



使用社群服務安全小撇步

電子郵件社交工程防治宣導講習

資訊處 網路管理組 張維廷

2019.04.15

工商服務時間





2019/4/9 (週二) 上午 10:06

Wisely <wisely@mail.tku.edu.tw>

[通知] 請您盡速更改淡江單一登入之密碼

收件者 'Wisely'

您好,

本組收到【臺灣學術網路危機處理中心】資安訊息通知，您的校級 email 信箱疑似密碼外洩，為確保資訊安全與個人隱私，請盡速更改密碼，更改密碼網址是 <https://sso.tku.edu.tw>，若不知道如何更改密碼或是更改密碼過程中遇到問題，可撥分機 2468 由資訊處服務台協助變更密碼。

註 1: 若您已於 3/21 收到【臺灣學術網路危機處理中心】資安訊息通知且已更改密碼者，可以不用再更改。

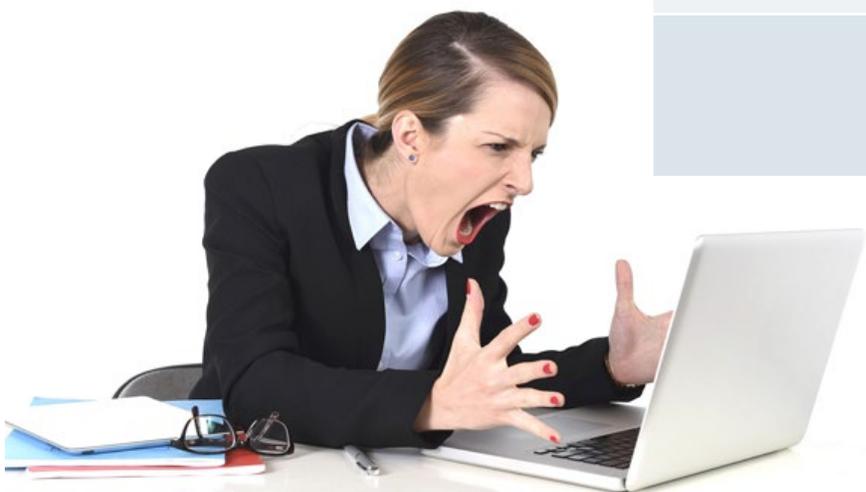
註 2: 這不是詐騙信，如有疑問可聯絡網路管理組王裕仁(分機 2628)，謝謝!

淡江大學資訊處 網路管理組
TKU-OIS Network Management Section
Tel: (02)2621-5656 ext.2628 FAX: (02)2620-9893
E-Mail: ficx@mail.tku.edu.tw

騙

本校受災狀況

學術網路外洩筆數	96,784	0.8%
本校外洩筆數	772	39%
扣除重複信箱筆數 (有些人改過密碼又重複外洩)	687	35%
其中信箱存在279筆, 不存在346筆, 非校級信箱62筆		





2019/3/13 (週三) 上午 03:15

wisely@mail.tku.edu.tw

Hackers know password from your account. Password must be changed now.

收件者 wisely@mail.tku.edu.tw

Hello!

I have very bad news for you.

21/10/2018 - on this day I hacked your OS and got full access to your account wisely@mail.tku.edu.tw

So, you can change the password, yes... But my malware intercepts it every time.

How I made it:

In the software of the router, through which you went online, was a vulnerability.

I just hacked this router and placed my malicious code on it.

When you went online, my trojan was installed on the OS of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses)

A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.

But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!

I'm talk you about sites for adults.

I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea....

I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).

After that, I made a screenshot of your joys (using the camera of your device) and glued them together.

Turned out amazing! You are so spectacular!

I'm know that you would not like to show these screenshots to your friends, relatives or colleagues.

I think \$740 is a very, very small amount for my silence.

Besides, I have been spying on you for so long, having spent a lot of time!

Pay ONLY in Bitcoins!

My BTC wallet: 1H1K8MfLEJgCCfDEkTJmv9GJJd3XzEFGR

You do not know how to use bitcoins?

Enter a query in any search engine: "how to replenish btc wallet".

It's extremely easy

For this payment I give you two days (48 hours).

As soon as this letter is opened, the timer will work.



收件者 wisely@mail.tku.edu.tw
我們已將此郵件轉換為純文字格式。

272833566478_842052.doc
213 KB

勒索病毒主要攻擊管道-網路釣魚!
三不三要 反檔案綁架▶



- 校友服務暨資源發展處 OATKU
- 信箱 (2)
- 草稿
- 已傳送
- 後續
- 所有文件
- 垃圾
- 垃圾桶
- 視圖
- 資料夾
- 工具
- 其他郵件

收件人: 網路管理組/TKU@淡江大學
寄件人: 校友服務暨資源發展處/TKU
日期: 04/16/2019 08:58 上午
主旨: 轉寄: 發票申請

- 回覆 全
- 發票申請
- 外國語文學院
- 收件人: 發
- 附件檔

校友服務暨資源發展處
承辦人: ○○○ (分機 812○)

----- 轉寄人 校友服務暨資源發展處/TKU 時間 04/16/2019 08:58 上午 -----
 收件人: 淡江大學校友服務暨資源發展處 <fl@oa.tku.edu.tw>
 寄件人: 外國語文學院 <irma.garcia@hospitalesmac.com>
 日期: 04/15/2019 05:08 下午
 主旨: 發票申請

您好!
您的發票
(請參閱附加檔案: 272833566478_842052.doc)
万事如意 您好!
外國語文學院
您的發票已附上。
tf@oa.tku.edu.tw

