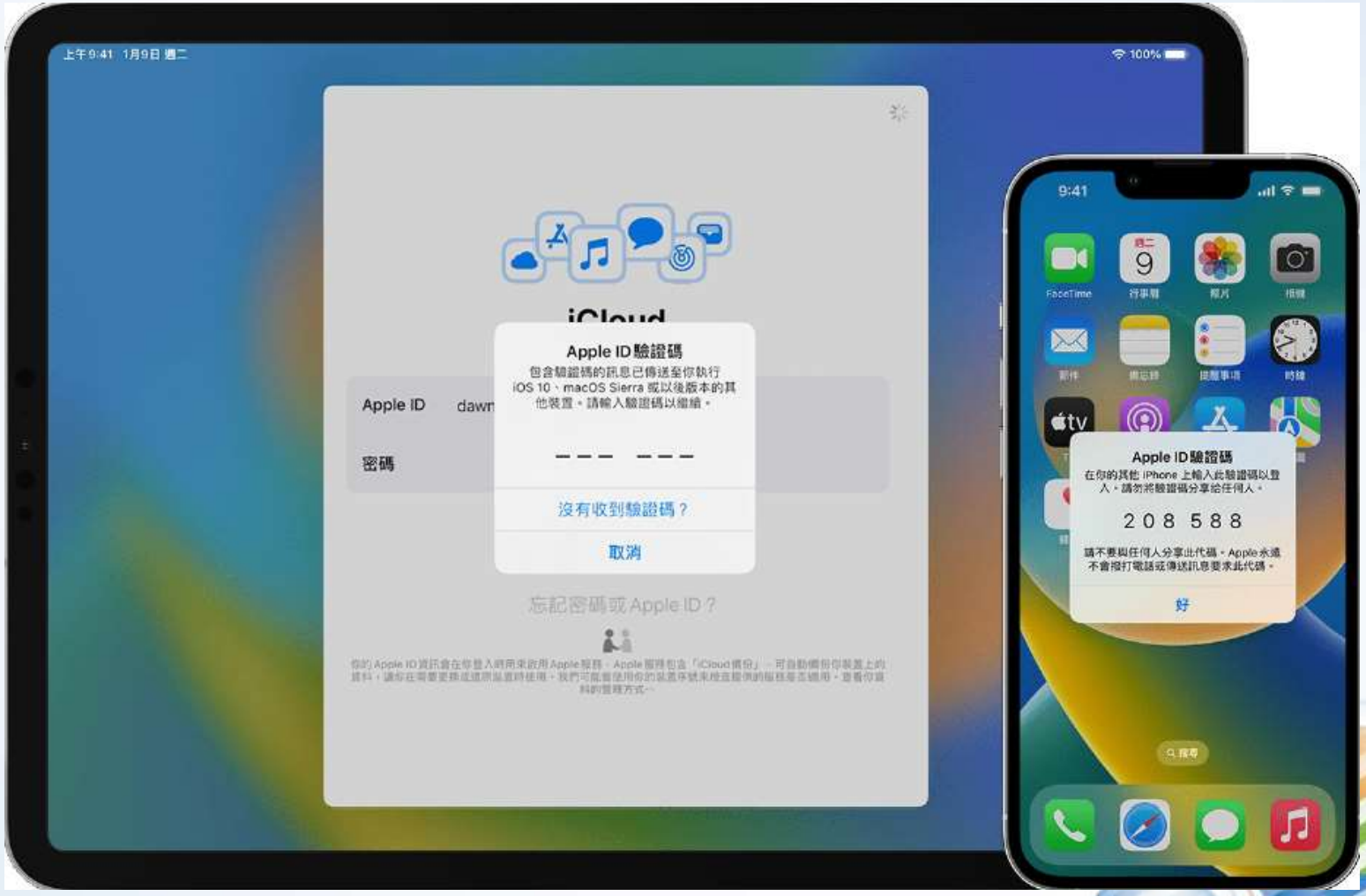
OTP, One-Time Password

密碼會隨著時間變動(1分鐘)





一次性密碼OTP


Apple ID驗證碼
包含驗證碼的訊息已傳送至你執行 iOS 10、macOS Sierra 或以後版本的其他裝置。請輸入驗證碼以繼續。
Apple ID
密碼
沒有收到驗證碼？
取消
忘記密碼或 Apple ID？
Apple ID驗證碼
在你的其他 iPhone 上輸入此驗證碼以登入。請勿將驗證碼分享給任何人。
208 588
請不要與任何人分享此代碼。Apple 永遠不會撥打電話或傳送訊息要求此代碼。
好

一次性密碼OTP

Common Factors for Authentication

- Something you know
  - password, secret key
- Something you have
  - smart card, cell phones, OTP dongles
- Something you are
  - fingerprint or other biometric information

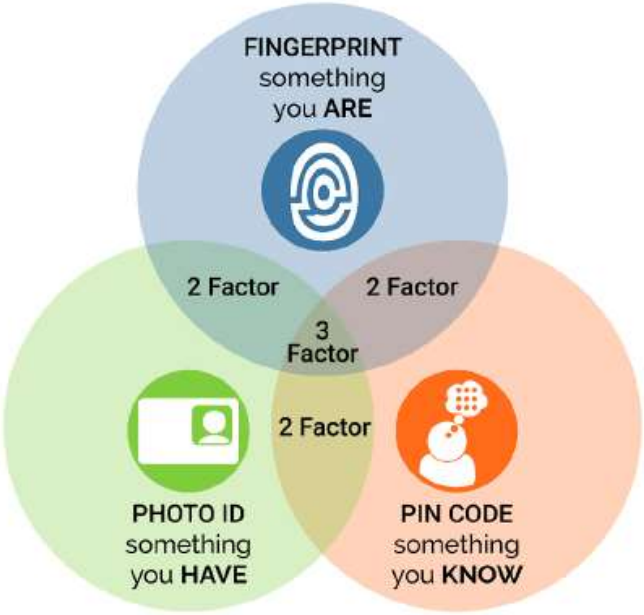
Two/multi factors authentication

- Combine two/more of the three factors

一次性密碼OTP

Multi/Two Factors Authentication

- Combine two/more of the three factors



無密碼新時代PassKeys


泛科學
PanSci

永遠走在最前面
Always Ahead

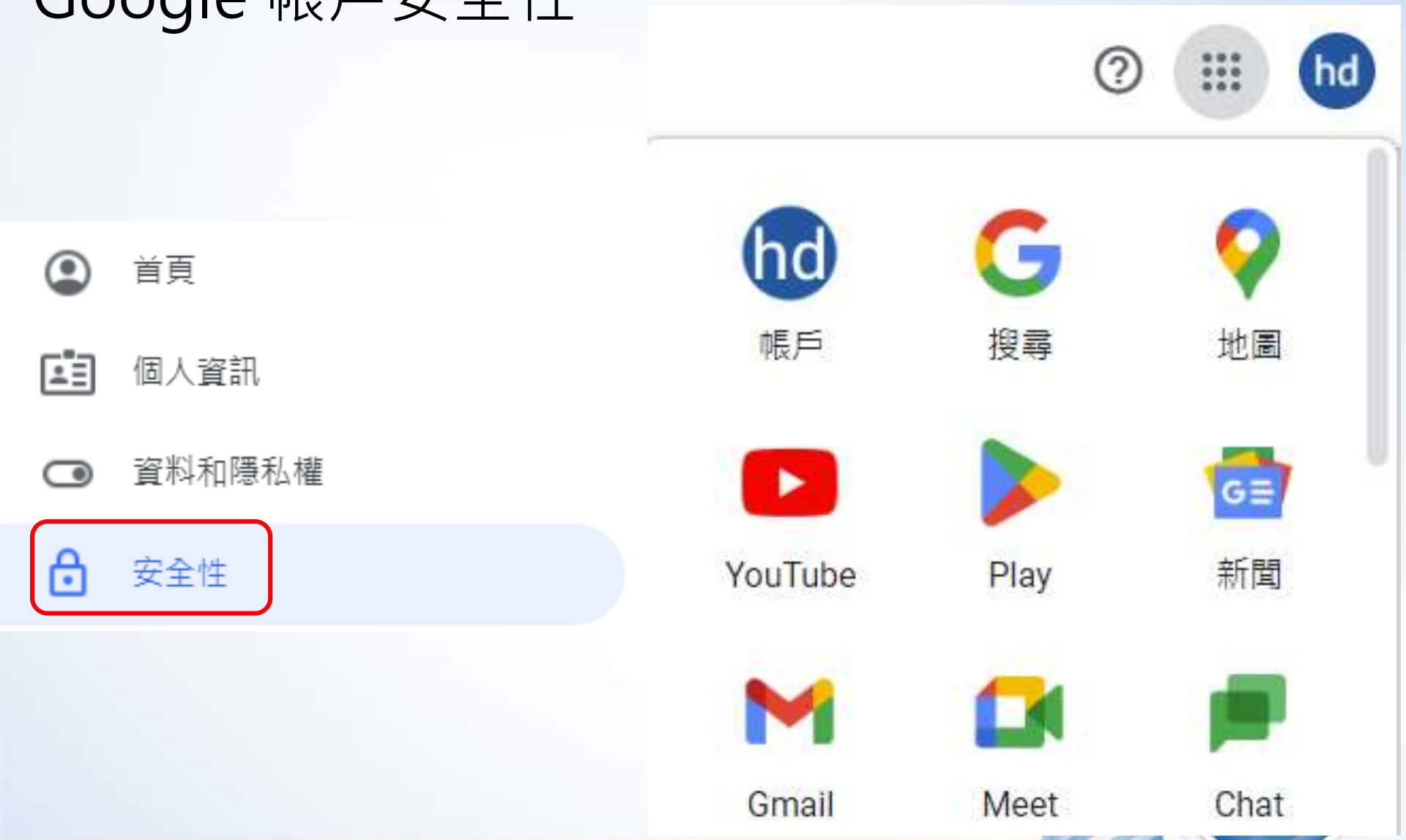
常見應用場景

中華電信
Chunghwa Telecom

Google 驗證


Google
選擇帳戶
hd
hd wang
mimicwang1978@gmail.com
未登入
使用其他帳戶
移除帳戶

Google 帳戶安全性



Google 密碼變更


您登入 Google 的方式
請定期更新這些資訊，確保您隨時都能順利登入自己的 Google 帳戶
兩步驟驗證
兩步驟驗證已停用
使用您的手機登入帳戶
已關閉
密碼
上次變更時間：2022年11月17日
備援電話號碼
0952
備援電子郵件
請驗證 hardlims@hotmail.com

Google 密碼變更


密碼
請選用高強度密碼；此外，切勿在其他帳戶中重複使用該密碼。瞭解詳情
變更密碼後，您會在裝置上登出帳戶，但某些裝置例外。
新密碼
密碼強度：
至少要有 8 個字元。請勿使用與其他網站帳戶相同的密碼，或是任何容易破解的密碼 (例如寵物的名字)。為什麼？
確認新密碼
變更密碼

Google 密碼變更


您登入 Google 的方式
請定期更新這些資訊，確保您隨時都能順利登入自己的 Google 帳戶
兩步驟驗證
兩步驟驗證已停用
使用您的手機登入帳戶
已關閉
密碼
上次變更時間：凌晨12:11
備援電話號碼
0952
備援電子郵件
請驗證 hardlims@hotmail.com

Google 密碼變更

針對 mimicwang1978@gmail.com 發出的安全性警示

G Google <no-reply@accounts.google.com>

上午 12:11

收件者: hardlims@hotmail.com

E-mail通知密碼變更

這是系統針對 mimicwang1978@gmail.com 發出的安全性警示副本，而 hardlims@hotmail.com 是該帳戶的備援電子郵件地址。 如果您對這個帳戶沒有印象，請移除該帳戶。

