新型態駭客手法
智慧型手機社交工程

手機病毒｜扮廣告小遊戲潛入101個Apps、4億人中招恐被偷錢洩私隱

撰文：蔡浩騰
出版：2023-06-04 10:00　更新：2023-06-04 10:00

手機病毒｜手機 Apps 的種類非常多元化，近年還有些打著可以「賺錢」的旗號的遊戲 Apps 上架，玩家只要每日登入遊戲就可以賺取小量金錢或分數

熱門文章

查看更多 >

手機病毒偽裝成廣告遊戲 101個Apps被揭帶毒 逾4億人中招銀行資料恐外洩

Top10帶SpinOk木馬病毒App

1. Noizz: video editor with music (1億次下載)
2. Zapya – File Transfer, Share (1億次下載；Dr. Web表示 SpinOK 存在於 6.3.3 版本到 6.4 版本中，但在當前版本6.4.1中已經不存在)
3. VFly: video editor&video maker (5千萬次下載)
4. MVBit – MV video status maker (5千萬次下載)
5. Biugo – video maker&video editor (5千萬次下載)
6. Crazy Drop (1千萬次下載)
7. Cashzine – Earn money reward (1千萬次下載)
8. Fizzo Novel – Reading Offline (1千萬次下載)
9. CashEM: Get Rewards (500萬次下載)
10. Tick: watch to earn (500萬次下載)病毒 / 惡意 Apps 4 大危險特徵


超亮手電筒
Surpax Technolo
超亮手電筒
Mobile Apps In 免費
超亮手電筒
Zentertain 免費
FREE
爆亮手電筒
Rabbit Tank St 免費
千尋影視
Qianxun Team 免費
熱門
電視劇
Hot TV Shows
YunYun Creati 免費
電視連續劇聲音
Jose Reyes 免費
韓劇
Korea TV Shows
YunYun Creati 免費
PPS
PPS影音HD
PPS.TV 免費
秀
美图秀秀
Meitu, Inc.
贴
秀
美图贴贴
Meitu, Inc. 免費
秀
美颜相机
Meitu, Inc. 免費
百度魔图
Baidu HK 免費
美拍
Meitu, Inc.

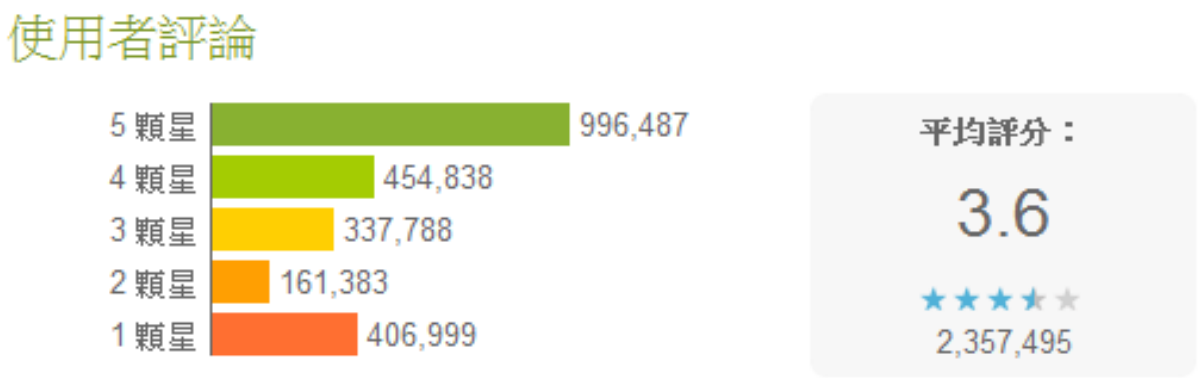

https://play.google.com/store/apps/details?id=goldenshorestechnol
最亮的手電筒免費 - Googl...
Google play
搜尋
+Benny
應用程式
頻別
我的應用程式
購物
遊戲
編輯精選
最亮的手電筒免費
GoldenShores Technologies, LLC
免費
這個應用程式可以存取：
位置
使用裝置的位置資訊
相片/多媒體/檔案
使用下列一或多個項目：裝置上的檔案 (例如圖片、影片或音訊檔案)、裝置的外部儲存空間
相機/麥克風
使用下列一或多個項目：相機、麥克風
選擇裝置
Far EasTone Telecommunications HTC HTC_M8x
我們簡化了應用程式權限。瞭解詳情
取消
安裝
Flashlight Free®

如何判定Android App是否為惡意軟體

下載前:

1.使用者評價

誰說都不公平，使用者說最公平，看評價，是4星或5星就可以下載?不，等一下，請確定評價人數至少要500到1000人，因為10人可能是灌水



如何判定Android App是否為惡意軟體

如何判定Android App是否為惡意軟體

看完軟體，來看看開發員，建議只下載頂尖開發員的軟體，因為大部分知名品牌都有頂尖開發員資格，所以這樣可以避免被騙

如何判定Android App是否為惡意軟體

下載後:

1.手機耗電量

當駭客到你的手機抓檔案，耗電量當然會增加，所以隨時注意耗電量是否異常

2.背景運作軟體

駭客不可能在你用軟體時才來抓檔案，一定是讓軟體背景運作，隨時都可以抓，所以可以到設定→應用程式→正在運作的服務，確定裡面沒有沒看過的程式在跑，如果有，請強制停止(通常叫作MonitorService)

手機上網安全問題

結果是…

將重要的資料寄給非授權的人

備忘錄放至網路留言板

關鍵文件透過印表機列印出

將資料、圖檔、文件燒錄至CD內

據統計有80%的資料遺失,是因為內部人員有意或無意之下所造成的結果

隱私權的過去與今日

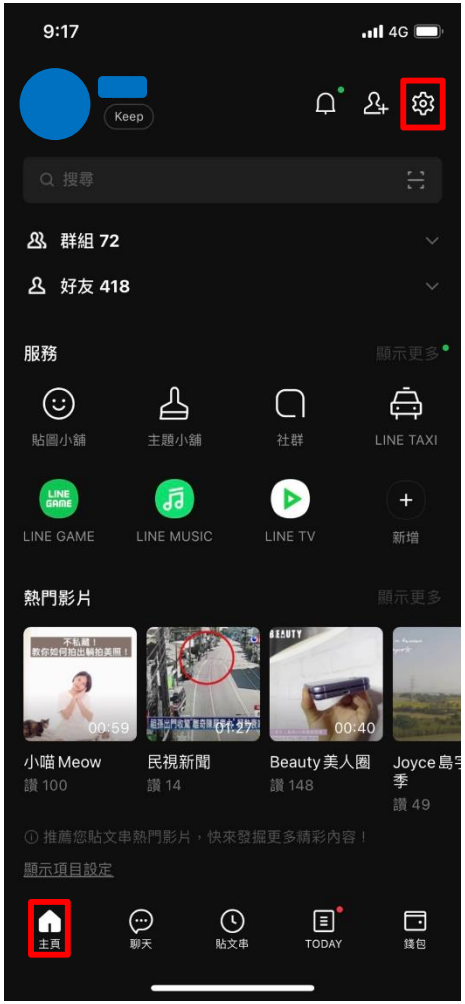
- **電影：被監控/追蹤是很可怕的一件事**
- 追蹤工具：
  - 高科技追蹤晶片
  - 衛星
  - 攝影機
  - 人員監控