万事如意
外國語文學院
tf@oa.tku.edu.tw



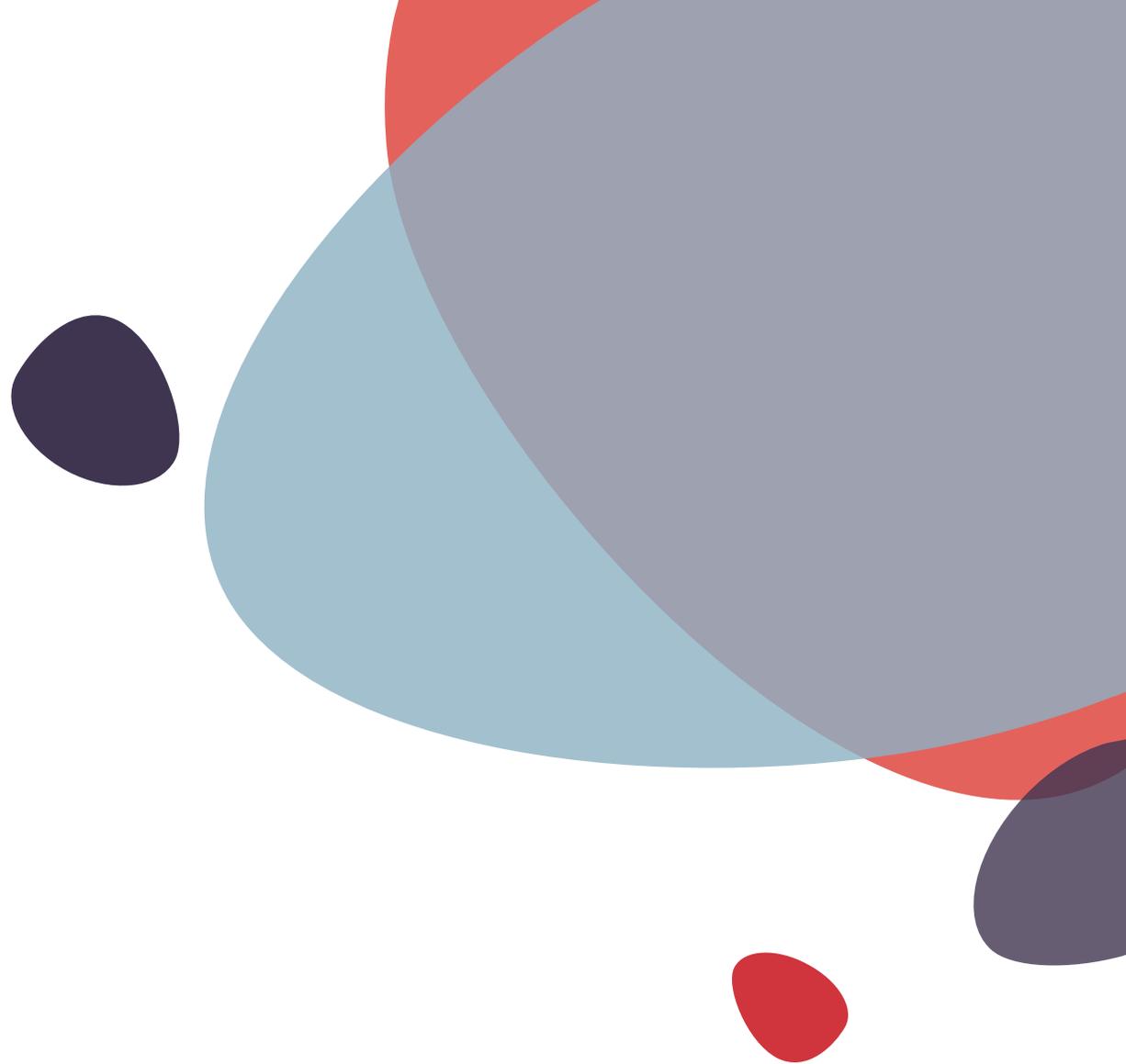
omino Web Access

名稱	原始
防護掃描	C:\U

關閉

暫停掃描(P) 關閉(C)