Google

您的密碼已變更

hd mimicwang1978@gmail.com

您的 Google 帳戶 (mimicwang1978@gmail.com) 密碼已變更。如果您沒有變更密碼，建議您還原帳戶。

您也可以前往以下網址查看帳戶安全相關活動：

https://myaccount.google.com/notifications

您的 Google 帳戶和服務有重大異動，系統特此發送這封電子郵件通知您。

Google 備援電話號碼

Google 備援電話號碼

Google 備援電子郵件

Google 備援電子郵件

Google 備援電子郵件

驗證備援電子郵件地址

請輸入系統傳送到 hardlims@hotmail.com 的 6 位數驗證碼。沒有收到相關電子郵件嗎？ 傳送新的驗證碼。

驗證碼

0 / 6

取消　　驗證

Google 備援電子郵件

Google 備援電子郵件

驗證備援電子郵件地址

請輸入系統傳送到 hardlims@hotmail.com 的 6 位數驗證碼。沒有收到相關電子郵件嗎？ 傳送新的驗證碼。

驗證碼

521916

6 / 6

取消　　驗證

Google 備援電子郵件

您的電子郵件地址已成為以下帳戶的備援電子郵件地址： mimicwang1978@gmail.com

Google <no-reply@accounts.google.com>
上午 12:18

收件者: hardlims@hotmail.com

這是系統針對 mimicwang1978@gmail.com 發出的安全性警示副本，而 hardlims@hotmail.com 是該帳戶的備援電子郵件地址。 如果您對這個帳戶沒有印象，請移除該帳戶。

Google

您的電子郵件地址已通過備援電子郵件地址驗證

mimicwang1978@gmail.com 現在使用您的電子郵件地址做為備援電子郵件地址。如果您對這個帳戶沒有印象，可以將自己的電子郵件地址從該帳戶移除。移除電子郵件地址

您也可以前往以下網址查看帳戶安全相關活動：
https://myaccount.google.com/notifications

您的 Google 帳戶和服務有重大異動，系統特此發送這封電子郵件通知您。

Google 使用您的手機登入帳戶

Google 使用您的手機登入帳戶

Google 使用您的手機登入帳戶

Google 使用您的手機登入帳戶

手機畫面

Google 使用您的手機登入帳戶

Google 使用您的手機登入帳戶

Google 使用您的手機登入帳戶

針對 mimicwang1978@gmail.com 發出的安全性警示

Google <no-reply@accounts.google.com>
上午 10:00

收件者: hardlims@hotmail.com

這是系統針對 mimicwang1978@gmail.com 發出的安全性警示副本，而 hardlims@hotmail.com 是該帳戶的備援電子郵件地址。 如果您對這個帳戶沒有印象，請移除該帳戶。