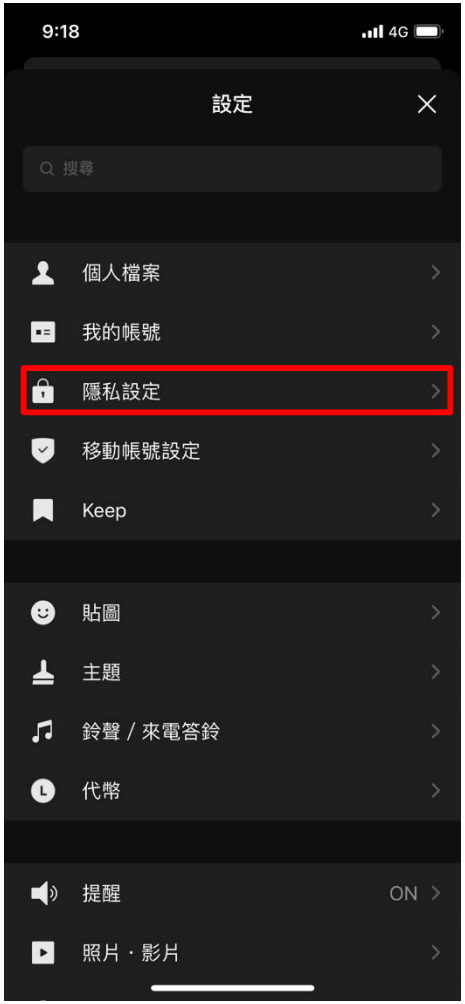
- **今日：透過各種管道主動透露行蹤**
- 管道：
  - Email
  - 社交網站打卡
  - **手機安裝病毒程式**

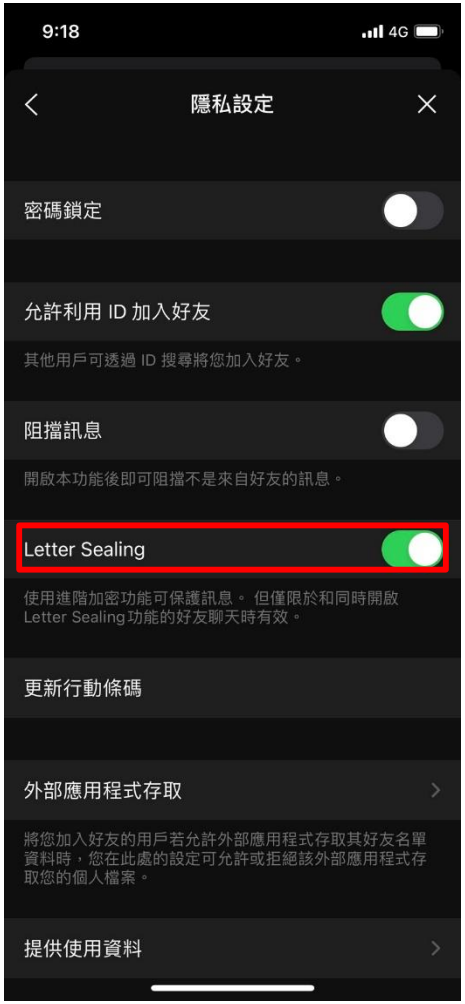
LINE 驚傳遭到駭客入侵，府院高層等 100 多人帳號被鎖定

我國府院高層人士驚傳遭駭客鎖定，藉由 LINE 入侵、擷取內容再外流，LINE 系統偵測到異常後，立即採取必要措施保護用戶，並由台灣總公司向執法單位報案。由於被鎖定的對象牽涉府院高層人士，恐有國家安全疑慮，國安單位展開專案調查。