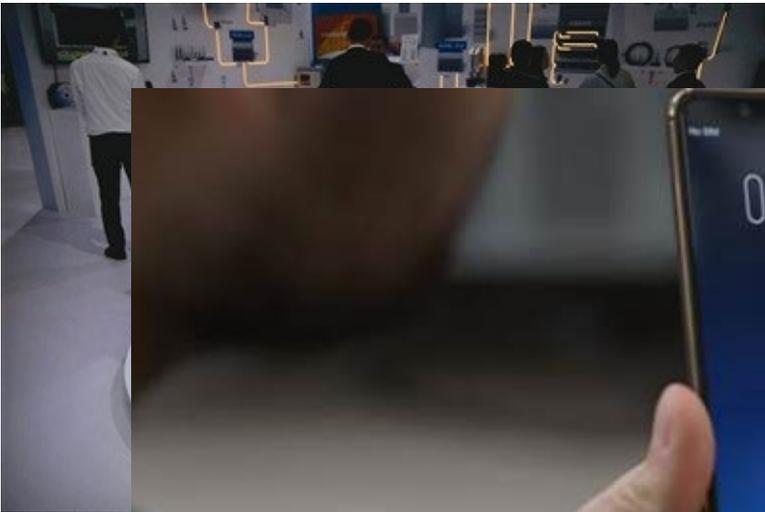
非蘋陣營





iPhone不再潮 蘋果神話面臨挑戰





MWC19™
Barcelona

25-28 February 2019

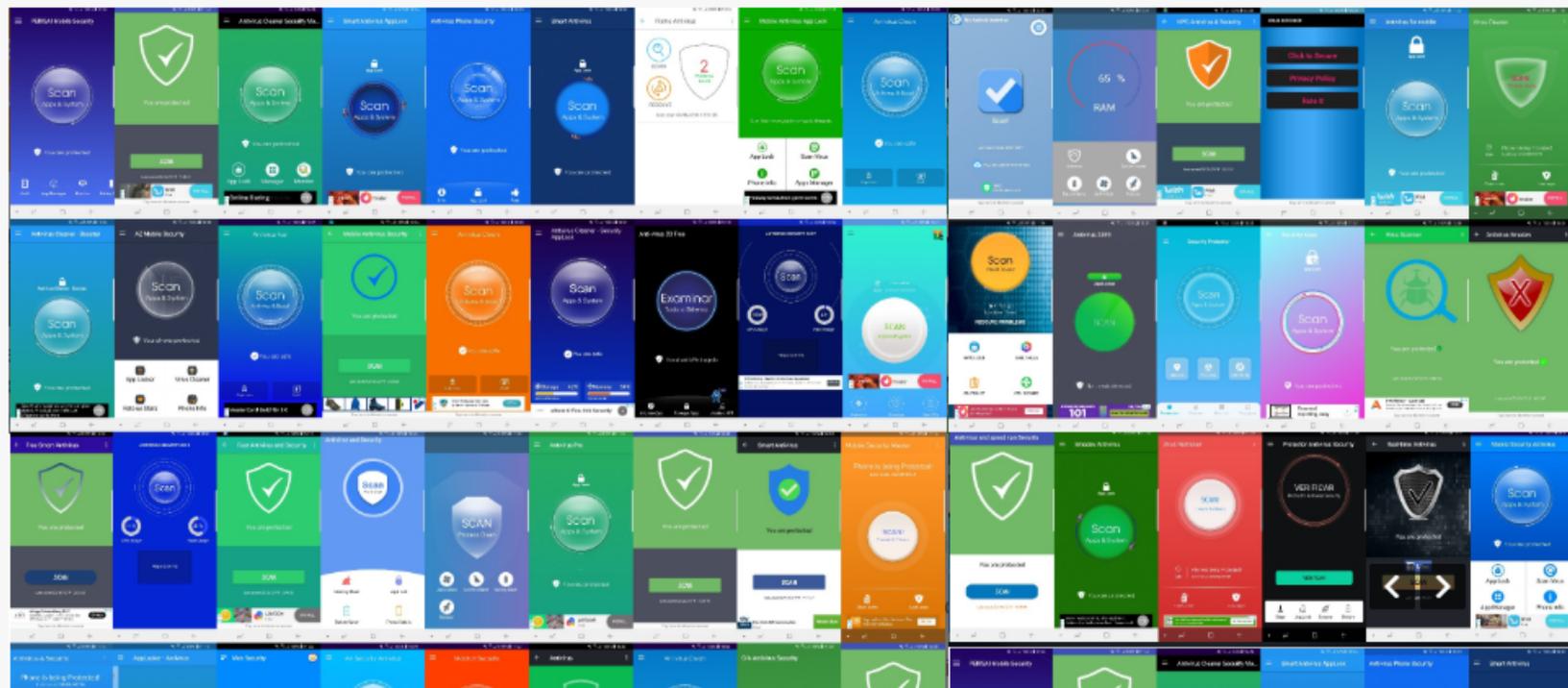
研究：Android防毒軟體只有3成有效，更有2成5反而不安全

AV-Comparatives針對250款反惡意程式app進行測試，發現有四分之一的Android防毒軟體其實是木馬程式或垃圾軟體

文/ 林妍濤 | 2019-03-15 發表

讚 5.3 萬 按讚加入iThome粉絲團

讚 1,172 分享



AV-Comparatives研究發現，功能表現糟糕的安卓防毒軟體介面往往很類似，可能是開發商草率地套用相同版型所打造。(圖片來源 / AV-Comparatives)



行動上網病毒防不勝防，Android手機用戶可能想到下載防毒強化手機安全。不過一項研究顯示，連Google官方的 Play Store上的防毒軟體或反惡意程式軟體，僅三分之一具備一定水準的防護能力，其他的不是偽造程式，就是沒什麼效果，更有24%屬於不安全的程式。



The best antivirus software for Android

About the Institute | News | Tests | Statistics | Contact

Tests for home users

[Android Antivirus >](#)

[MacOS Antivirus >](#)

[Windows Antivirus >](#)

Tests for business users

[Android Antivirus >](#)

[MacOS Antivirus >](#)

[Windows Antivirus >](#)

Internet of Things (IoT)

[Smart Home >](#)

[IP Cameras >](#)

[Smart Watches & Fitness-Tracker >](#)

[Other >](#)

AhnLab V3 Mobile Security 3.1



AVTIV AVL 2.7



avast Mobile Security 6.15



AVG AntiVirus Free 6.15



Avira Antivirus Security 5.6



Bitdefender Mobile Security 3.3



cheetahmobile Security Master 4.8



F-Secure Mobile Security 17.6



GDATA Internet Security 26.5



business users



[More >](#)

[Android Antivirus >](#)

[MacOS Antivirus >](#)

[Windows Antivirus >](#)

Internet of Things (IoT)



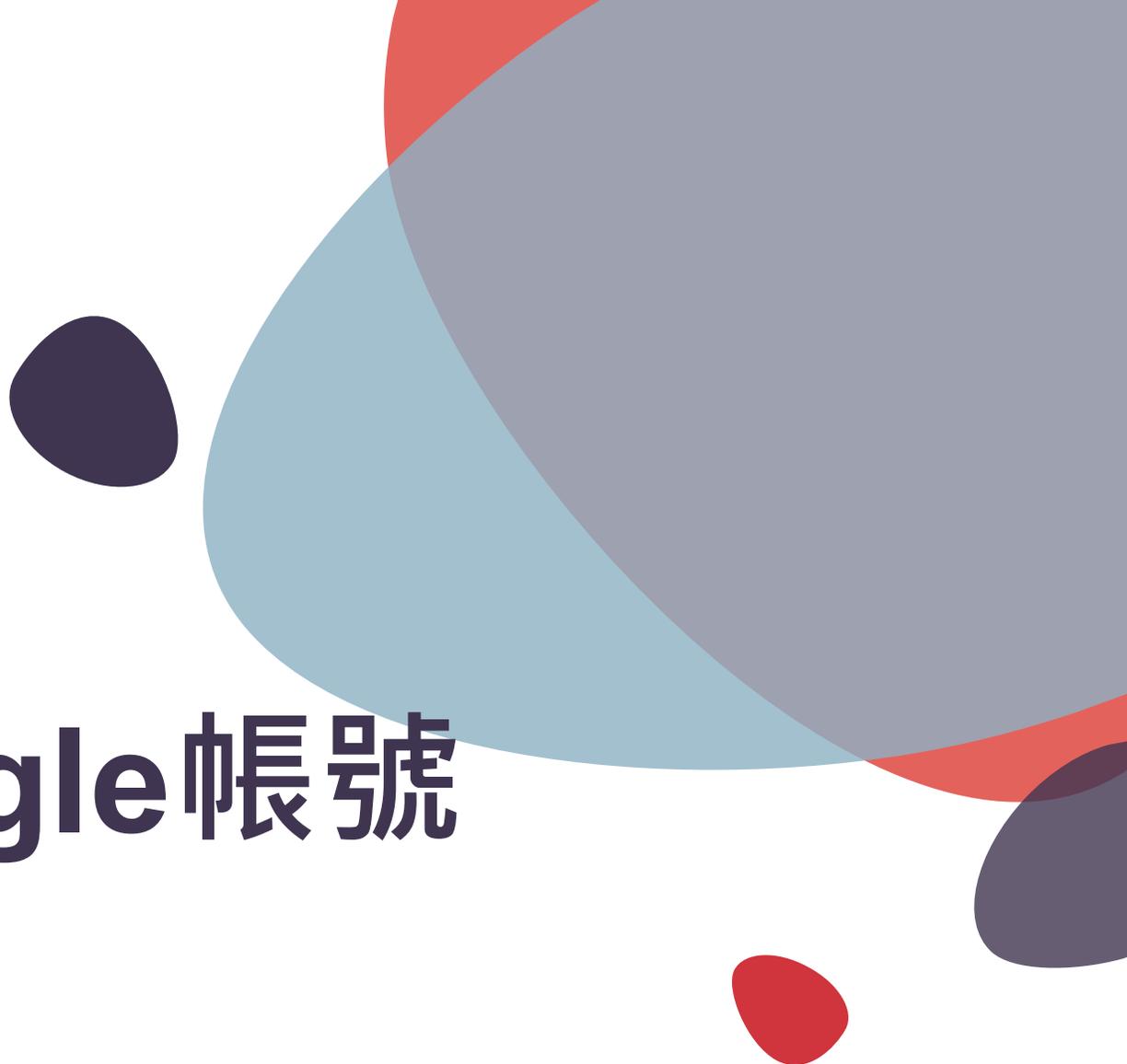
[More >](#)