Google

Oppo R9s 上有新的登入活動

hd mimicwang1978@gmail.com

我們發現您的 Google 帳戶在 Oppo R9s 裝置上有新的登入活動。如果登入帳戶的是您本人，就不需要採取任何動作；如果不是，我們將協助您保護帳戶。

查看活動

您也可以前往以下網址查看帳戶安全相關活動：
https://myaccount.google.com/notifications

您的 Google 帳戶和服務有重大異動，系統特此發送這封電子郵件通知您。

© 2023 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Google 使用您的手機登入帳戶

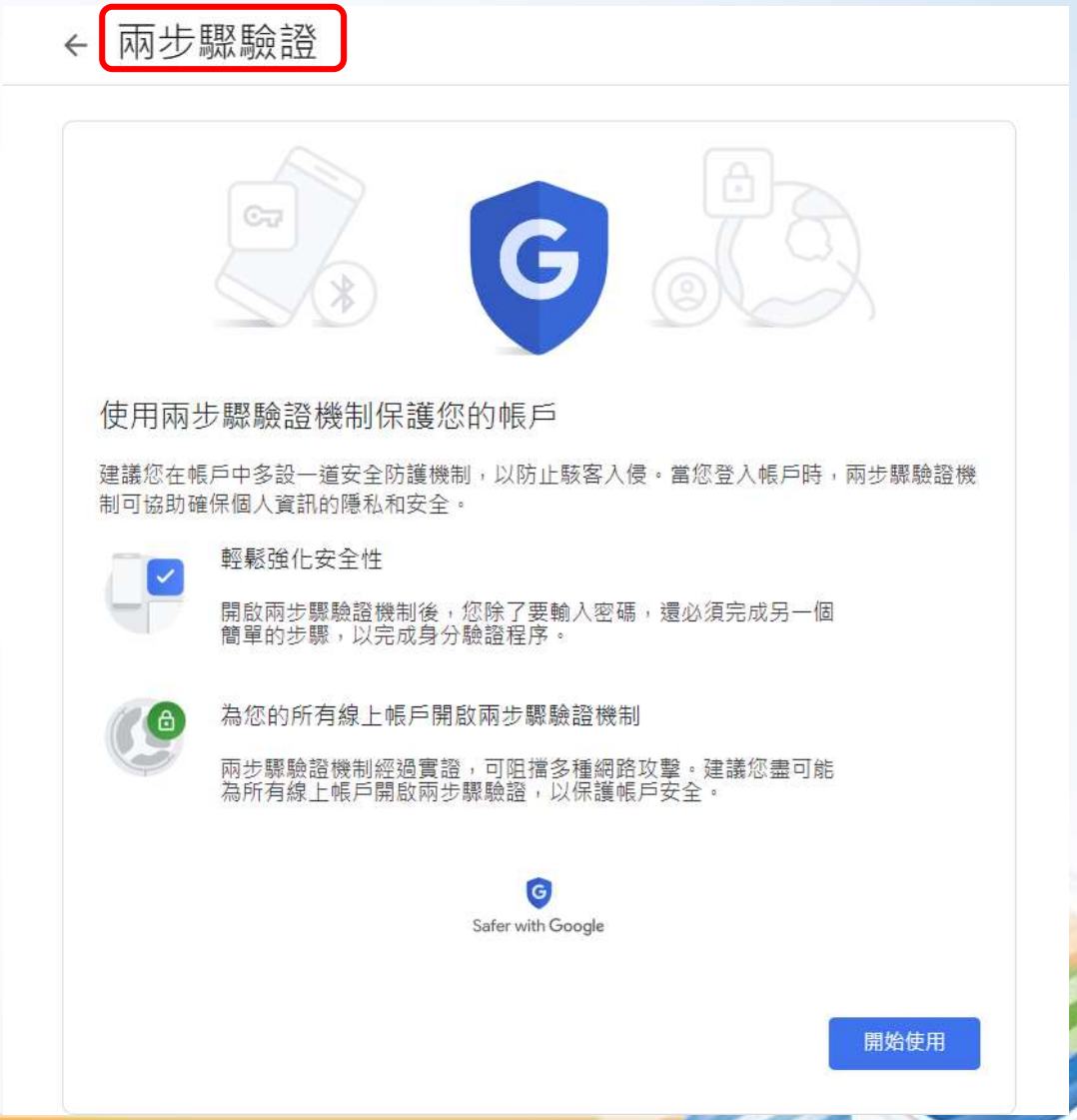
Google 使用您的手機登入帳戶

電腦畫面

手機畫面

Google 兩步驟驗證

MFA/2FA



Google 兩步驟驗證

MFA/2FA

Google 兩步驟驗證

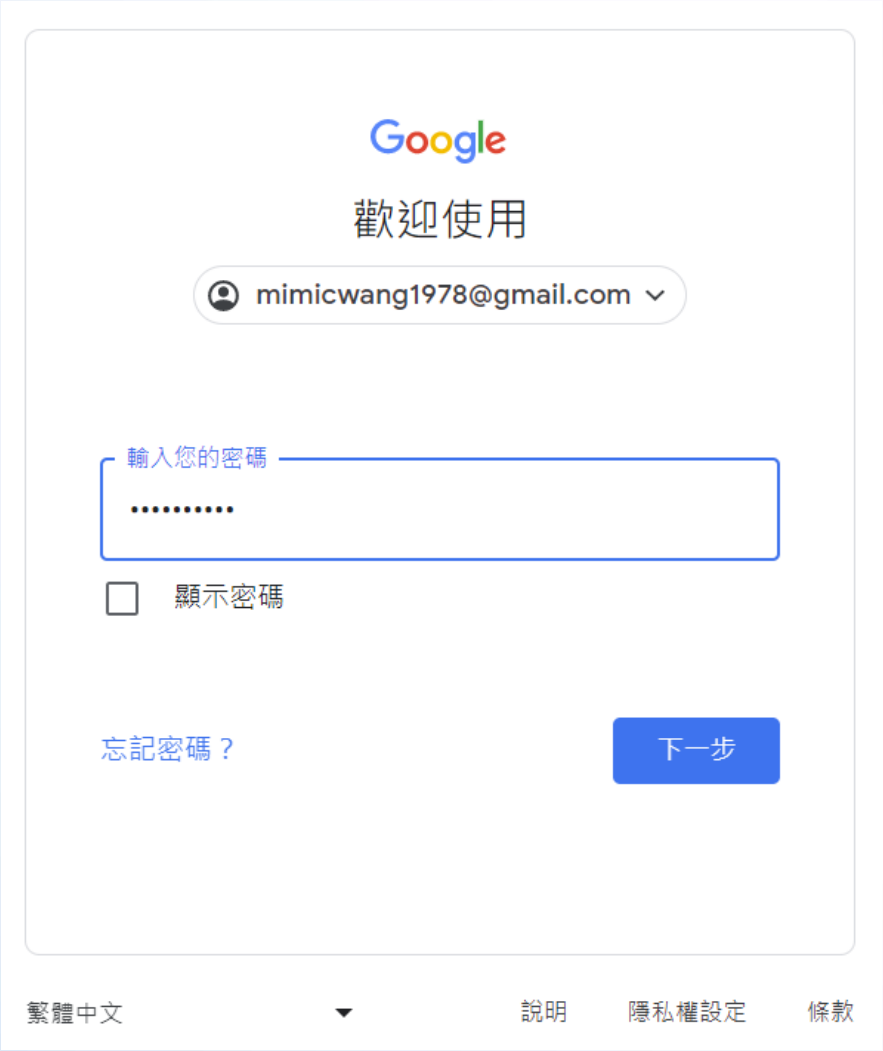
MFA/2FA

Google 兩步驟驗證

Google 兩步驟驗證

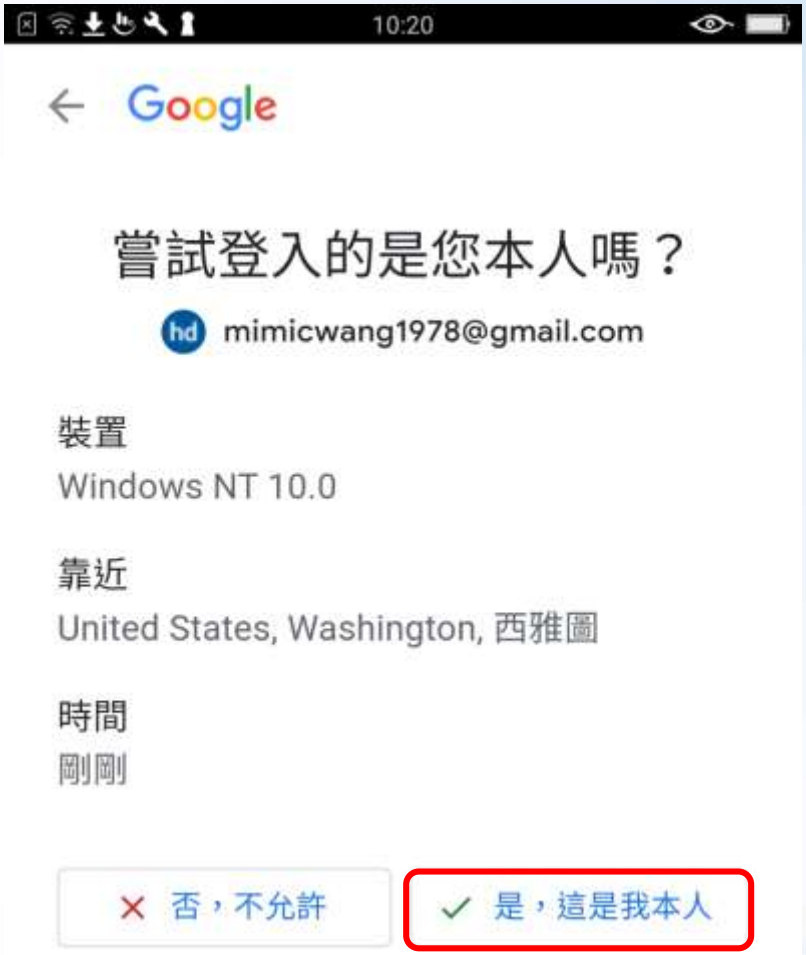
Google 兩步驟驗證

Google 兩步驟驗證



Google 兩步驟驗證

指紋或圖形驗證碼解鎖手機



Google 兩步驟驗證

Google 兩步驟驗證

MFA

多/雙因子認證MFA/2FA

Google

密碼

Something you know

手機

Something you have

生物辨識

指紋

臉部辨識

Something you are

圖形鎖/PIN

Something you know

Goole提示

手機簡訊

Google 兩步驟驗證

新增更多可驗證您身分的第二個步驟

建議您設定額外的備用步驟。這樣一來，即使其他選項無法使用，您仍可透過備用步驟順利登入帳戶。

備用碼

有了這種可列印的一次性通行碼，即使手機不在身邊 (例如差旅途中) 也能登入帳戶。 >

Authenticator 應用程式

您可以透過 Authenticator 應用程式取得免付費驗證碼，即使手機未連上網路也能使用。Android 和 iPhone 均適用。 >

安全金鑰

安全金鑰是一種驗證方式，讓您能夠安全登入帳戶。安全金鑰可分為手機內建的安全金鑰、藍牙安全金鑰，以及直接插入電腦 USB 連接埠的安全金鑰。 >

Google 兩步驟驗證

Google 兩步驟驗證

每組備用碼僅能
使用一次

Google 兩步驟驗證

Google 兩步驟驗證

Google 兩步驟驗證

Google 兩步驟驗證

新增更多可驗證您身分的第二個步驟

建議您設定額外的備用步驟。這樣一來，即使其他選項無法使用，您仍可透過備用步驟順利登入帳戶。

備用碼

有了這種可列印的一次性通行碼，即使手機不在身邊 (例如差旅途中) 也能登入帳戶。

Authenticator 應用程式

您可以透過 Authenticator 應用程式取得免付費驗證碼，即使手機未連上網路也能使用。Android 和 iPhone 均適用。

安全金鑰

安全金鑰是一種驗證方式，讓您能夠安全登入帳戶。安全金鑰可分為手機內建的安全金鑰、藍牙安全金鑰，以及直接插入電腦 USB 連接埠的安全金鑰。

Google 兩步驟驗證

← Authenticator 應用程式

您可以透過驗證器應用程式取得驗證碼，不用再等待驗證碼訊息。此外，即使手機未連上網路，也可以取得驗證碼。

首先，請前往 Google Play 商店或 iOS App Store 下載 Google Authenticator。

+ 設定驗證器

Google 兩步驟驗證

設定驗證器應用程式

- 開啟 Google Authenticator 應用程式並輕觸 [+]
- 選擇 [掃描 QR 圖碼]

無法掃描 QR 圖碼嗎？

Google 兩步驟驗證

Google 兩步驟驗證

Google

兩步驟驗證

為保護您的帳戶，Google 想確認是您本人正在嘗試登入

mimicwang1978@gmail.com

選擇您要使用的登入方式：

在手機或平板電腦上輕觸 [是]

使用手機或平板電腦取得安全碼 (即使離線也能取得)

從 **Google Authenticator** 應用程式取得驗證碼

透過以下電話號碼接收驗證碼：···· ··· ·23

需支付一般簡訊費用

無法在這個裝置上使用

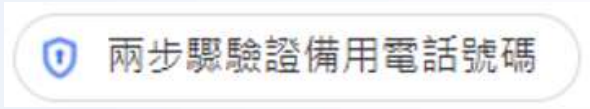
輸入您的任何一個 8 位數備用碼

或者試試看帳戶救援功能

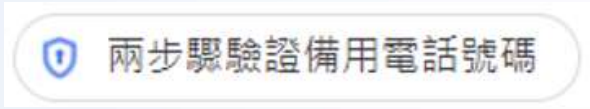
Google 兩步驟驗證

Google 兩步驟驗證

Google 兩步驟驗證



Google 兩步驟驗證



新增電話號碼

輸入手機號碼

- Google 會使用這個電話號碼協助您登入帳戶。如果您的帳戶有異常活動時，也會透過這個電話號碼向您示警。
- 請勿使用 Google Voice 號碼。
- 電信業者可能會向您收取費用。

進一步瞭解 Google 如何使用這項資訊

您要透過哪一種方式接收 Google 傳送的登入驗證碼？

傳送簡訊

取消　繼續

新增電話號碼

輸入手機號碼

0952 187 123

- Google 會使用這個電[redacted]助您登入帳戶。如果您的帳戶有異常活動時，也會透過這個電話號碼向您示警。
- 請勿使用 Google Voice 號碼。
- 電信業者可能會向您收取費用。

進一步瞭解 Google 如何使用這項資訊

您要透過哪一種方式接收 Google 傳送的登入驗證碼？

傳送簡訊

取消　繼續

Google 兩步驟驗證

兩步驟驗證備用電話號碼

← 兩步驟驗證電話號碼

以下號碼可接收登入驗證碼。您或許還可以使用其他號碼來進行 Google 帳戶救援程序。管理備援電話號碼

0952 [redacted]
已驗證
驗證碼會透過簡訊傳送

0952 [redacted]
驗證碼會透過簡訊傳送

驗證電話號碼

+ 新增兩步驟驗證備用電話號碼

驗證這個電話號碼

驗證碼將傳送到這個電話號碼

0952 [redacted]

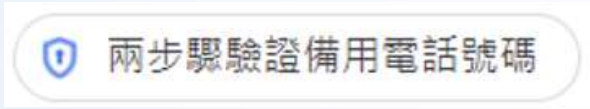
當您新增用於兩步驟驗證的電話號碼後，Google 會撥打電話或傳送訊息，以確認這是您的號碼。

- Google 會使用這個電話號碼協助您登入帳戶。如果您的帳戶有異常活動時，也會透過這個電話號碼向您示警。
- 請勿使用 Google Voice 號碼。
- 電信業者可能會向您收取費用。

進一步瞭解 Google 如何使用這項資訊

取消 繼續

Google 兩步驟驗證



驗證這個電話號碼

Google 已將驗證碼傳送到 0952 [redacted]。

輸入驗證碼

返回　　取消　驗證

驗證這個電話號碼

Google 已將驗證碼傳送到 0952 [redacted]。

輸入驗證碼

G-686212

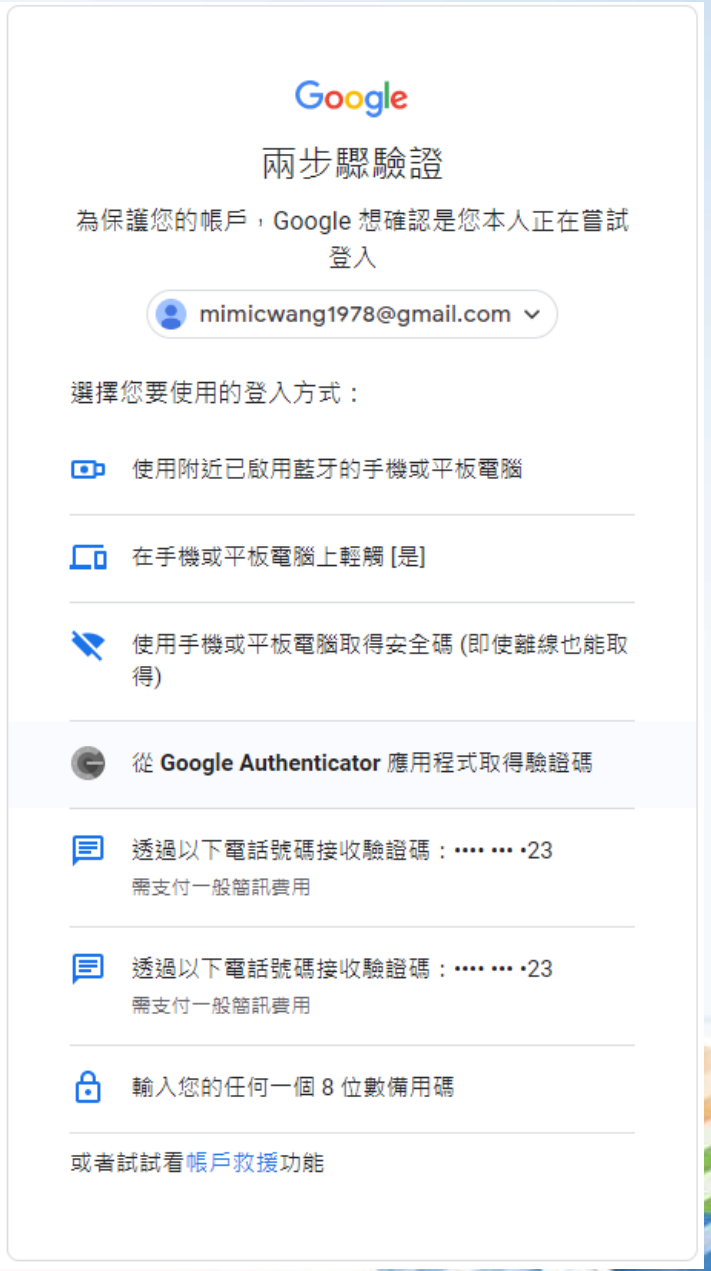
返回　　取消　驗證

Google 兩步驟驗證

Google 兩步驟驗證

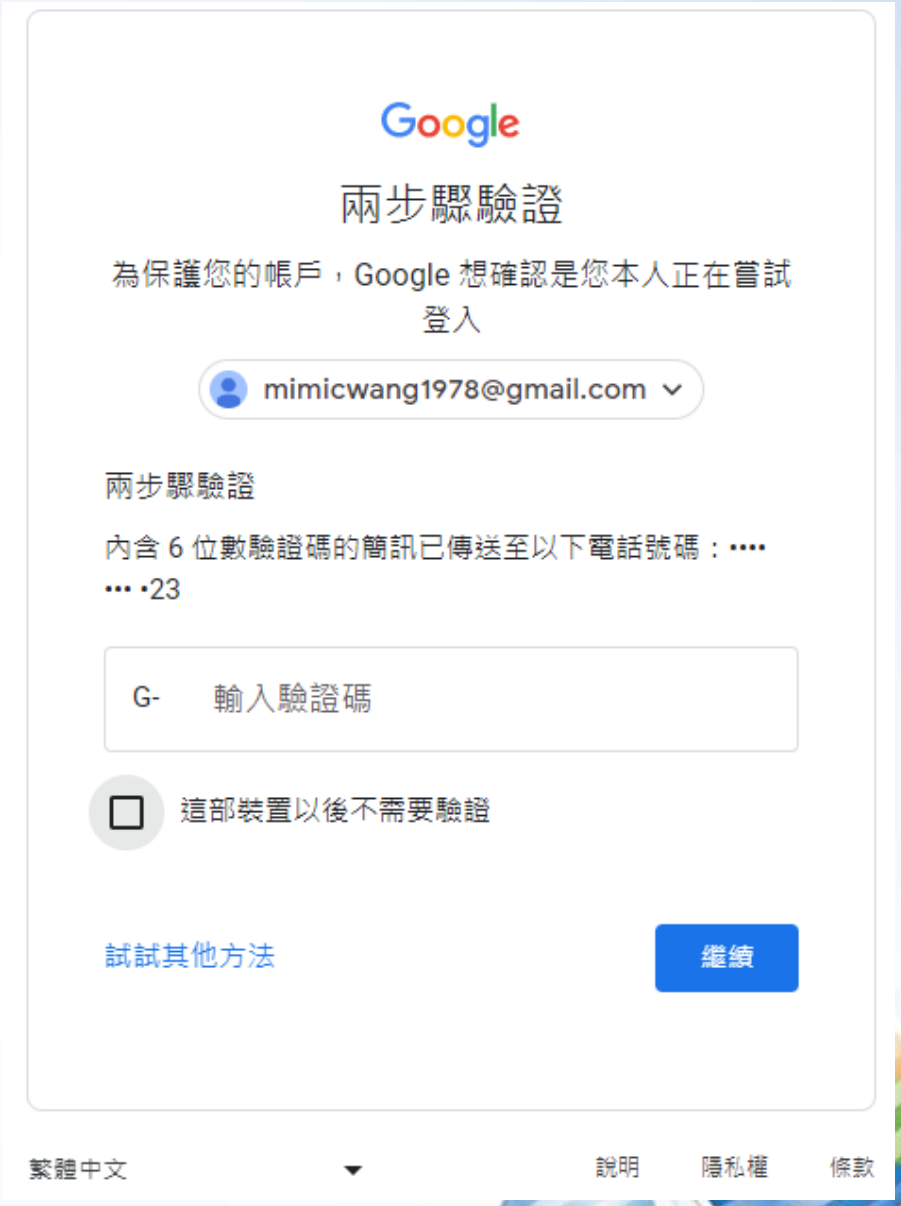
兩步驟驗證備用電話號碼

Google 兩步驟驗證



Google 兩步驟驗證

兩步驟驗證備用電話號碼



Google 兩步驟驗證

安全金鑰

Security key

USB

NFC

Bluetooth

cable

Source:https://cloud.google.com/titan-security-key?hl=zh-tw

Google 兩步驟驗證

安全金鑰

Google 兩步驟驗證

安全金鑰

USB Security Key

For use with your computer. You can also connect to your Android device that supports NFC.