訊息加密功能-IOS

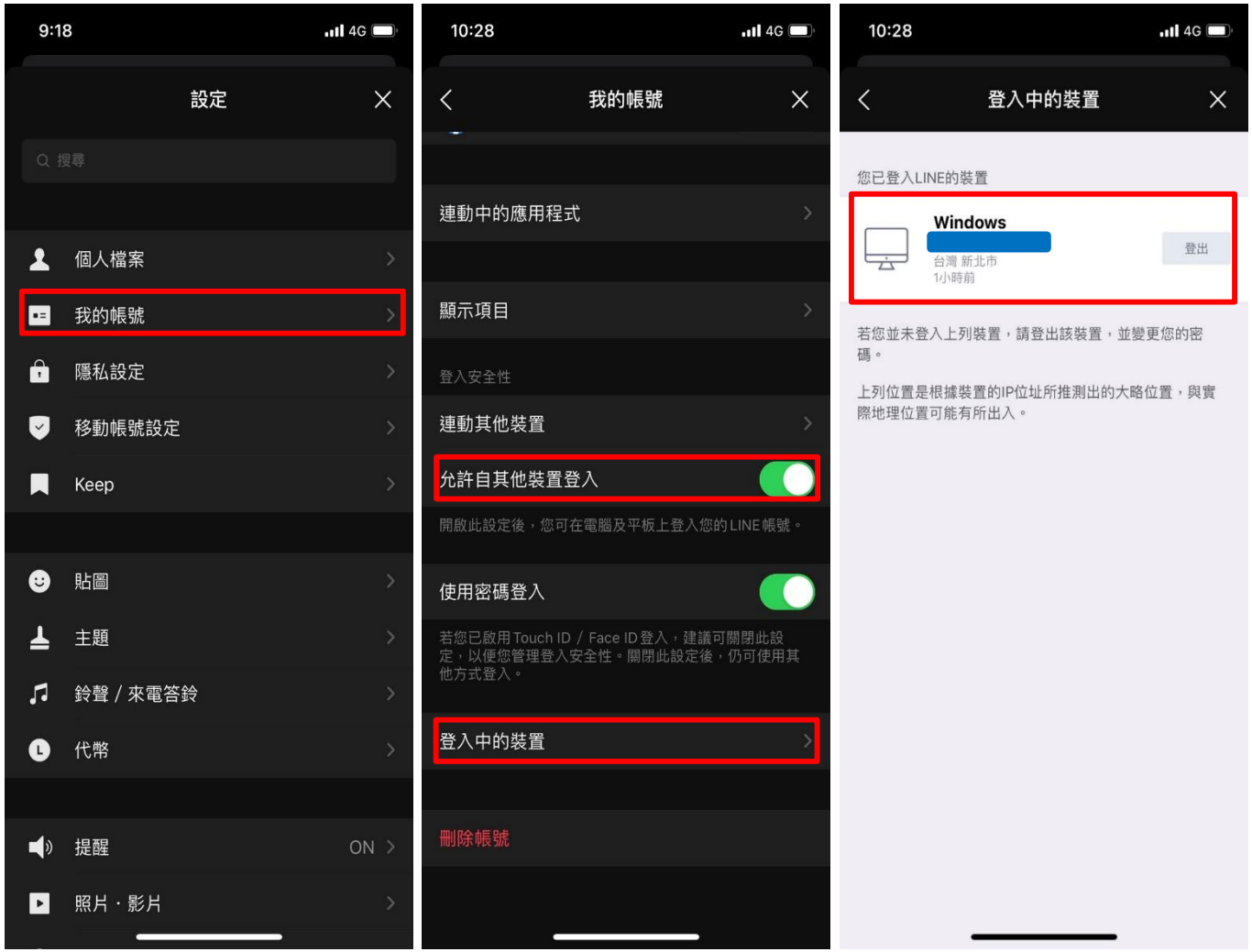

9:17
4G
Keep
搜尋
群組 72
好友 418
服務
顯示更多
貼圖小舖
主題小舖
社群
LINE TAXI
LINE GAME
LINE MUSIC
LINE TV
新增
熱門影片
顯示更多
00:59
01:27
00:40
小喵 Meow
讚 100
民視新聞
讚 14
Beauty 美人圈
讚 148
Joyce 島
季
讚 49
推薦您貼文串熱門影片，快來發掘更多精彩內容！
顯示項目設定
主頁
聊天
貼文串
TODAY
錢包


9:18
4G
設定
搜尋
個人檔案
我的帳號
隱私設定
移動帳號設定
Keep
貼圖
主題
鈴聲 / 來電答鈴
代幣
提醒
ON
照片・影片

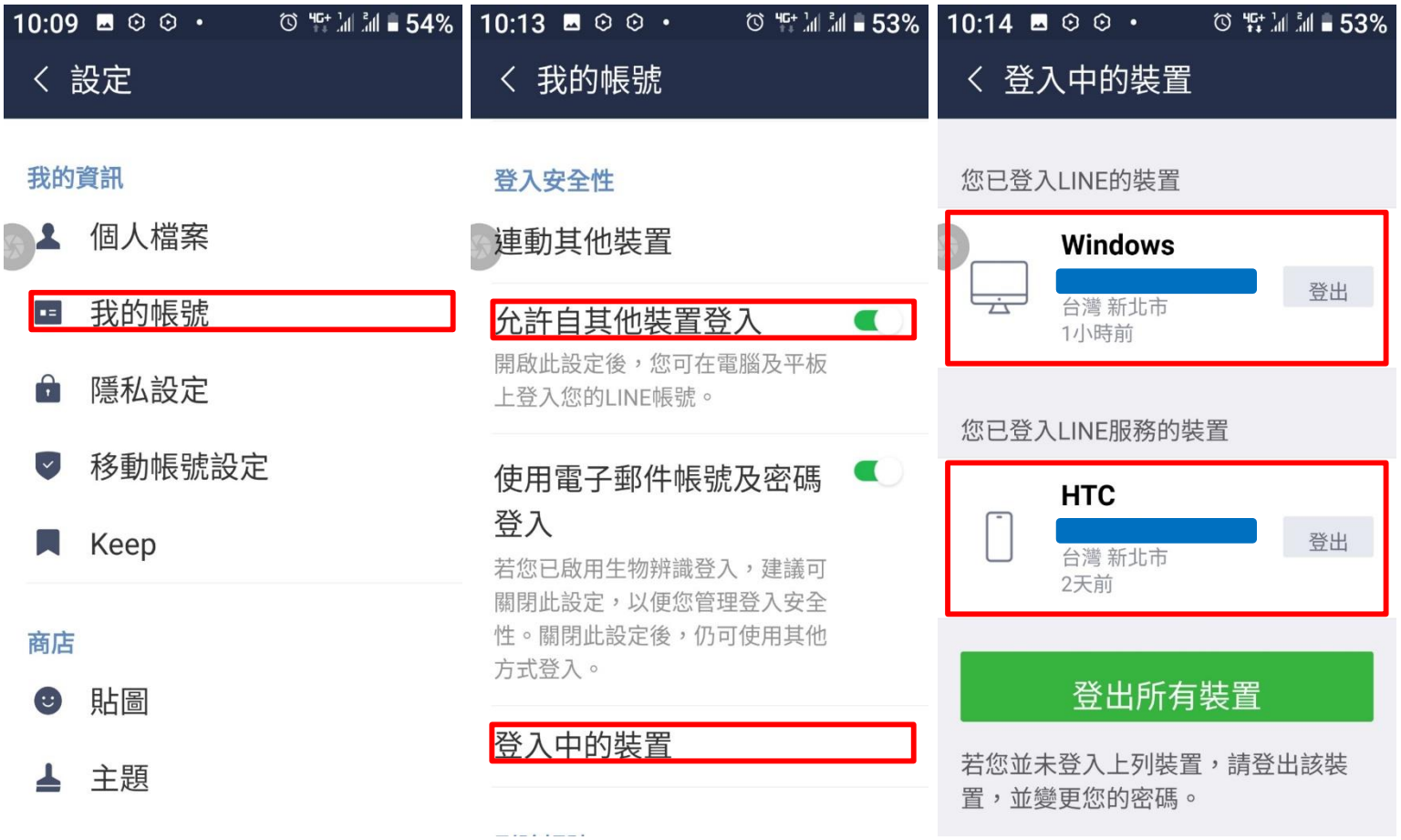

9:18
4G
隱私設定
密碼鎖定
允許利用 ID 加入好友
其他用戶可透過 ID 搜尋將您加入好友。
阻擋訊息
開啟本功能後即可阻擋不是來自好友的訊息。
Letter Sealing
使用進階加密功能可保護訊息。 但僅限於和同時開啟 Letter Sealing功能的好友聊天時有效。
更新行動條碼
外部應用程式存取
將您加入好友的用戶若允許外部應用程式存取其好友名單資料時，您在此處的設定可允許或拒絕該外部應用程式存取您的個人檔案。
提供使用資料