[Smart Home >](#)

[IP Cameras >](#)

[Smart Watches & Fitness-Tracker >](#)





Android的Google帳號

新增您的帳戶



只要登入帳戶，即可讓您的裝置發揮更多妙用。 ⓘ

輸入您的電子郵件

[或是建立新帳戶](#)



안드로이드

啟用兩步驟驗證 大幅提昇帳戶安全性



登入程序略有不同

您必須輸入驗證碼：
在您輸入密碼後，系統會要求您輸入
一組透過簡訊、錄音帶或行動專用
程式取得的驗證碼。

在登入帳戶時，系統會要求您輸入
不必在您的裝置上輸入驗證碼。

避免不肖人士入侵帳戶

確保您的帳戶受到妥善保護：
只要您（或其他人）或惡意的電腦登入
您的帳戶，系統就會要求輸入驗證
碼。



Google Authenticator

Google LLC 工具

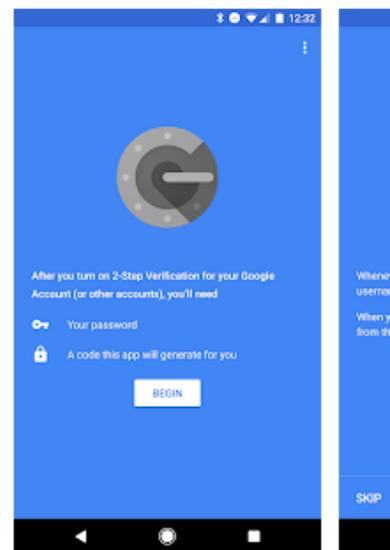
★★★★☆ 187,448

3+

這個應用程式與你所有的裝置都相容。

加入願望清單

安裝



Google Authenticator 可在你的手機上產生兩步驟驗證碼。

兩步驟驗證機制會在你登入帳戶時，要求進行第二步驟驗證，因此能進一步確保你的 Google 帳戶安全無虞。啟用這項功能後，登入帳戶時除了輸入密碼，還必須輸入 Google Authenticator 應用程式在你手機上產生的驗證碼。



Two Factor Auth (2FA)

List of websites and whether or not they support [2FA](#).

Add your own favorite site by submitting a pull request on the [GitHub repo](#).