Bluetooth Security Key

For use with iOS or Android devices. You can also use the cable to connect to your computer.

Google 兩步驟驗證

USB

Google 兩步驟驗證

安全金鑰

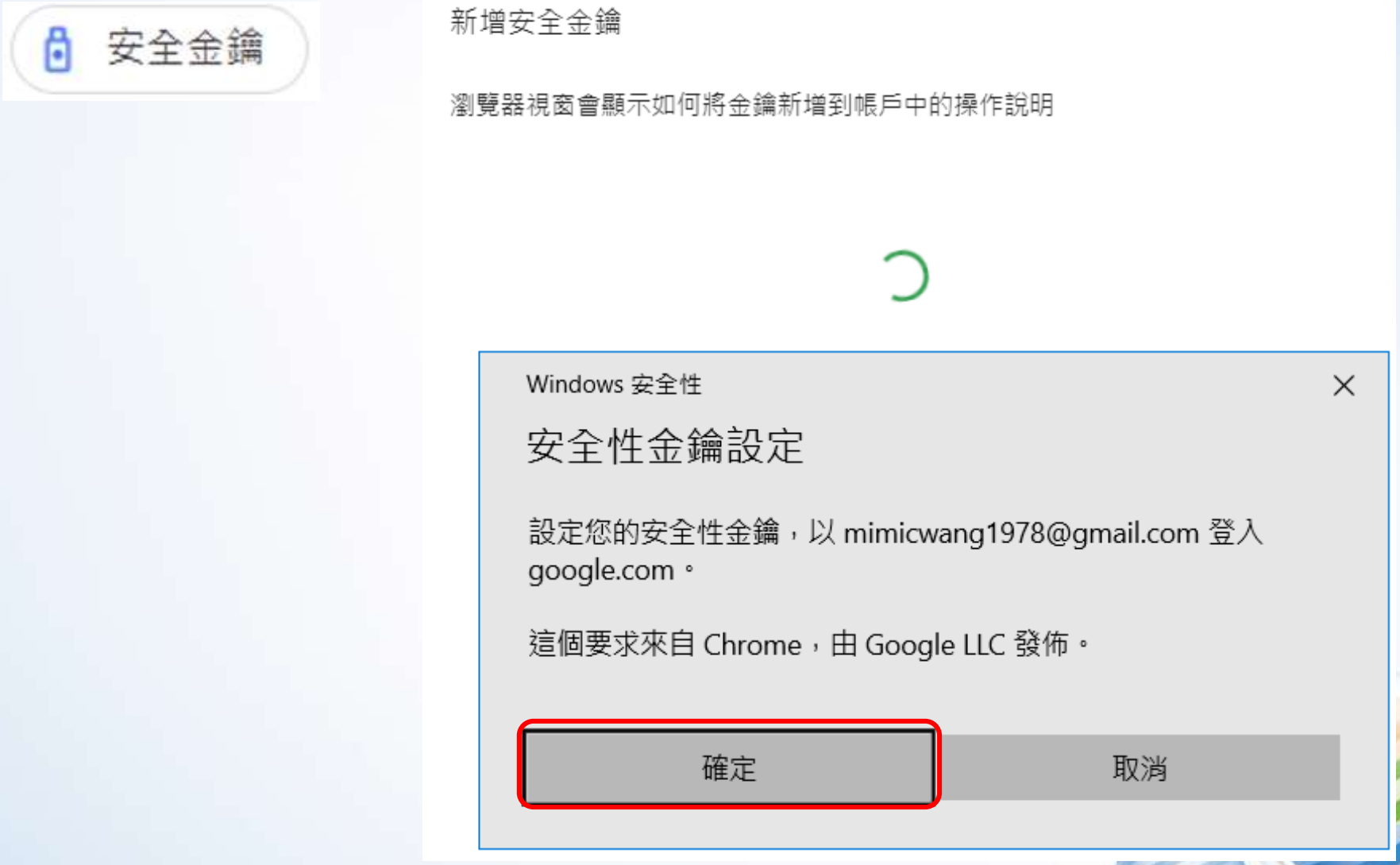
Security key

Google 兩步驟驗證

安全金鑰

Google 兩步驟驗證

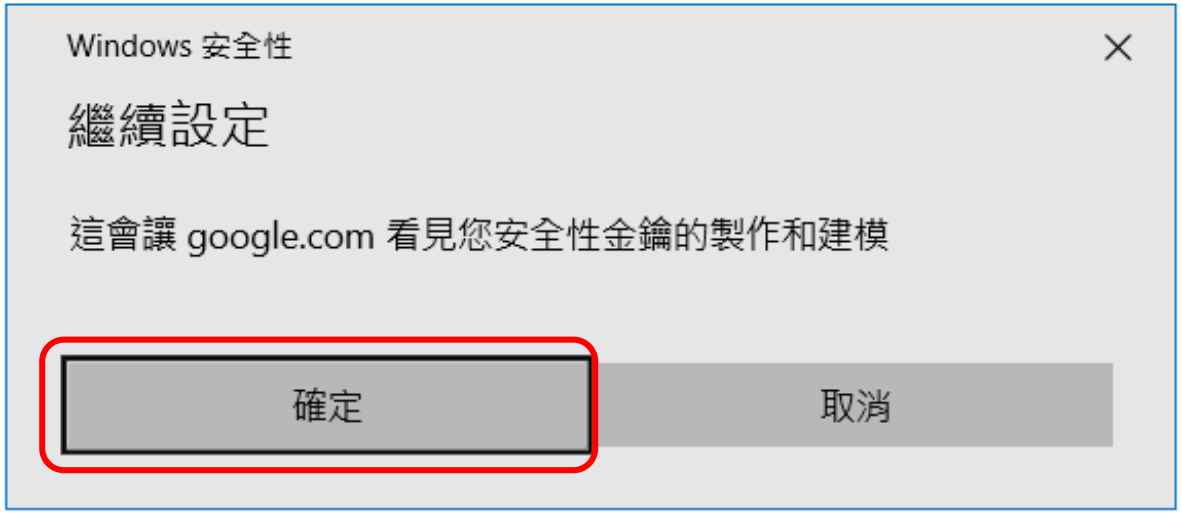
Google 兩步驟驗證



Google 兩步驟驗證

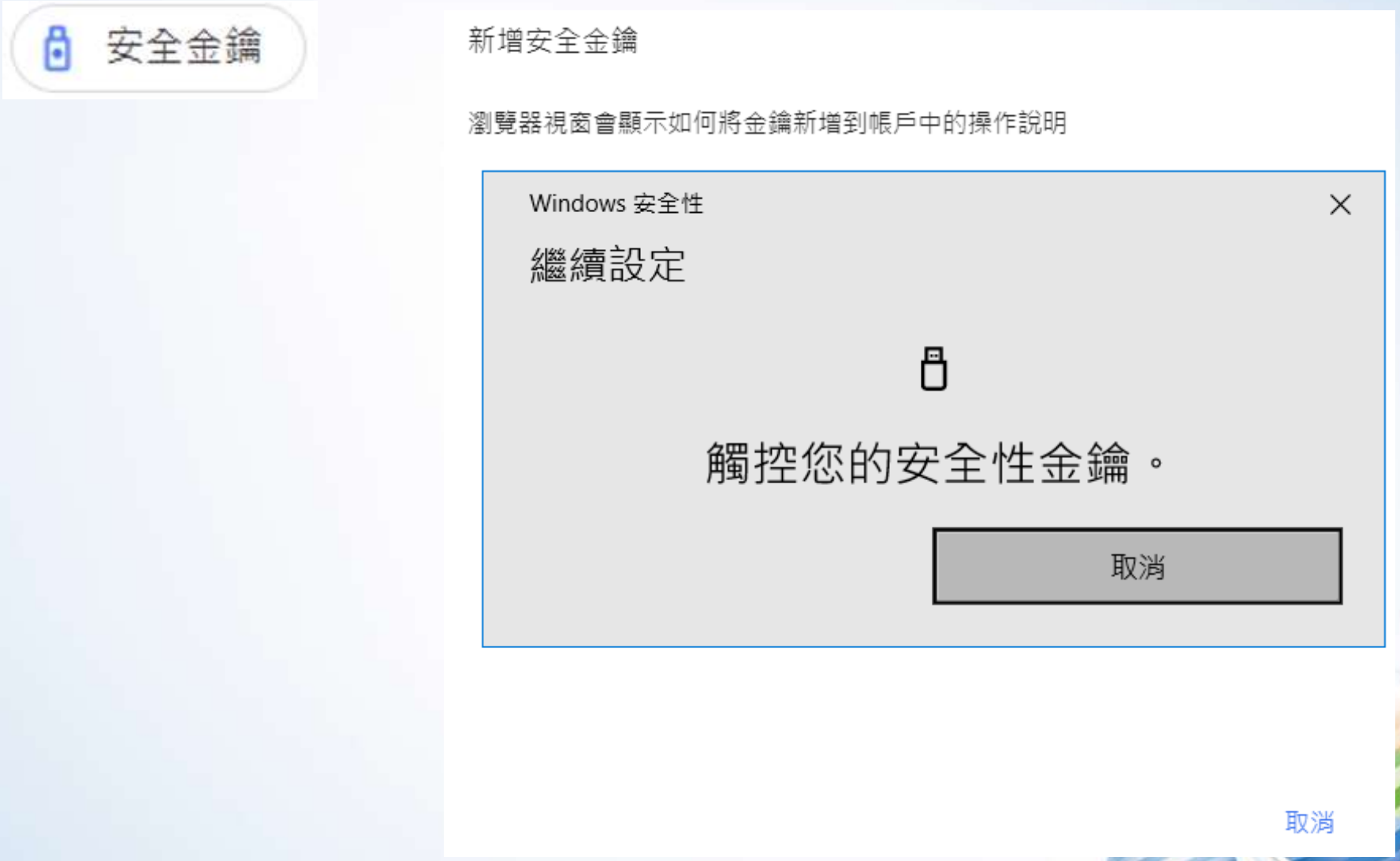
新增安全金鑰

瀏覽器視窗會顯示如何將金鑰新增到帳戶中的操作說明



取消

Google 兩步驟驗證



Google 兩步驟驗證

安全金鑰

為金鑰命名

請設定一個方便識別的金鑰名稱

安全金鑰名稱

0 / 20

繼續

為金鑰命名

請設定一個方便識別的金鑰名稱

mimicwang1978

長度上限為 20 個半形字元 13 / 20

繼續

Google 兩步驟驗證

已新增安全金鑰

您的帳戶已開啟兩步驟驗證，現在可以使用安全金鑰了。

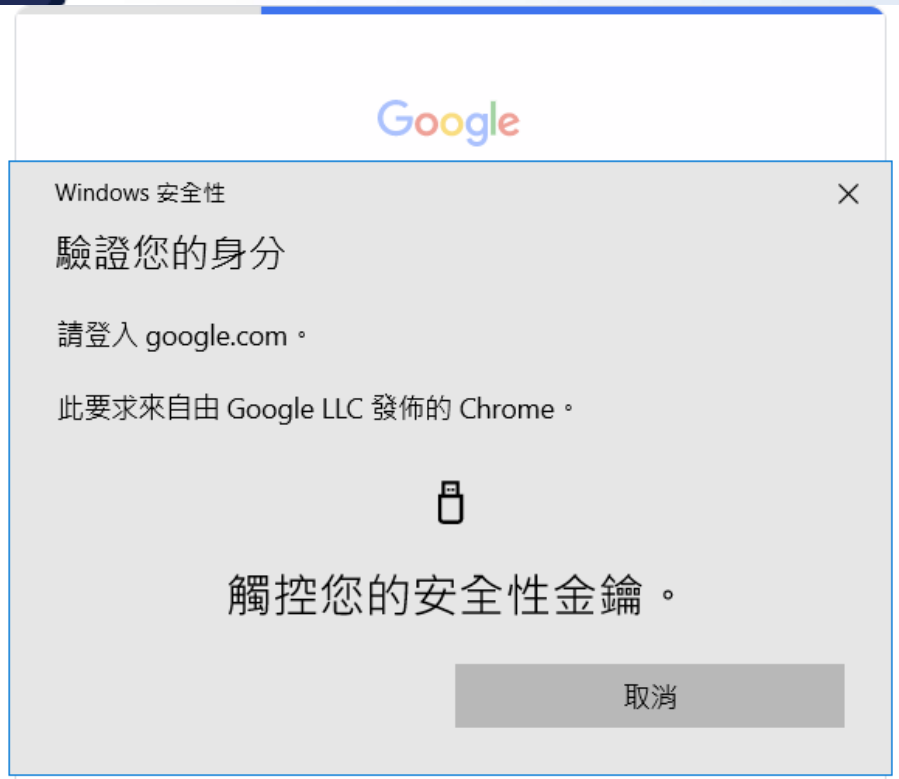
請隨身攜帶安全金鑰，確保您能隨時登入 Google 帳戶。

返回

繼續

Google 兩步驟驗證

Google 兩步驟驗證



Google 兩步驟驗證

安全金鑰

Google

兩步驟驗證

為保護您的帳戶，Google 想確認是您本人正在嘗試登入

mimicwang1978@gmail.com

大功告成

這部裝置以後不需要驗證

繼續

Google 兩步驟驗證

Google 兩步驟驗證

Google 兩步驟驗證