訊息加密功能-Android

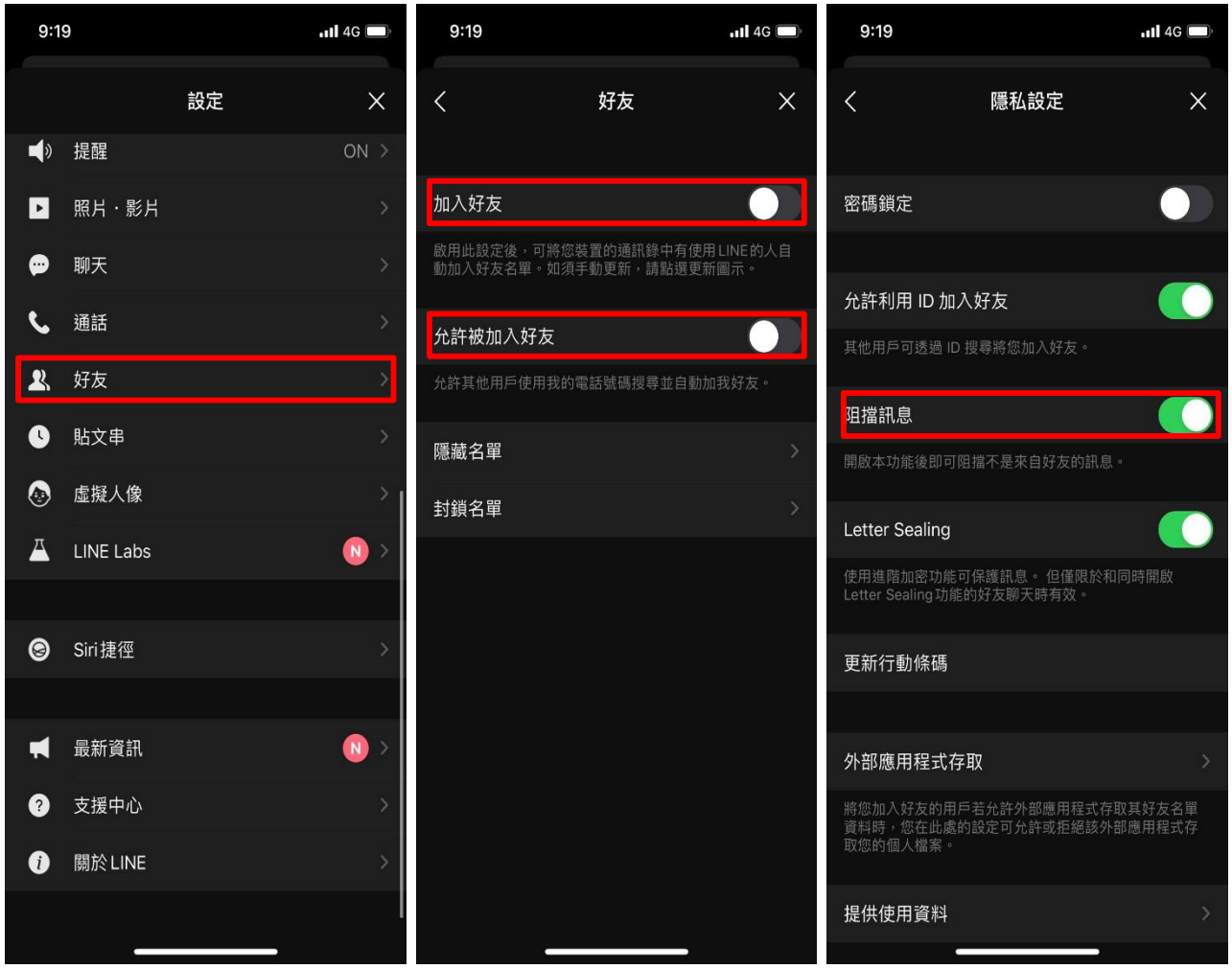
陌生裝置登入-IOS


9:18
4G
設定
搜尋
個人檔案
我的帳號
隱私設定
移動帳號設定
Keep
貼圖
主題
鈴聲 / 來電答鈴
代幣
提醒
ON
照片・影片
10:28
4G
我的帳號
連動中的應用程式
顯示項目
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，您可在電腦及平板上登入您的LINE帳號。
使用密碼登入
若您已啟用 Touch ID / Face ID 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
刪除帳號
10:28
4G
登入中的裝置
您已登入LINE的裝置
Windows
台灣 新北市
1小時前
登出
若您並未登入上列裝置，請登出該裝置，並變更您的密碼。
上列位置是根據裝置的IP位址所推測出的大略位置，與實際地理位置可能有所出入。