🔍 Search websites



Backup and Sync



Banking



Betting



Cloud Computing



Communication



Cryptocurrencies



Developer



Domains



Education



Email



Entertainment



Finance



Food

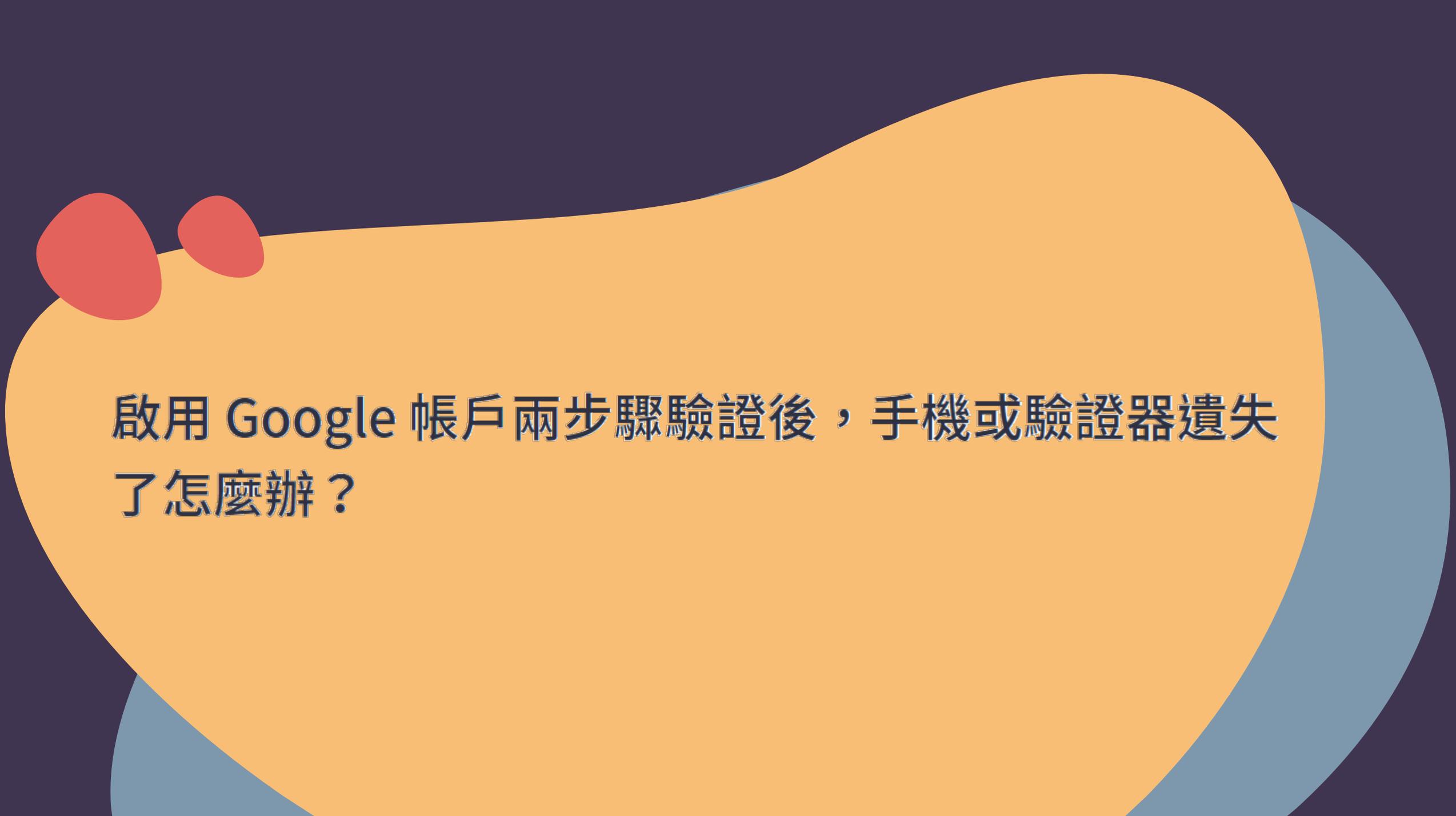


Gaming



Government





啟用 Google 帳戶兩步驟驗證後，手機或驗證器遺失了怎麼辦？

負責兩步驟驗證的裝置遺失時，拾獲的人能登入你的帳戶嗎

先說結論，裝置拾獲者可以對你的網路帳號進行有限度的操作，但是在大多數的狀況下無法取得登入你的網路帳號並取得帳號所有權。

例外狀況

- 網路帳號的密碼設定的太簡單，或是跟你的個資很有關聯導致很好猜中，這時候第二步驟驗證關鍵裝置在他手上，猜中密碼後馬上就可以登入帳號內。
- 你的裝置不是遺失，而是被帶有特地目的的人偷走；這種人通常很可能事前已經想辦法知道你的密碼，所以取得能獲取驗證碼的裝置後，他自然能取得你的帳號所有權。

當行動裝置遺失時，你該採取的行動

- 無論裝置找不找的回來，第一時間都先使用遠端管理工具將行動裝置鎖定或清除所有資料。
 - Android 裝置: 使用「Android 裝置管理員」就可以進行這些遠端操作。
 - iOS 裝置: 使用「尋找我的 iPhone」進行遠端操作。
- 假如遺失的裝置內有連線用的 SIM 卡，記得在最短時間內將 SIM 卡停用。

兩步驟驗證三要件

帳戶

缺一不可



密碼

驗證碼

用於第二步驟驗證

平日就該做好的帳戶救援準備工作

- 準備一台受信任的裝置

- 填妥帳戶內的備援資料

- 記錄備用碼

- 確認裝置上的 Android 裝置管理員已完成設定



兩步驟驗證

為進一步確保您的電子郵件、相片和其他內容的安全，請完成下列步驟。



輸入驗證碼

無論是哪一種裝置，私人的一定要勾選
[這部電腦以後不需驗證]

在月半前輸入... 已及要及無的... 已及要及無的...

驗證

這部電腦以後不需要驗證

[嘗試其他登入方式](#)

2:23

https://accounts.google.com



兩步驟驗證



輸入驗證碼

使用 Google Assistant 登入

密碼

驗證

這部電腦以後不需要驗證

[嘗試其他登入方式](#)

Facebook史上最大漏洞攻擊！為了帳號安全，你該知道的7件事

2018.09.30 by  蕭閱云



Facebook發生史上最大漏洞攻擊事件，5千萬帳號暴露在高風險中。如果你最近也被強制重新登入，那你的帳號可能也掌握在駭客的手中。

雙重驗證

增加額外防護

新增備份

請設定備用選項，以便在你所選的帳號防護方式無法使用時順利登入。

設定額外的安全措施



接收不明登入活動的警告

開啟 • 如果任何人從與平常不同的裝置或瀏覽器登入你的帳號，我們就會通知你

編輯



選擇你帳號被鎖住時能夠聯絡的朋友 (3 到 5 位)

你信賴的聯絡人可以傳送 Facebook 代碼和網址，協助你重新登入帳號

編輯





特徵一：網頁上沒有公司地址以及客服電話(或是無人接聽)，只留下電子信箱。

特徵二：售價明顯低於市場行情。

特徵三：常以限時或倒數方式吸引民眾。

特徵四：免運費、號稱有7天鑑賞期及可拆箱驗貨。

特徵五：只能使用貨到付款或信用卡付款(有信用卡盜刷風險)。

特徵六：網頁大多會夾雜簡體字。



一頁式詐騙廣告穿插在熱門新聞中,一不小心就容易掉入陷阱



到新地方旅遊嗎？

我們之前從未看過您在此處登入。請在下方選擇一種方式以驗證您為帳號使用者本人。[了解更多](#)

順帶一
並不支

取驗證
之類的



+8860888
傳送文字訊息



+8860888
以電話通知驗證碼



lear.....@gmail.com
以電子郵件傳送驗證碼

取消

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate !\[\]\(1c70f21f694d12b9fc928edb998ea27b_img.jpg\) !\[\]\(f7dfa3fa22bde1ecd2591e917461d0b1_img.jpg\)](#)

';--have i been pwned?