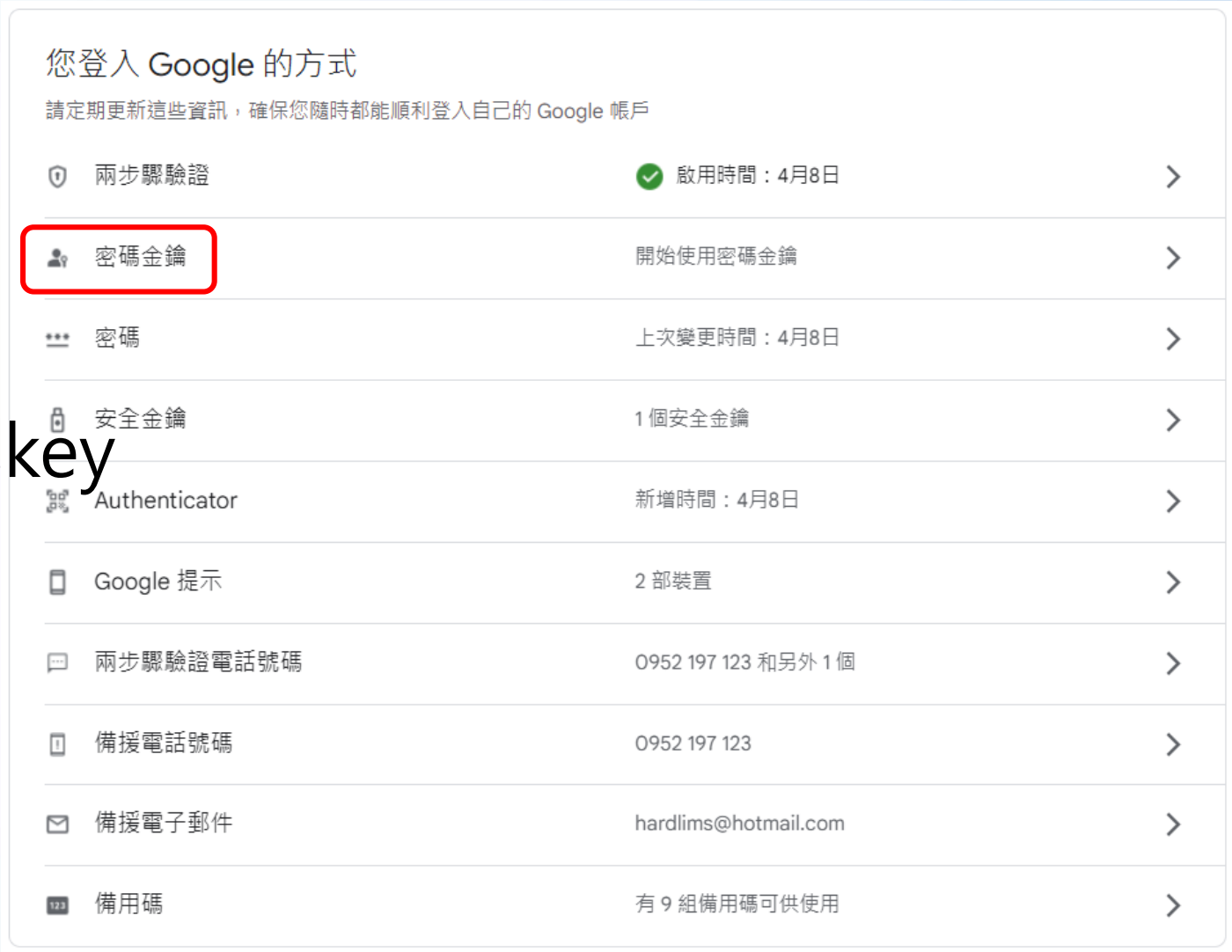
MFA


您登入 Google 的方式
請定期更新這些資訊，確保您隨時都能順利登入自己的 Google 帳戶
兩步驟驗證
啟用時間：4月8日
密碼
上次變更時間：4月8日
安全金鑰
1 個安全金鑰
Authenticator
新增時間：4月8日
Google 提示
2 部裝置
兩步驟驗證電話號碼
0952 和另外 1 個
備援電話號碼
0952
備援電子郵件
hardlims@hotmail.com
備用碼
有 9 組備用碼可供使用

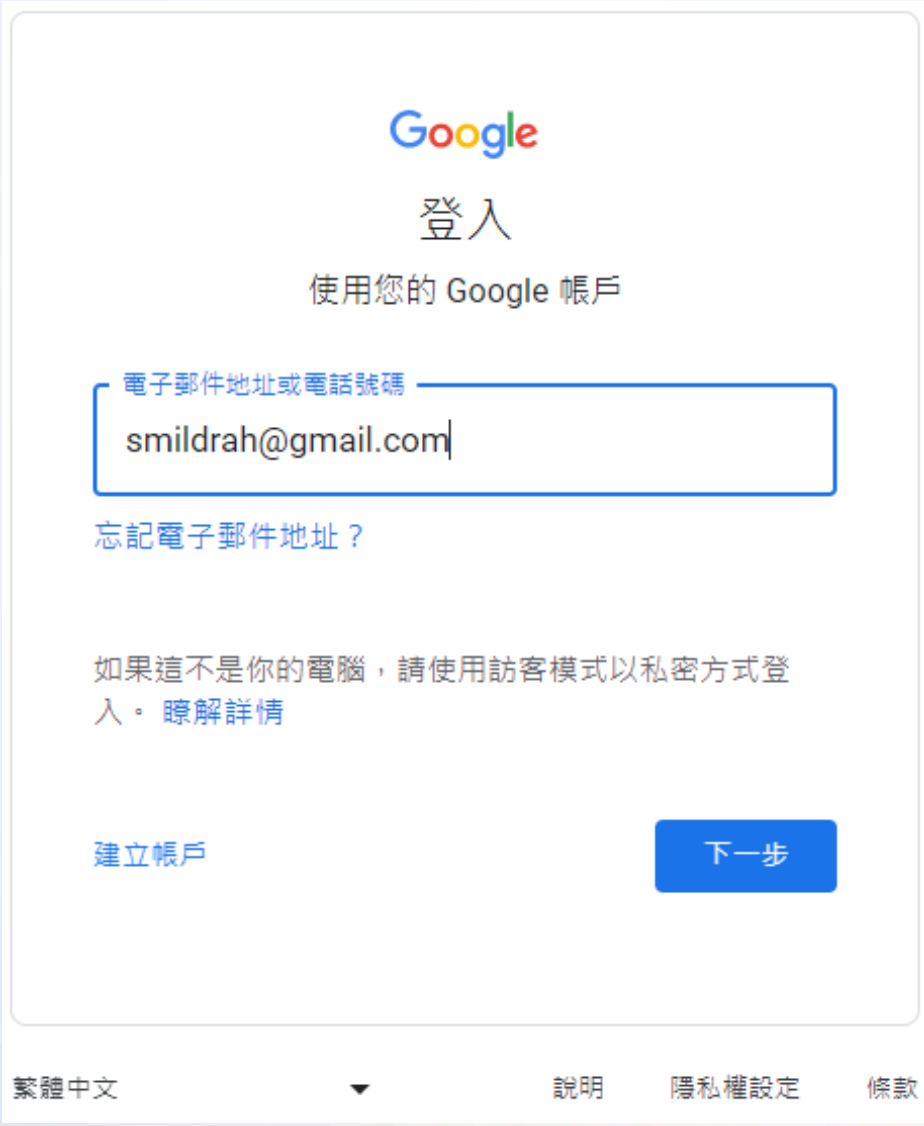
2023年5月開始.....

Google 開始支援 Passkey

傳說中的Passkey出現了~

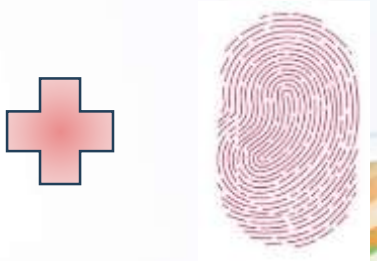


Google passkey



Google passkey

Google passkey



Google passkey

Binance MFA

BINANCE

歡迎回來！

s****@gmail.com

密碼

••••••••••••

登錄

忘記密碼？

Binance MFA

BINANCE

安全驗證

電子郵件驗證碼

取得驗證碼

輸入發送給 smi***@gmail.com 的 6 位數代碼

手機號碼驗證碼

取得驗證碼

輸入發送給 952* 的 6 位數代碼

提交

安全驗證不可用？

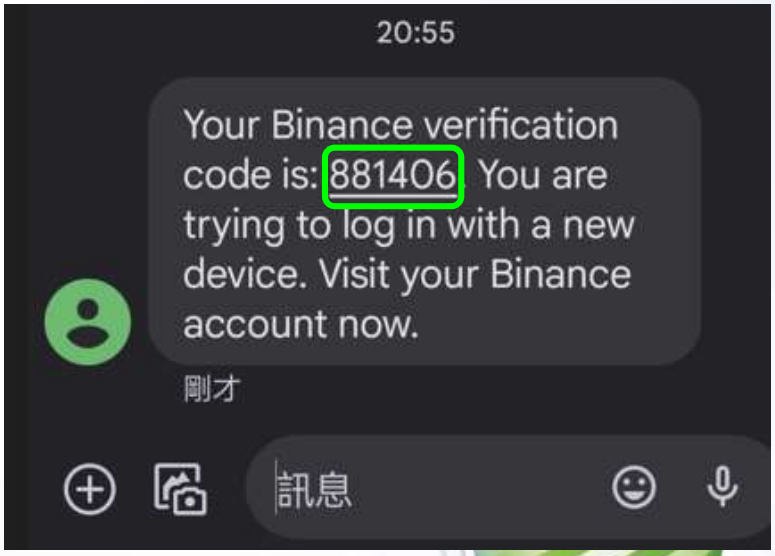
Binance MFA


BINANCE
短信驗證碼已發送。請檢查。
安全驗證
電子郵件驗證碼
驗證碼已傳送
輸入發送給 smi***@gmail.com 的 6 位數代碼
手機號碼驗證碼
驗證碼已傳送
輸入發送給 952 的 6 位數代碼
提交
安全驗證不可用？