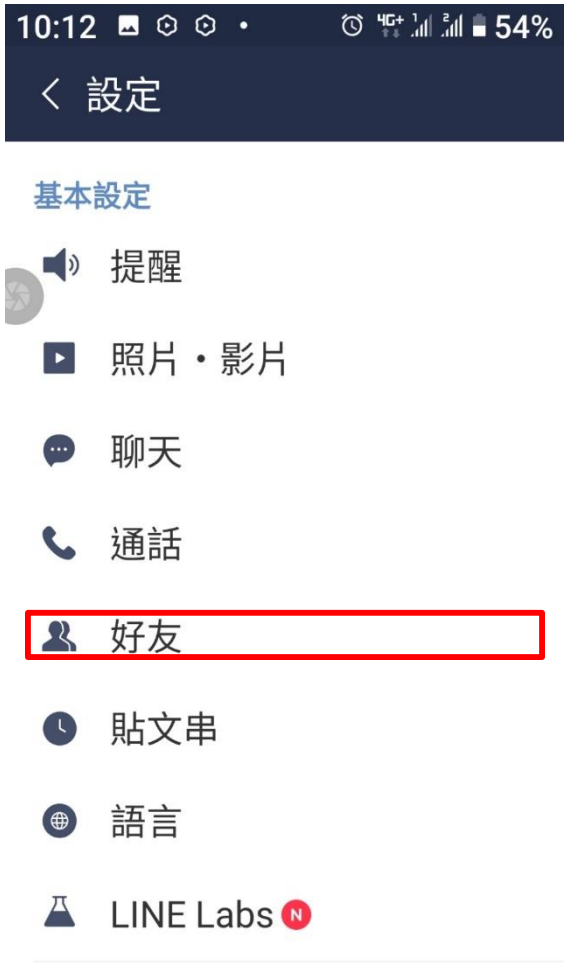
陌生裝置登入-Android



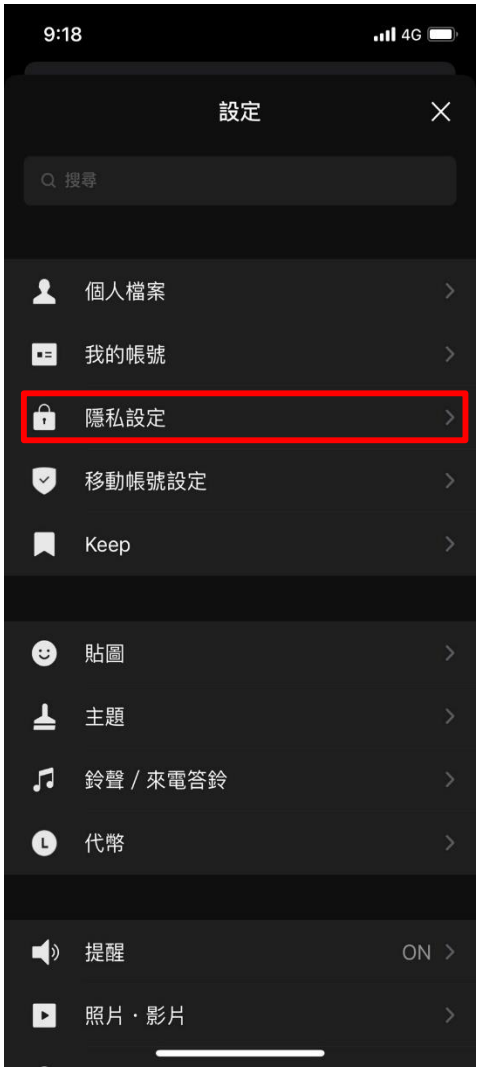
好友&隱私設定建議-IOS

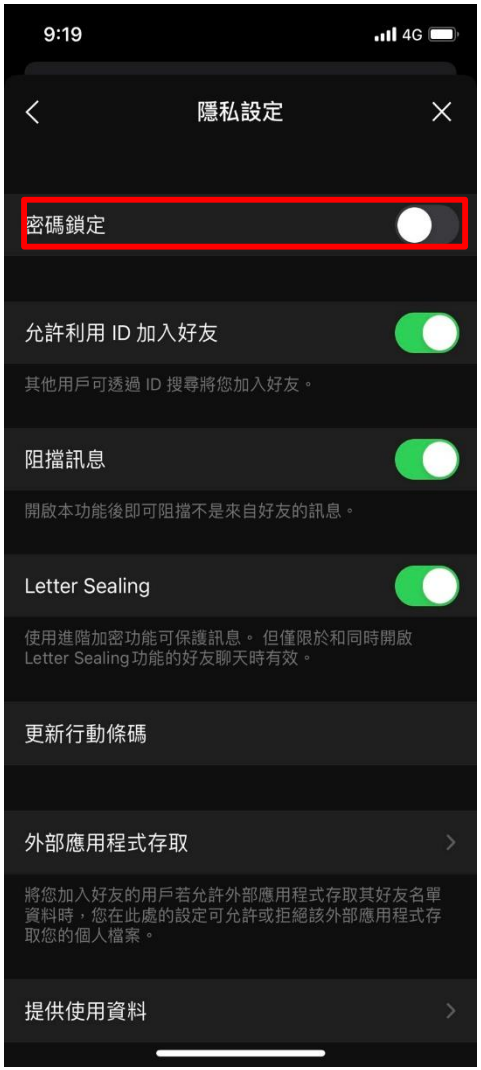


好友&隱私設定建議-Android



密碼鎖定-IOS


9:18
4G
設定
搜尋
個人檔案
我的帳號
隱私設定
移動帳號設定
Keep
貼圖
主題
鈴聲 / 來電答鈴
代幣
提醒
ON
照片・影片


9:19
4G
隱私設定
密碼鎖定
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


設定新密碼
請輸入新密碼
1
2
3
4
5
6
7
8
9
取消
0

密碼鎖定-Android

LINE 密碼鎖定功能

LINE的「其他」→「設定」→「隱私設定」。

避免添加不明 LINE ID 的人為朋友

LINE的「其他」→「設定」→「隱私設定」。

防止來自陌生人的消息

LINE的「其他」→「設定」→「隱私設定」。

LETTER SEALING

LINE的「其他」→「設定」→「隱私設定」。

外部應用程式存取

LINE的「其他」→「設定」→「隱私設定」→「外部應用程式存取」。