Check if you have an account that has been compromised in a data breach



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

359

pwned websites

7,840,611,051

pwned accounts

92,846

pastes

113,328,586

paste accounts

Largest breaches

Recently added breaches



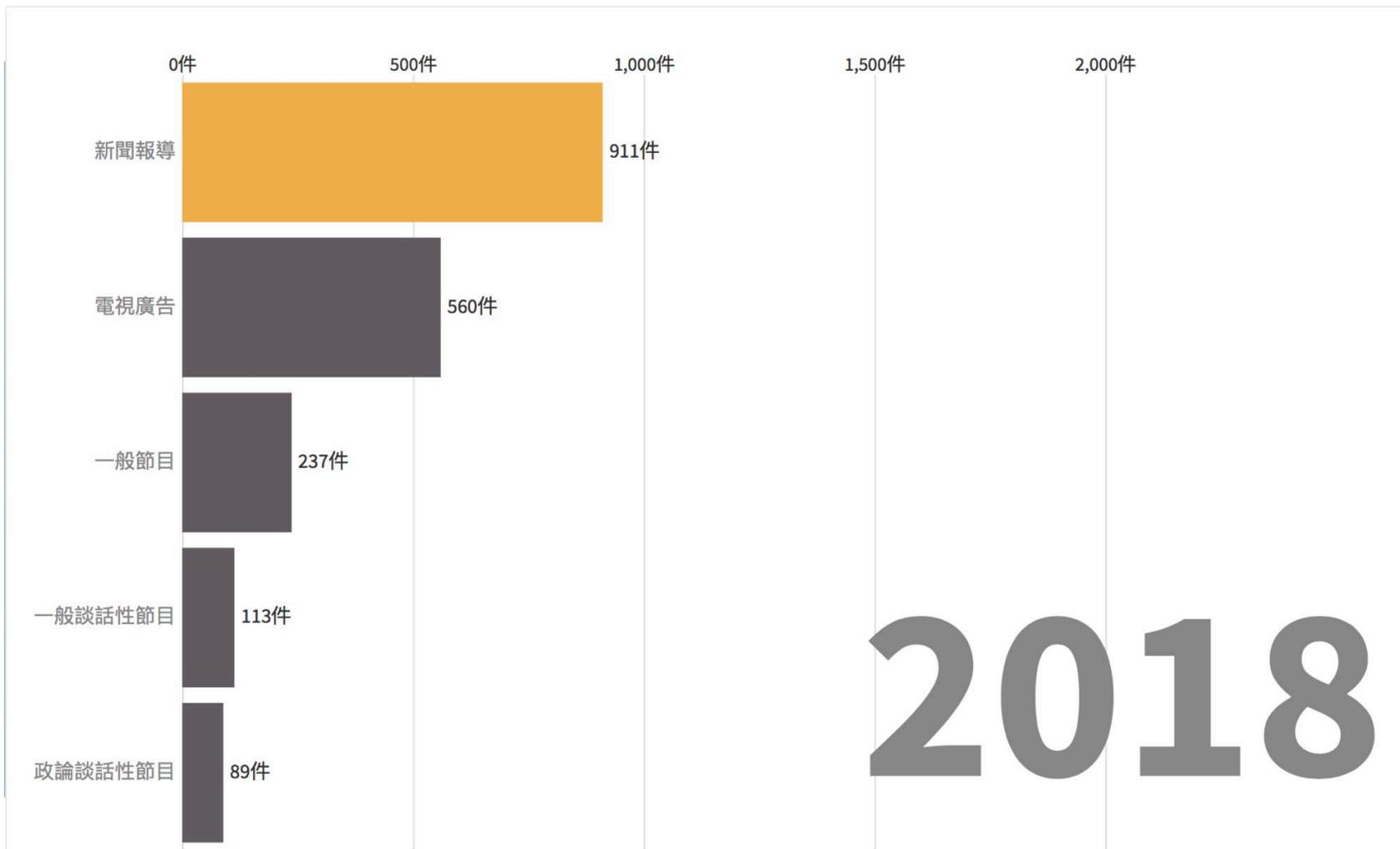
新手機的第二套APP是？



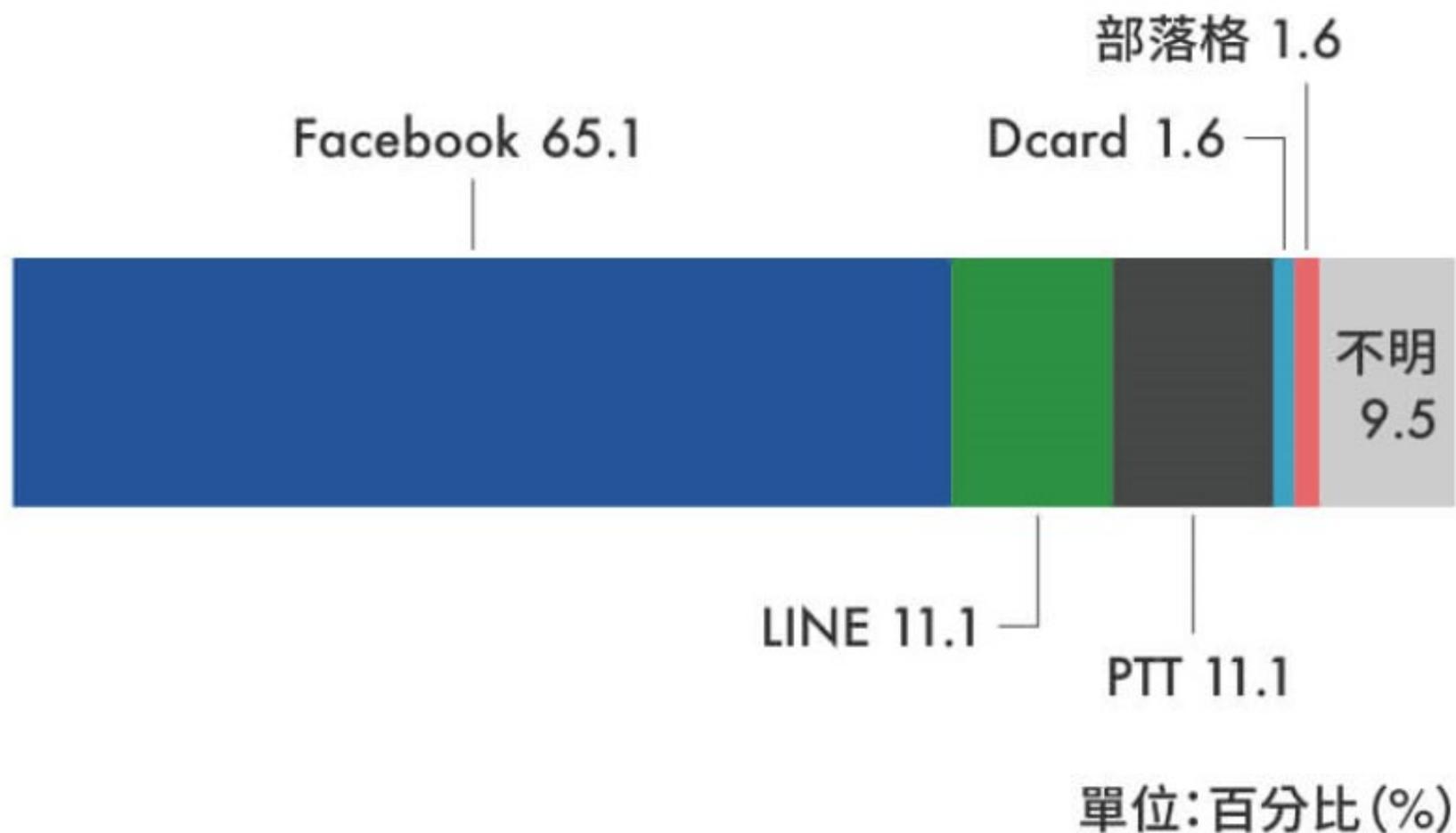
LINE



假訊息氾濫成災 台灣成國際認證謠言大國



被判謠言罪的網路謠言是用什麼平台被散佈？



資料來源：法務部檢察機關公開書類查詢系統

謠言沒人管 公嬾瘋傳江蕙郭董費玉清複雜關係



美國麻省理工大學媒體實驗室針對 Twitter 上超過 300 萬位用戶的資料進行研究，發現假訊息的傳播速度是一般訊息的 6 倍。

謠言發生多久，法院才能做出決定？



資料來源：法務部檢察機關公開書類查詢系統

20~24
NCC多案混為一談 民眾質疑與其立場不同變箭靶

19:03:22 **韓流發威** 頭髮不多收穫不少! 央視點評"韓流"登陸

19:03:26 **韓流發威** 貼身採訪韓國瑜 外媒女記者大讚市長貼心

19:03:31 **韓流出訪** 韓國瑜廈門訪南普陀寺 方丈親贈"心安事隆"

19:03:36 **韓流出訪** 韓參訪南普陀寺 借鏡宗教觀光"帶人進高雄"

19:03:41 **韓流出訪** 2020徵召傳不完 韓國瑜獲贈字畫自虧:心不安

19:03:51 **衝拼經濟** 韓國瑜拚招商!工總將加碼投資高雄逾800億