Binance MFA

電子郵件驗證碼

手機號碼驗證碼



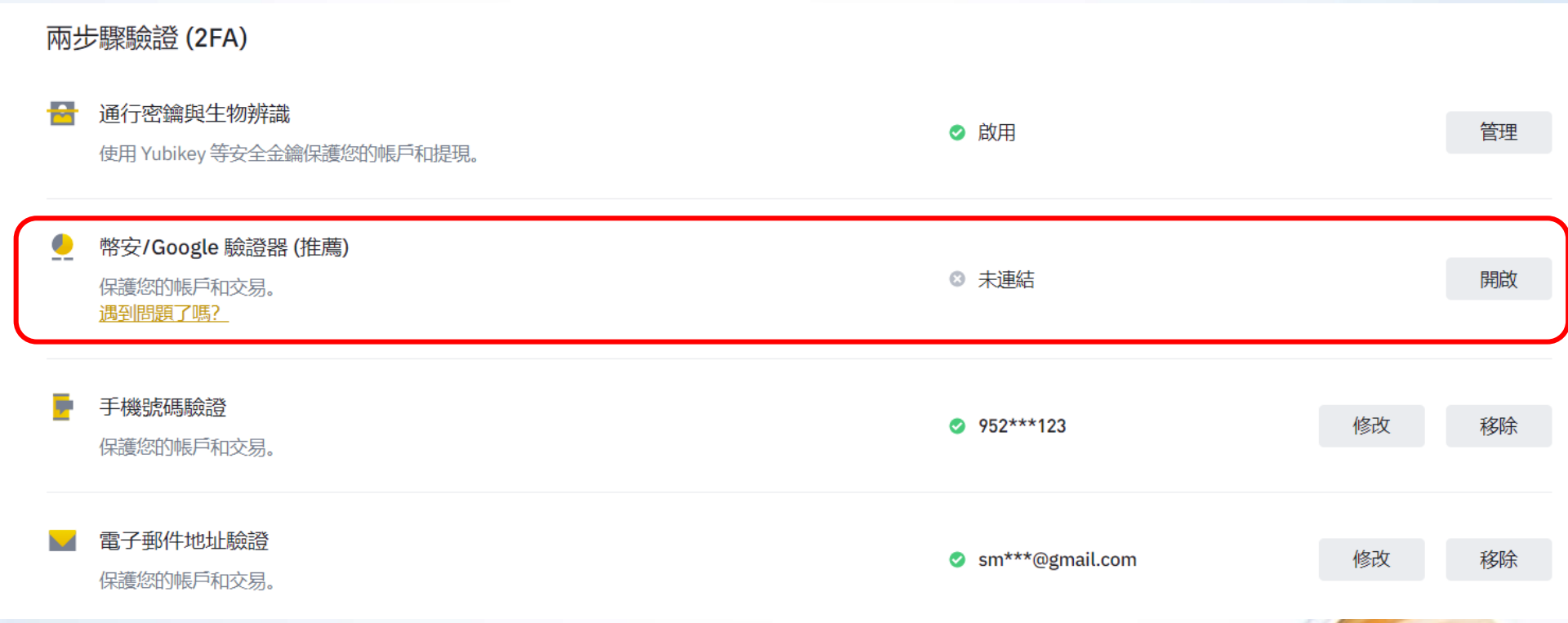
Binance MFA


BINANCE
安全驗證
電子郵件驗證碼
425749
重新發送代碼
輸入發送給 smi***@gmail.com 的 6 位數代碼
手機號碼驗證碼
881406
重新發送代碼
輸入發送給 952 的 6 位數代碼
提交
安全驗證不可用？

Binance MFA


BINANCE
買幣 TWD
市場
交易
衍生品
理財
金融業務
NFT
機構
廣場
總覽
賬戶安全
身份證明
支付方式
返佣
卡券中心
任務中心
API管理
子賬戶
設定
Anonymous-User-f1139
個人
用户ID
用戶類型
Twitter
未連結
上次登錄時間
2023-04-17 20:54:49(185.213.82.164)
今年復活節推薦好友，分享高達 10,000 USDT!
立即領取
總資產估值
充值
提現
購買加密貨幣
41064 BTC
≈ $

Binance MFA


兩步驟驗證 (2FA)
通行密鑰與生物辨識
使用 Yubikey 等安全金鑰保護您的帳戶和提現。
啟用
管理
幣安/Google 驗證器 (推薦)
保護您的帳戶和交易。
遇到問題了嗎?
未連結
開啟
手機號碼驗證
保護您的帳戶和交易。
952***123
修改
移除
電子郵件地址驗證
保護您的帳戶和交易。
sm***@gmail.com
修改
移除

Binance MFA


啟用幣安/Google 驗證器
1 下載App
2 掃描二維碼
3 備份密鑰
4 啟用幣安/Google 驗證器
5 去完成
驗證您的帳戶以啟用驗證器
手機號碼驗證碼
取得驗證碼
輸入發送給 952** 的 6 位數代碼
電子郵件驗證碼
取得驗證碼
輸入發送給 smi***@gmail.com 的 6 位數代碼
驗證碼
請輸入來自幣安/Google 驗證器的 6 位數驗證碼
安全驗證不可用？
上一步
下一步

Binance MFA


‹ 賬戶安全
啟用幣安/Google 驗證器
1
下載App
2
掃描二維碼
3
備份密鑰
4
啟用幣安/Google 驗證器
5
去完成
驗證器已啟用
您已成功啟用驗證器來保護您的帳戶。
回到安全頁面

Binance MFA


兩步驟驗證 (2FA)
通行密鑰與生物辨識
使用 Yubikey 等安全金鑰保護您的帳戶和提現。
啟用
管理
幣安/Google 驗證器 (推薦)
保護您的帳戶和交易。
遇到問題了嗎?
啟用
修改
移除
手機號碼驗證
保護您的帳戶和交易。
952
修改
移除
電子郵件地址驗證
保護您的帳戶和交易。
sm***@gmail.com
修改
移除