外部應用程式存取

LINE的「其他」→「設定」→「隱私設定」→「外部應用程式存取」。

提供資料使用

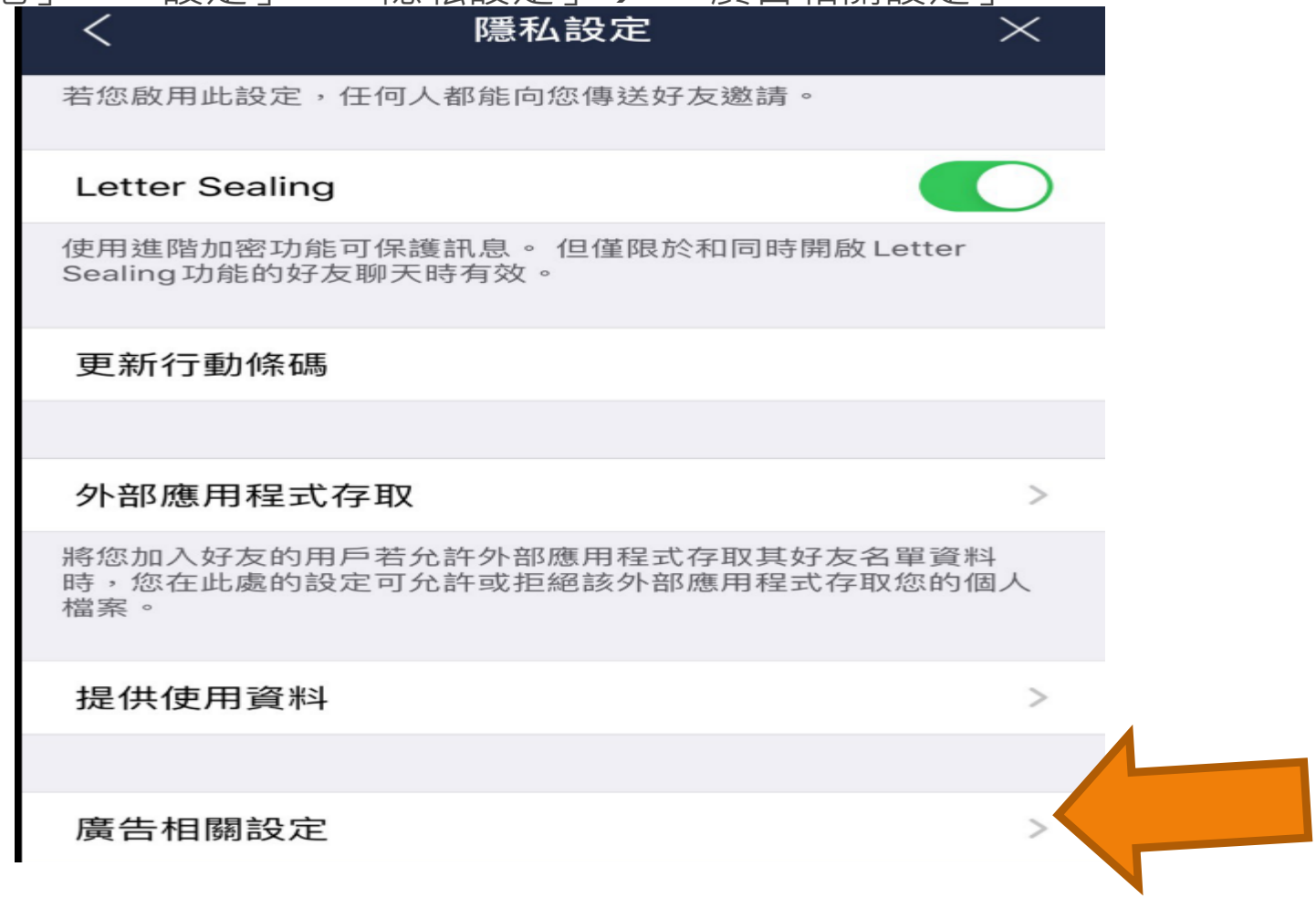
LINE的「其他」→「設定」→「隱私設定」→「提供資料使用」。

提供資料使用

LINE的「其他」→「設定」→「隱私設定」→「提供資料使用」。

廣告相關設定

LINE的「其他」→「設定」→「隱私設定」→「 廣告相關設定」 。



廣告相關設定

LINE的「其他」→「設定」→「隱私設定」→「 廣告相關設定」 。

LINE 我的帳號FB安全設定

LINE的「其他」→「設定」→「我的帳號」 。

LINE 我的帳號FB安全設定

LINE的「其他」→「設定」→「我的帳號」 。

檢查手機以外 LINE 的登錄狀態

LINE的「其他」→「設定」→「我的帳號」 。

檢查手機以外 LINE 的登錄狀態

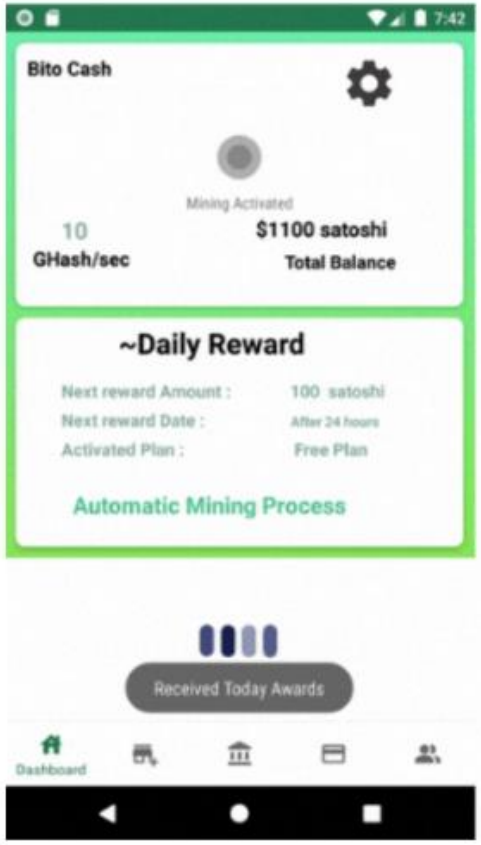
LINE的「其他」→「設定」→「我的帳號」 。

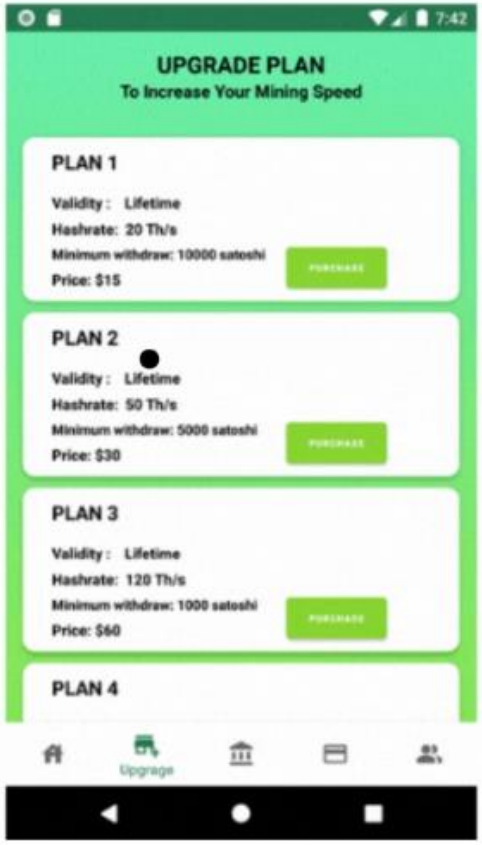
遠端工作介面模糊化衍伸的資安問題

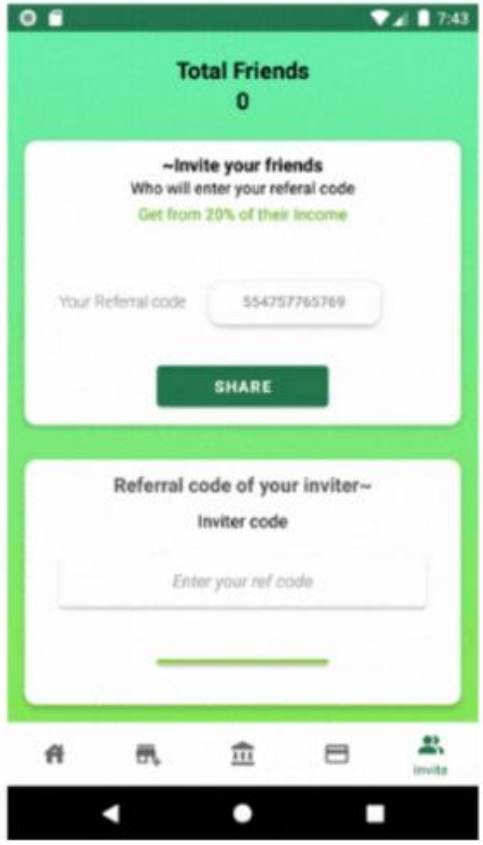