19:04:38 **韓流登陸** 拚訂單觸法?陸委會喊話 擬開罰韓國瑜50萬

19:03:56 **成績亮眼** 訂單破52億 韓成績單還有"高深.雙港論壇"

19:04:43 **韓流登陸** 綠委要求提"韓國瑜條款" 藍委轟:腳鐐條款

19:04:48 **擬錮韓戰** 陸委會擬開錮韓國瑜 高思博:淪綠朝錦衣衛

19:04:48 **擬錮韓戰** 陸委會擬開錮韓國瑜 高思博:淪綠朝錦衣衛

19:04:54 **擬錮韓戰** 韓見中聯辦賣台? 陳明通曾"宴請"中聯辦..

19:04:58 **抹黑酸韓** 陸國台辦:民進黨扯韓後腿 民眾會擦亮眼睛

19:05:45 **熱情迎接** 穿Q版韓國瑜T恤 韓粉守候廈大迎接韓國瑜

19:07:51 **隔海回嗆** 陳致中告外患罪 韓:怎麼不去自首外遇罪?

19:07:55 **隔海回嗆** 陸委會擬設韓國瑜條款修法 韓:真是開倒車

19:07:59 **大選布局** 2020選不選 韓國瑜:老鼠偷拖鞋 大的在後面

19:08:07 **韓流登陸** 台商座談變粉絲會 選舉礦泉水列廈大展示櫃

19:08:09 **韓流登陸** 迎賓小童超可愛 韓國瑜.李佳芬抱抱笑開懷

19:08:15 **推銷高雄** 邀陸"雙冰"代言? 韓:高雄已有白冰冰.韓冰

19:08:31 **中天聲明** 以鼓勵與監督角度 對韓市長拚經濟施政作為報導

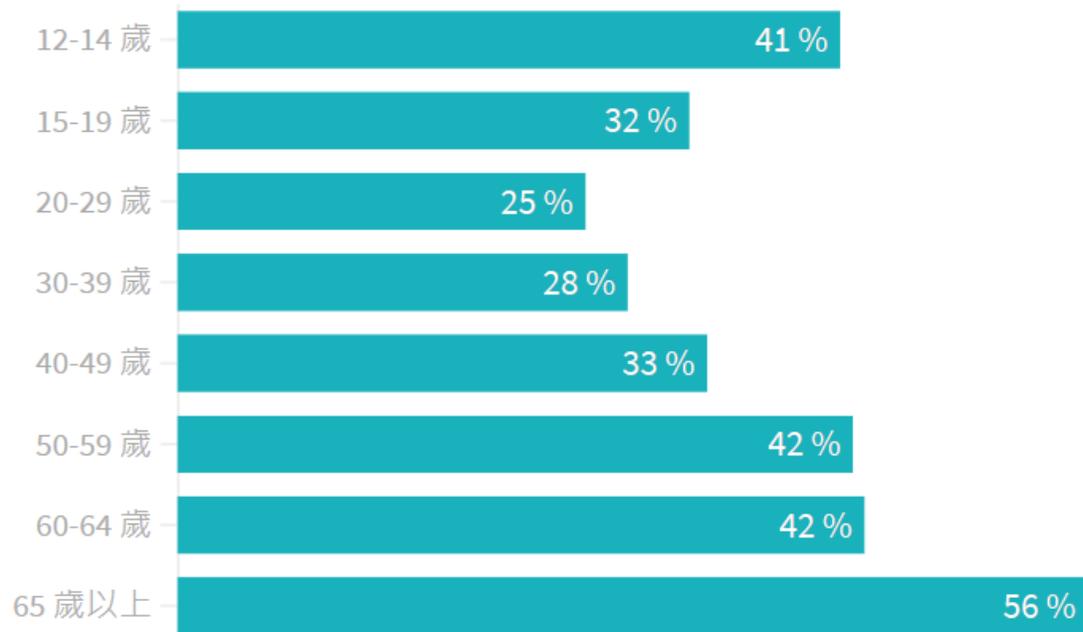
2019年 3月 27日

韓總計數器

35.199.161.19/ ▼

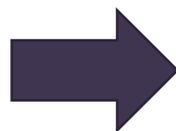
韓總計數器已終止，讓我們互道一聲晚安，從4/1至4/3號總計為下. 3489. 你可以下載從4/2號至4/3的計數統計資料(JSON格式). 點此下載. file name: 當下紀錄的UTC ...