Binance MFA

Binance MFA


BINANCE
安全驗證
驗證碼
請輸入來自幣安/Google 驗證器的 6 位數驗證碼
切換至其他驗證方法
提交
安全驗證不可用？

Binance MFA

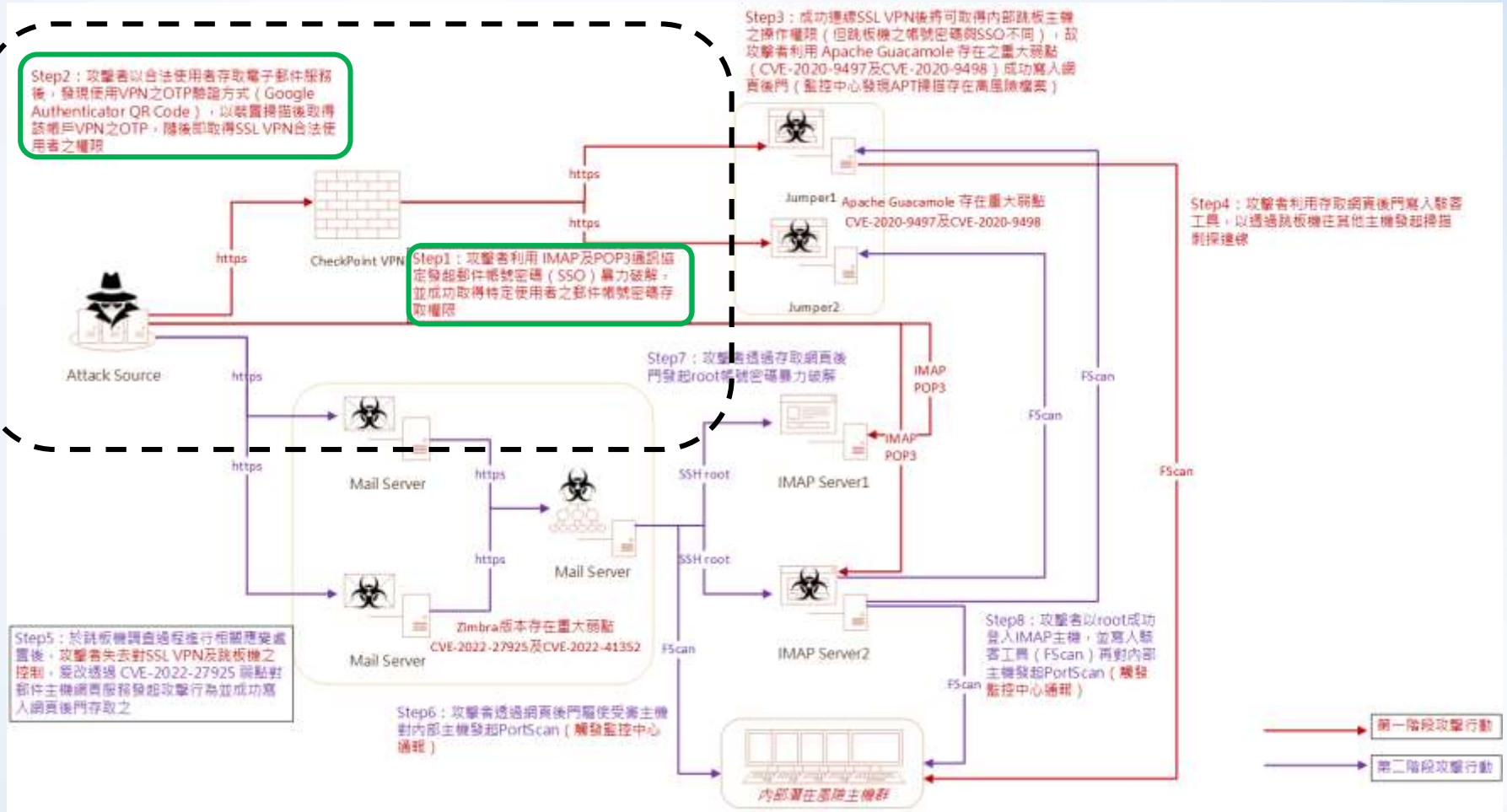

安全驗證
驗證碼
請輸入來自幣安/Google 驗證器的 6 位
切換至其他驗證方法
安全驗證不可用？
選擇驗證器
電子郵件地址驗證
手機號碼驗證

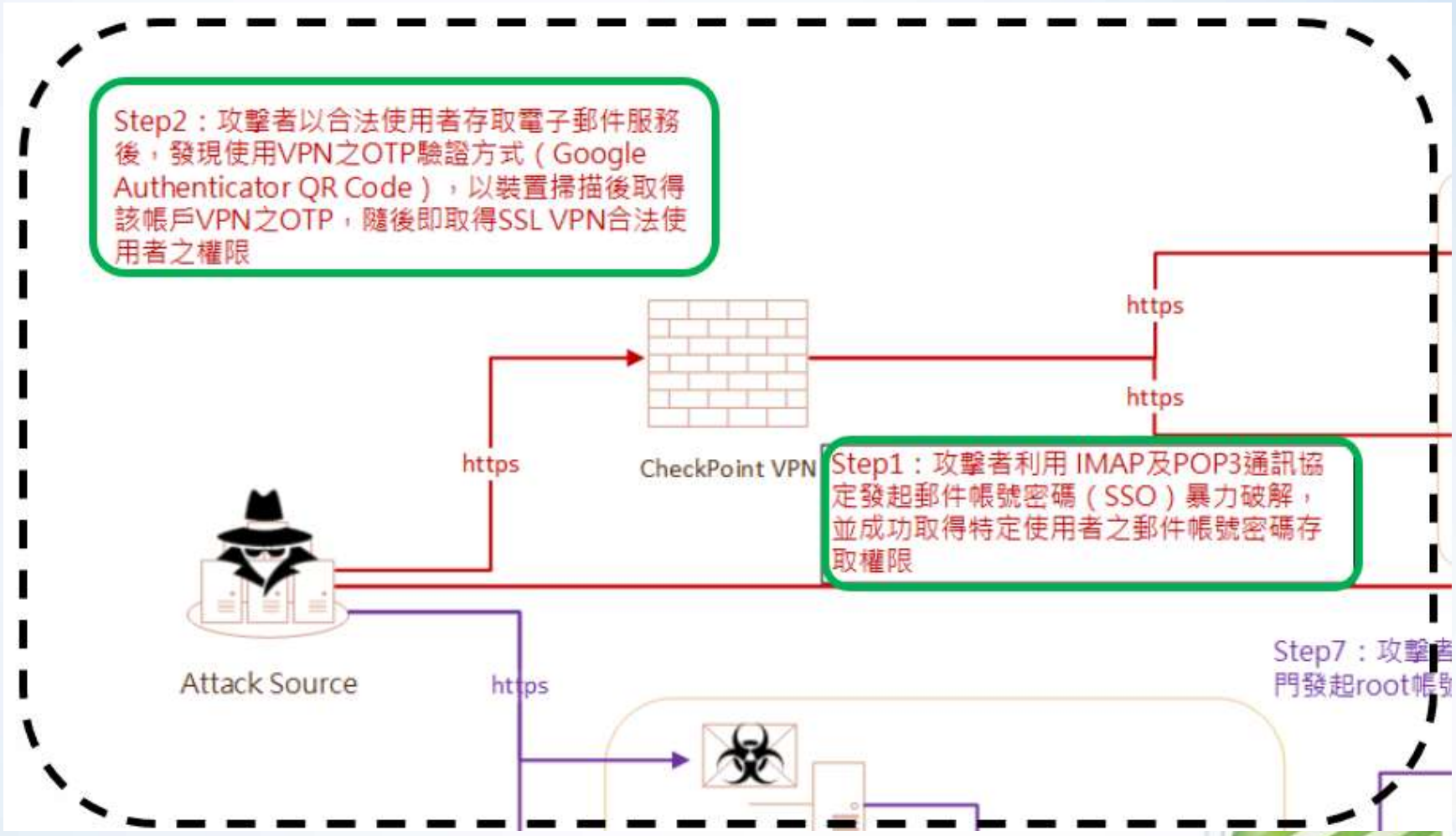
永遠走在最前面
Always Ahead

實際攻擊案例分享

中華電信
Chunghwa Telecom

實際攻擊案例一、
VPN多因素認證繞過


Step3：成功連線SSL VPN後將可取得內部跳板主機之操作權限（但跳板機之帳號密碼與SSO不同），故攻擊者利用 Apache Guacamole 存在之重大弱點（CVE-2020-9497及CVE-2020-9498）成功寫入網頁後門（監控中心發現APT掃描存在高風險檔案）
Step2：攻擊者以合法使用者存取電子郵件服務後，發現使用VPN之OTP驗證方式（Google Authenticator QR Code），以裝置掃描後取得該帳戶VPN之OTP，隨後即取得SSL VPN合法使用者之權限
Step1：攻擊者利用 IMAP及POP3通訊協定發起郵件帳號密碼（SSO）暴力破解，並成功取得特定使用者之郵件帳號密碼存取權限
Step4：攻擊者利用存取網頁後門寫入駭客工具，以透過跳板機往其他主機發起掃描與探測連線
Step5：於跳板機調查過程進行相關惡意處置後，攻擊者失去對SSL VPN及跳板機之控制，爰改透過 CVE-2022-27925 弱點對郵件主機網頁服務發起攻擊行為並成功寫入網頁後門存取之
Step6：攻擊者透過網頁後門層使受害主機對內部主機發起PortScan（觸發監控中心通報）
Step7：攻擊者透過存取網頁後門發起root帳號密碼暴力破解
Step8：攻擊者以root成功登入IMAP主機，並寫入駭客工具（FScan）再對內部主機發起PortScan（觸發監控中心通報）
Jumper1
Jumper2
Apache Guacamole 存在重大弱點
CVE-2020-9497及CVE-2020-9498
CheckPoint VPN
Attack Source
Mail Server
Mail Server
Mail Server
Zimbra版本存在重大弱點
CVE-2022-27925及CVE-2022-41352
IMAP Server1
IMAP Server2
內部署在雲端主機群
https
SSH root
IMAP
POP3
FScan
第一階段攻擊行動
第二階段攻擊行動


Step2：攻擊者以合法使用者存取電子郵件服務後，發現使用VPN之OTP驗證方式（Google Authenticator QR Code），以裝置掃描後取得該帳戶VPN之OTP，隨後即取得SSL VPN合法使用者之權限
https
https
https
CheckPoint VPN
Step1：攻擊者利用 IMAP及POP3通訊協定發起郵件帳號密碼（SSO）暴力破解，並成功取得特定使用者之郵件帳號密碼存取權限
Attack Source
https
Step7：攻擊者
門發起root帳號

實際攻擊案例一、VPN多因素認證繞過

alice@a.com

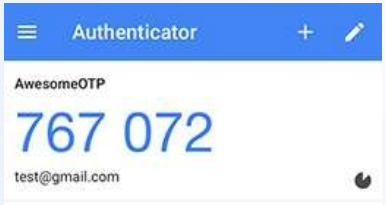
andy@a.com

tony@a.com

密碼暴力破解

A公司

alice信箱發現
Google authenticator



Username
Username alice
Password
Password Aa@123456

Username
Username alice
Password
Password Aa@123456

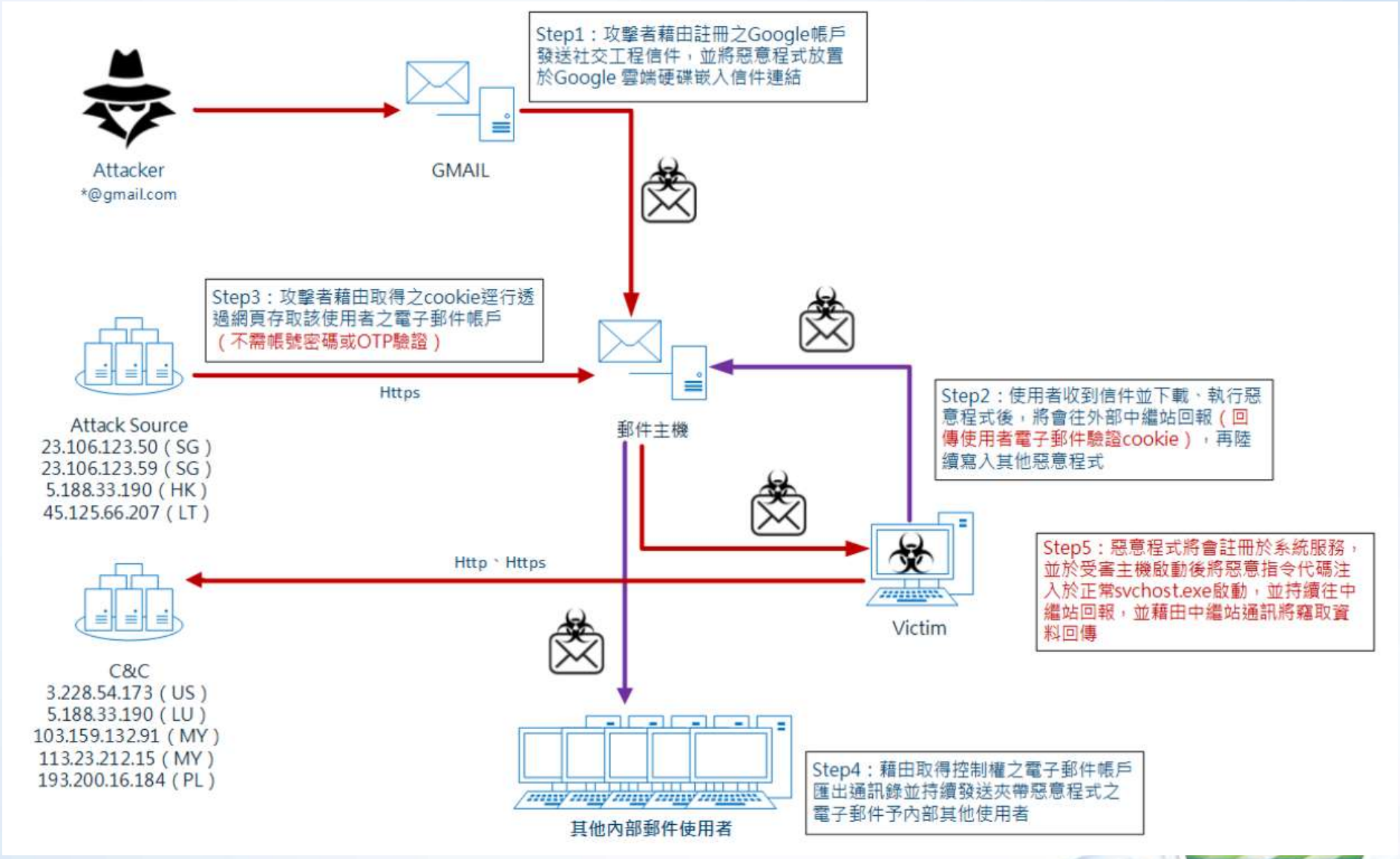
從 Google Authenticator 應用程式取得驗證碼
輸入安全碼 767072

成功透過VPN
進入A公司

入侵關鍵點

- 多因子認證QR Code應妥善保存
- 多因子認證機制應限定單一裝置綁定/限制綁定來源
- 密碼強度不足
- 密碼共用(郵件帳密=VPN帳密)

實際攻擊案例二、
WebMail多因素認證繞過


Step1：攻擊者藉由註冊之Google帳戶發送社交工程信件，並將惡意程式放置於Google 雲端硬碟嵌入信件連結
Attacker
*@gmail.com
GMAIL
Step3：攻擊者藉由取得之cookie逕行透過網頁存取該使用者之電子郵件帳戶（不需帳號密碼或OTP驗證）
Https
Attack Source
23.106.123.50 (SG)
23.106.123.59 (SG)
5.188.33.190 (HK)
45.125.66.207 (LT)
郵件主機
Step2：使用者收到信件並下載、執行惡意程式後，將會往外部中繼站回報（回傳使用者電子郵件驗證cookie），再陸續寫入其他惡意程式
Http、Https
Step5：惡意程式將會註冊於系統服務，並於受害主機啟動後將惡意指令代碼注入於正常svchost.exe啟動，並持續往中繼站回報，並藉由中繼站通訊將竊取資料回傳
Victim
C&C
3.228.54.173 (US)
5.188.33.190 (LU)
103.159.132.91 (MY)
113.23.212.15 (MY)
193.200.16.184 (PL)
Step4：藉由取得控制權之電子郵件帳戶匯出通訊錄並持續發送夾帶惡意程式之電子郵件予內部其他使用者
其他內部郵件使用者

實際攻擊案例二、WebMail多因素認證繞過

惡意連結(google drive)

Gmail

Username

Username

Password

Password

從 Google Authenticator 應用程式取得驗證碼

輸入安全碼

透過cookie直接繞過雙因子認證，
成功登入andy的WebMail

A公司

Andy
點擊社交信件

電子郵件驗證cookie

透過Andy信箱，寄送
釣魚信件給內部同仁

入侵關鍵點

- 人員資安意識薄弱，點擊釣魚信件
- 前端網頁登入的驗證機制(Cookie)時效過長

實際攻擊案例三、
假網站釣魚信件多因素認證繞過

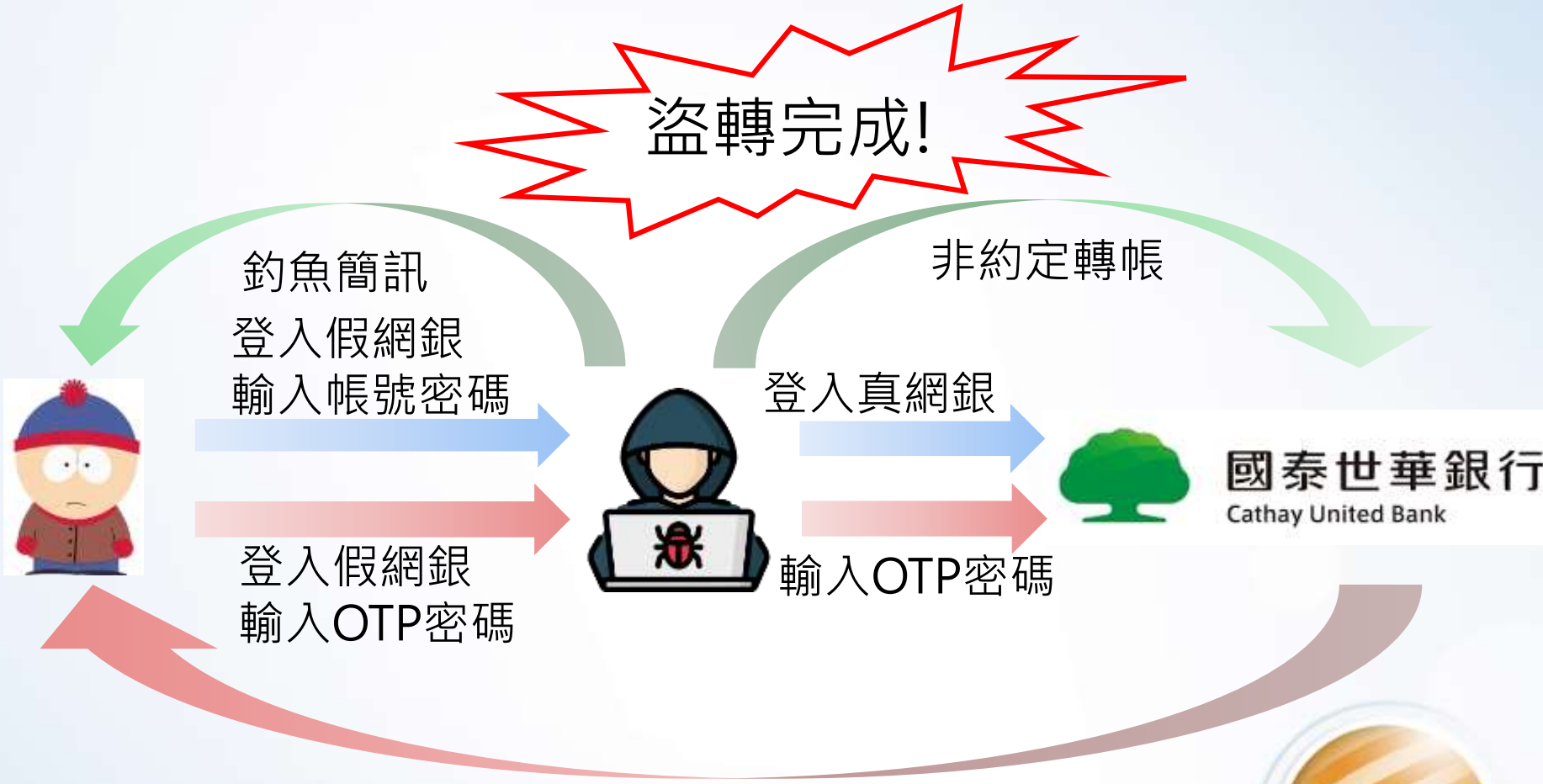
ithome.com.tw
https://www.ithome.com.tw › news

假冒銀行釣魚簡訊詐騙規模擴大，繼國泰世華 - iThome

2021年2月9日 — 最近半個多月來，國內多家金融機關與刑事警察局都發出慎防釣魚網站的警告，因為有網路犯罪集團接連假冒國泰世華、台新銀行名義發送大量釣魚簡訊，誤導民眾 ...


TVBS新聞台 HD
掃描訂閱TVBS NEWS
假冒國泰世華釣魚簡訊 3天21人被騙300萬
掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道

國泰世華網銀盜轉案



雙因子認證
OTP 簡訊認證碼

入侵關鍵點

- 社交工程信件防範

實際攻擊案例四、
社交工程資料庫成熟應用(雙因素認證繞過)

yahoo.com

https://tw.tech.yahoo.com › news › 34卡友遭盜刷百...

34卡友遭盜刷百萬！ 永豐銀：爭議款不必繳 - Yahoo奇摩新聞

2023年1月31日 — 春節期間，很多卡友反映永豐銀信用卡被盜刷，金管會今天(31日)最新公布，一共有34名受害者，盜刷金額達到110萬，初步調查用途都是在國外網路商店買 ...


TVBS新聞台 HD
TVBS
34卡友遭盜刷百萬 永豐銀:爭議款不必繳
掌握新聞脈動 ▶ 訂閱TVBS NEWS頻道

永豐銀盜刷案

受害者收到手機簡訊與電子郵件OTP密碼，卻不曉得發生何事?

因為付款授權頁面在駭客螢幕前

取得OTP認證碼完成盜刷!

電子郵件

手機簡訊

社交工程資料庫成熟應用

個人/企業敏感性資料

中華民國內政部 MINISTRY OF THE INTERIOR, R.O.C. (TAIWAN)

中華航空 CHINA AIRLINES

微風 Breeze

iRent

UBike 微笑單車

數據分析與資料組合將
產生更多**新的攻擊手法**

大量的個資外洩.....

永豐銀盜刷案


盜刷完成!
取得OTP密碼
信用卡
網路消費
輸入OTP密碼
永豐銀行
Bank SinoPac
OTP 認證碼
簡訊+Email

入侵關鍵點

- 電子郵件信箱密碼遭竊
- 帳號密碼共用
- 個資與機敏資料外洩
- 社交工程資料庫成熟應用

永遠走在最前面
Always Ahead

日常作業應注意事項

中華電信
Chunghwa Telecom

人員安全：遇見不明人士，要進行盤查

若遇不明人士在辦公區域內走動，應主動詢問其來意；發現可疑狀況應加以制止，或通知相關人員處理。

即使是認識之同仁，進出其沒有權限出入之區域，也要加以勸阻或通知相關人員處理。

資料安全：桌面與螢幕淨空

- 實體資料
  - 因處理業務保有敏感性、機密性電腦資料或檔案者，應加強安全保護措施，如下班時應該上鎖或以其他方法妥為收存。
  - 不再使用之機密文書資料：碎紙設備或其他無法還原原始資料之銷毀方式進行銷毀。
- 數位資料
  - 將資料直接儲存在電腦桌面上，很容易導致資料的外洩。

螢幕鎖屏快捷鍵【Win+L】&【Ctrl+Alt+Del】

資料安全：重要資料備份

- 不論是紙本或電子檔的重要資料，皆應：
  - 定期備份
  - 存放在不同地方(異地備份)。
- 資料備份原則
  - 資料價值較高時應優先備份。
  - 選擇適合之儲存媒介進行資料備份工作。
  - 按所欲備份的資料型態，選擇方法進行備份(如：完全備份、選擇性備份、增量備份)。
  - 備份的資料需定期做資料回復測試，確認備份資料的可用性。

資料安全：檔案傳輸

1. 電子方式傳送機密資料應加密。
2. 應確認對方的郵件地址，不要隨意轉寄未確認來源之信件。
3. 非必要或未經授權，不得將文件攜出。
4. 機密文件以人工傳遞需妥善保護，如：專人親送、密封。

資料傳輸安全控管(1/3)

政策面

管理面

技術面

- 訂定網路通訊、資訊設備及電腦病毒管理等程序書，並要求同仁遵守。
- 訂定電子郵件及使用者資訊設備安全等程序書，並要求同仁遵守。
- 禁止同仁將業務機敏資料上傳到個人雲端空間。
- 禁止同仁私架無線網路分享器或電子郵件伺服器。

資料傳輸安全控管(2/3)

政策面

管理面

技術面

- 接收資料前確認是否為相關業務資料；傳送資料前應確認內容是否正確。
- 收到不明的郵件不要隨意開啟附件及超連結、檔案或軟體。
- 避免使用免費的公用無線網路進行機敏資料傳輸。
- 傳送業務機敏資料須採取加密機制。
- 有連線外部網路進行檔案傳輸需求時，因公務需使用，必須申請並經由核准後使用。
- 定期檢視防火牆稽核軌跡，確認是否有異常傳輸的事件發生。

資料傳輸安全控管(3/3)

政策面

管理面

技術面

- 個人電腦與行動裝置應安裝防毒軟體，且保持在最新版本。
- 藉由SPAM機制過濾垃圾郵件。
- 防火牆及資安設備安全性更新時，經測試無誤後應盡速更新。
- 採取FTP傳輸時，禁止使用匿名登入，且FTP須有稽核軌跡。
- 定期檢視防火牆規則，確認無流量規則否仍須使用，減少資料外傳的可能管道。

防毒軟體應保持更新

防毒軟體的偵測與防範功能只有在該軟體運作時、且有時常更新病毒碼情形下，才會產生效用，以下注意事項：

- 定期執行掃毒。
- 安裝防毒軟體或反間諜軟體。
- 不關閉、不刪除防毒軟體。
- 隨時注意防毒軟體的病毒碼為最新狀態。
- 不要隨意複製或下載不明檔案。
- 不要隨意開啟檔案。

作業系統更新

- 系統管理人員應定期檢查電腦設備效能，並注意作業系統修補、更新及問題資訊，做適當之建議及設定。
- 作業系統安裝與設定完成後，應先以廠商提供之程式進行修補，除非必要才連接網路進行系統更新。
- 大部分的軟體都會提供一項「自動更新」功能，啟動自動更新功能為最方便也最迅速的一種定時更新方法。 若會影響到系統的運作，也需要確定沒有問題才可以進行更新。

應用系統更新(1/2)

- 駭客會針對各種軟體進行漏洞研究與開發，而零時差攻擊常 對組織造成極大資安風險。
- 防範訣竅檢查以下重要應用程式或軟體是否為最新版本：
  - 作業系統(Windows 10、Mac、Linux…等)
  - 網頁瀏覽程式(IE、FireFox、Chrome…等)
  - 辦公室應用軟體(Office、Adobe PDF、Winrar…等)
  - 電子郵件收發軟體(如outlook、outlook express…等)

應用系統更新(2/2)

- 進行Windows Update前，先確認新版修補程式(Patch)不會影響系統運作，再佈署至正式環境。
- 定期檢查電腦之更新狀態，確保無系統長期未安裝修補程式之情事發生，尤其新進同仁所配發之個人電腦、教育訓練或出差使用之筆記型電腦。

自我檢查

檢查作業系統之「Windows Update」是否已更新至最新狀態。

檢視路徑：

[設定]

→[更新與安全性]

→[Windows update]

→[檢視更新紀錄]

電腦使用安全(1/3)

離開座位，應鎖定電腦螢幕或設定螢幕保護程式。

長時間離開辦公室，記得將電腦關機。

電腦使用安全(2/3)

- 不要儲存登入資訊，並確定登出。
- 刪除網際網路暫存檔和歷史記錄的方式，或使用無痕模式。
- 不在公用電腦上輸入機密資訊。

電腦使用安全(3/3)

- 使用者應使用組織授權的網路進行連線，避免私自連接其他網路。
- 不要使用加密強度不足之網路連線，可能遭受未經確認的SSID 識別碼詐騙，使得傳輸資料遭竊聽、外洩，建議將無線網路設定為WPA3加密。
- 為了保護無線網路不被未經授權的使用者侵入，最基本且簡單的無線網路安全設定，就是設定SSID與修改密碼。

辦公室設備使用注意事項(1/2)

- 電腦閒置時，應設定螢幕保護程式或鎖定螢幕。
- 不應將使用者之帳號密碼紀錄於紙本。
- 定期檢視防毒軟體及Windows Update是否確實更新。

- 離開座位時，機密文件不應置於辦公桌。
- 下班前需清理工作場所。

- 儲存媒體(如USB隨身碟)應妥善保管。
- 使用、移動及存取多媒體應遵循管制程序。
- 報廢的儲存媒體需確實銷毀。

辦公室設備使用注意事項(2/2)

- 印表機、影印機應有專人負責。
- 會議後須將會議室桌面及白板淨空。

- 紙本文件回收前，應確認是否含有機密資訊。
- 文件銷毀需確實。

- 限制區域應有門禁管制非經允許與陪同，外部人員不得進入。
- 辦公區域檔案櫃、抽屜、辦公室應上鎖。

資訊安全

需要你我共同維護