老人與小孩是最不會查證網路訊息的族群



資料來源：國發會 / 各世代網路族網路訊息真實性查證情形

替 LINE 設定上鎖密碼，不怕被別人偷看



取消 Facebook 同步

設定

我的資訊

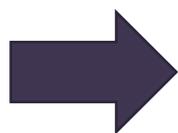
個人資料

我的帳號

隱私設定

移動帳號設定

Keep

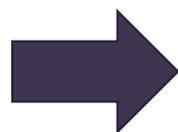


Facebook

解除

畫面會出現「同步功能已解除」的字眼，同時原本前一步驟 Facebook 項目的地方會變成「開始同步」。

從其他的裝置登入 LINE 帳號



關閉來自遊戲與應用程式的邀請訊息

連動中的應用程式

連動中的應用程式

LINE Q

LINE: Disney Tsum Tsum

LINE漫畫

LINE GIFTSHOP

Game OA Friends Invitation

LINE 購物



授權

連動中的應用程式

您可對連動應用程式設

未連動中的應用程式

關閉此設定後，即可拒

LINE: Disney Tsum Tsum



LINE: Disney Tsum Tsum

LINE

連動日期 2017/05/22 17:21

試著在時間內連接Tsum並消除他們來獲得高分。這是一款全新的益智遊戲，快來與你的LINE好友們一起比賽吧！

接收訊息



接收提醒



編輯權限

取消與本應用程式的連動

啟用點對點加密對談，聊天內容不外洩



禁止不認識的人隨意加你好友跟傳訊息

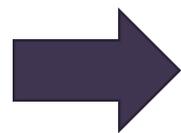
設定

我的資訊

 個人資料

 我的帳號

 隱私設定



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。



允許好友邀請

若您啟用此設定，任何人都能向您傳送好友邀請。



聊天 · 通話

備份及復原聊天記錄
備份後，聊天記錄將儲存於Google雲端硬碟。
若遺失或更換新的智慧手機時，也可復原已備份的聊天記錄。

Chats

背景

字體大小
普通

以Enter鍵傳送
設定後，按下Enter鍵即可傳送。

再度自動傳送
無法傳送的訊息於一定時間過後，將會再度自動傳送。

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。



備份及復原

上次備份
日期：-
容量合計大小：-

Google雲端硬碟

備份至Google雲端硬碟
備份後，聊天記錄將儲存於Google雲端硬碟。
若遺失或更換新的智慧手機時，也可復原已備份的聊天記錄。

Google帳號
尚未設定

復原

復原

備份及復原聊天記錄

上次備份

日期：2017/05/31 12:25
容量合計大小：28.00 KB

記錄

取消 確定



「LINE」要求取得以下權限：

查看及管理此 API 在 Google 雲端硬碟中的設定資料

如果選擇繼續，即表示您同意讓這個應用程式和 Google 根據各自的服務條款和隱私權政策使用您的資訊。

拒絕 允許

- 裝置限制：目前沒有特別限制特定類型的Android手機無法使用備份。
- 備份的範圍：目前先開放文字訊息備份，尚未包括圖片、影片等其他類型的內容。備份前如果有重要的圖片或檔案在LINE中，建議您先存在手機裝置或LINE Keep中，再開始進行備份。

2017.6.2 補充：圖片僅短暫保留在伺服器中。如您備份後發現聊天室內的圖片仍可瀏覽，即表示該圖片尚未超過下載期限；超過保存期限的圖片，在備份還原後將無法再瀏覽與恢復。

- 儲存位置：LINE訊息備份會存在您的Google雲端硬碟，倒是可先確認一下您的Google雲端硬碟容量是否已滿。此外，提醒也要更新一下您手機裡的Android作業系統，Android 2.1版本以上才有支援Google雲端硬碟呦！

【拆解假帳號詐騙四大手法】

手法一、特過特定連結或假網站、誘使加入其他詐騙帳號

破解之道：針對可疑帳號提供的網站連結，查明對照該網址名稱是否為品牌官方網站，以免受騙上當。

手法二、帳號名稱為知名品牌或商品帳號，卻為灰色盾牌

使用以假亂真的官方帳號。辨識LINE帳號的盾牌顏色，若標示為「灰色」盾牌，此為一般帳號，一般人都可申請。

「深藍色」盾牌，為認證帳號，所有具商業登記的商家均可填表、寄送備查資料向LINE@團隊申請認證，經認證通過後，帳號盾牌將可從灰色轉為深藍色。

「綠色」盾牌，為可靠的官方帳號。



非官方帳號
假的!

別上當受騙嘍!!

LINE貼圖隨機贈送
2017/10/02 00:00 ~ 2018/02/23 23:59

LINE歡慶6週年簽到

加入好友參加抽選

辨別真假帳號方法
天下沒有白吃的午餐

LINE貼圖詐騙

手法三、要求分享給更多好友或群組，才享有免費好康

此為詐騙帳號最經常使用的手法，且不斷推陳出新版。慣用手法都是要求用戶「大量轉發給親友，並需向好友推薦此帳號、或將優惠資訊分享給更多好友，才符合領取優惠的資格」、「分享給5個群組後，請耐心等待優惠序號發送」等。

手法四、要求加陌生帳號好友

會用假冒偽裝成官方品牌的形式，要求用戶加入可疑客服帳號、驗證帳號、詢問主辦單位，點擊後若跳出「好友畫面」，務必要提高警覺。



收到訊息時，若你
感到……

心情有趣

驚訝

創造恐慌

害怕



傳遞仇恨

反感



先停下
想分享給別人的心情



聽聽別人的建議

Google 看看是不是已經被證實是謠言？

轉傳給查證的 LINE 群組「真的假的」、

「MyGoPen」、「蘭姆酒吐司」



看一看

來源跟作者認識嗎？

是可靠的來源嗎？

標題跟內容一樣嗎？

是不是故意用了聳動的文字？

假訊息停看聽

假網站的特徵拆解

不明網址
以假亂真的假網站
不明按鍵要求辨識身份或聯絡客服
要求分享給更多人

165全民防騙超連結

165反詐騙諮詢專線關心您



如何封鎖檢舉LINE名單

假帳號的特徵拆解

知名品牌卻是灰色盾牌
分享才能拿貼圖、優惠
要求加入陌生帳號

LINE Pay

資訊安全管理系統標準



支付卡產業資料安全標準

Thank You!

Do you have any questions?