疫情資訊人心惶惶也成為一大誘餌，攻擊管道舉例來說，**電子郵件、假冒應用程式、惡意網域與社群等**，在企業遠距工作模式下，趨勢科技預期將有更多變臉詐騙 (Business Email Compromise, BEC) 出現，假冒供應商寄發銀行帳號或付款方式變更的郵件，企圖誘使企業員工匯款。而大眾對疫情資訊的迫切需求也將成為駭客入侵的機會點，駭客將持續利用與疫情相關的資訊散布釣魚郵件，引誘使用者點擊惡意連結或開啟惡意附件，以達到竊取個資等目的。

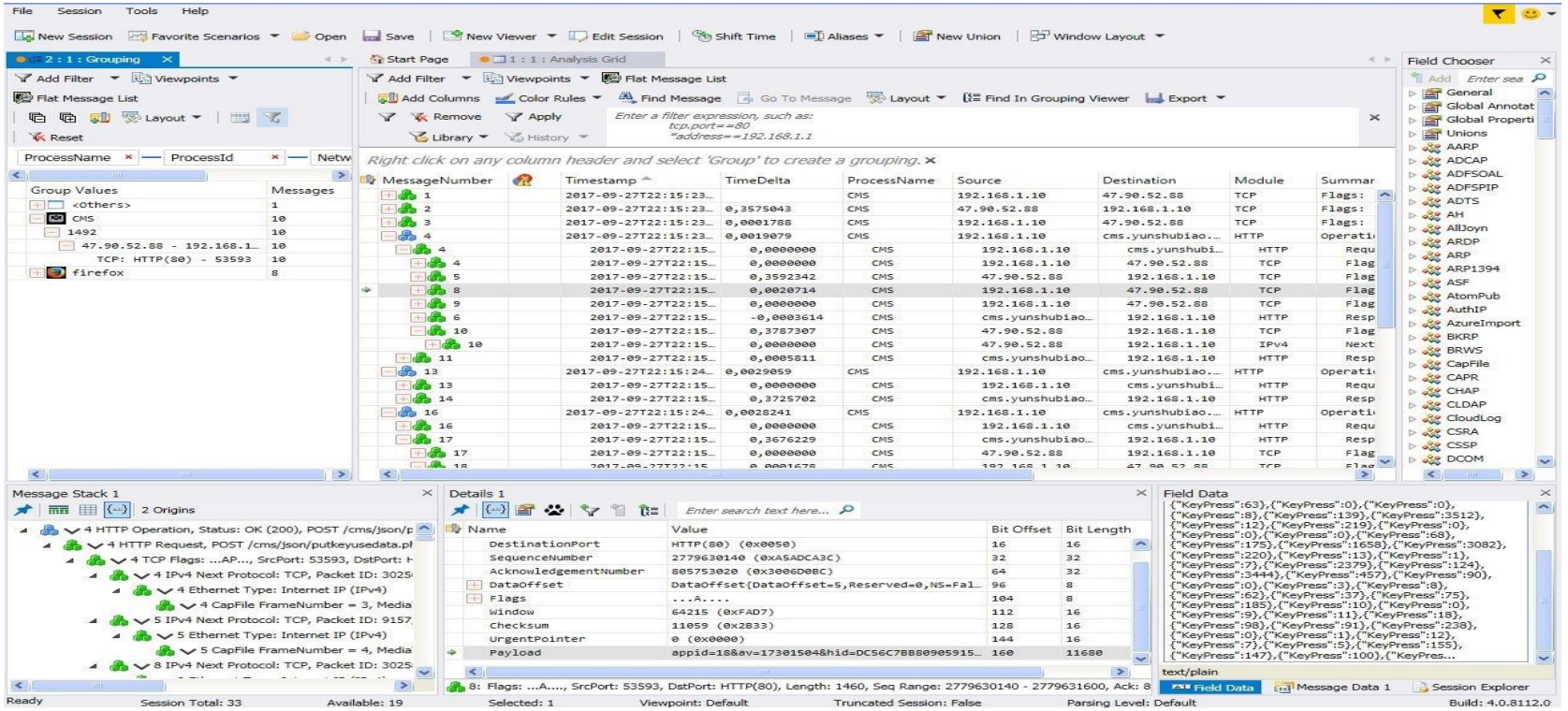
另外，在疫情期間不少公司**遠端辦公**，企業快速應變卻也造成資安上的漏洞，因為疫情形成混合辦公型態，使得邊界變模糊，趨勢科技認為駭客將利用家庭網路漏洞，對企業網路發動供應鏈攻擊，企圖找到 VPN 網路中具有關鍵數據或企業機密的目標，進一步攻擊以竊取企業資料。對此，零信任模式 (Zero Trust) 將在明年成為企業安全策略關鍵點之一，如何落實安全存取可視性及提升訪問資料的管理權限，將為企業防禦佈局重點。

Android用戶別上當！9萬人中招 Google Play 25款挖礦APP騙錢









云鼠标平台后台管理系统

Cloud mouse platform background management system

用户名:

密码:

记住密码

登录

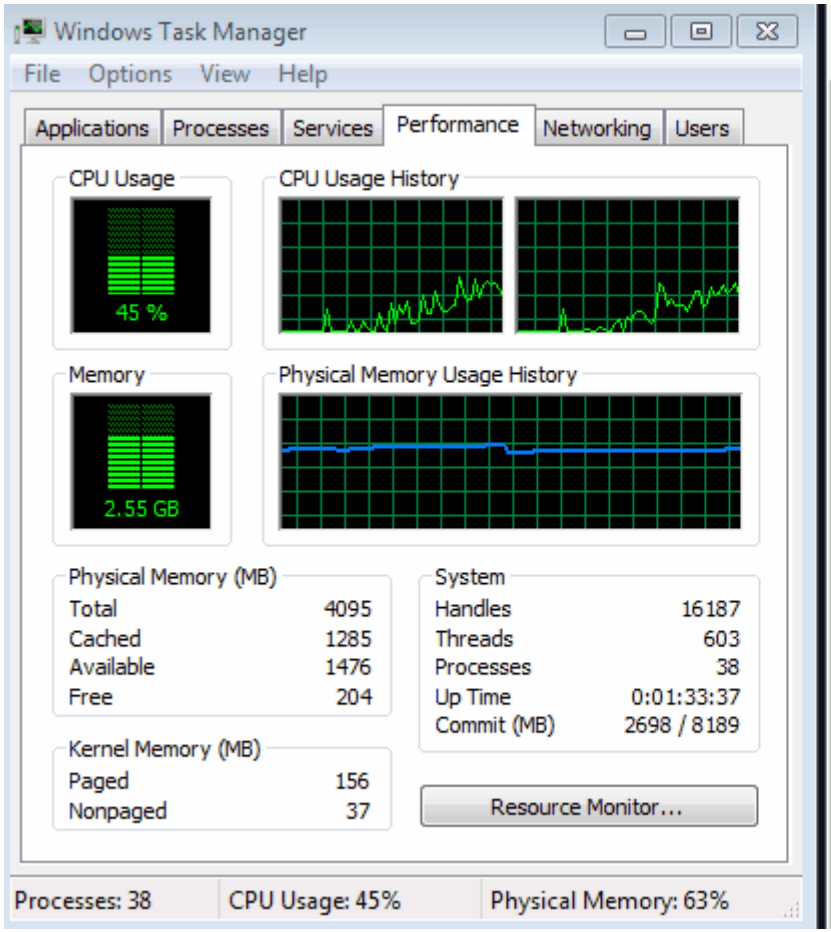
忘记密码 ^_^?

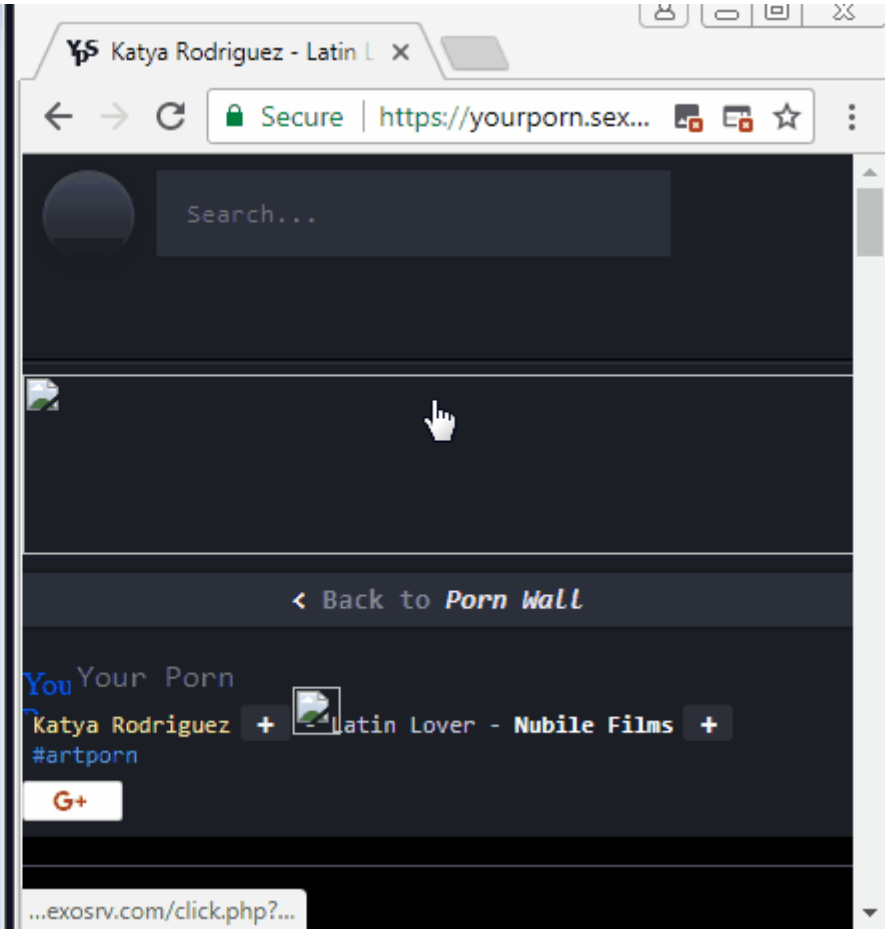
显示不好？建议使用支持HTML5技术的浏览器。

```
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "appid" = "18"
  Form item: "av" = "17301504"
  Form item: "hid" = "DC56C7BB809059157858C873C7B490DE705ED4FBB9DC0C617FF373F
  Form item: "uid" = "0"
  Form item: "did" = "280379760100190"
  Form item: "data" = "[{"KeyPress":1},{"KeyPress":0},{"KeyPress":78},{"KeyPr
```

```
  9 0.720896600   192.168.1.10   47.90.52.88   HTTP   725 POST /cms/json/putkeyusedata.php HTTP/1.1  (application/x-www-form-urlencoded
 13 1.102752900   192.168.1.10   47.90.52.88   HTTP   382 POST /cms/json/putuserevent.php HTTP/1.1  (application/x-www-form-urlencoded)
 16 1.478147200   192.168.1.10   47.90.52.88   HTTP   382 POST /cms/json/putuserevent.php HTTP/1.1  (application/x-www-form-urlencoded)
 19 1.859513200   192.168.1.10   47.90.52.88   HTTP   382 POST /cms/json/putuserevent.php HTTP/1.1  (application/x-www-form-urlencoded)
```

綁架挖礦又有新招


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
45 %
CPU Usage History
Memory
2.55 GB
Physical Memory Usage History
Physical Memory (MB)
Total 4095
Cached 1285
Available 1476
Free 204
System
Handles 16187
Threads 603
Processes 38
Up Time 0:01:33:37
Commit (MB) 2698 / 8189
Kernel Memory (MB)
Paged 156
Nonpaged 37
Resource Monitor...
Processes: 38
CPU Usage: 45%
Physical Memory: 63%


Katya Rodriguez - Latin L
Secure https://yourporn.sex...
Search...
Back to Porn Wall
You Your Porn
Katya Rodriguez + Latin Lover - Nubile Films +
#artporn
G+
...exosrv.com/click.php?...

惡意病毒軟體應用程式

惡意系統優化應用程式

Speed Clean-Phone Booster,Junk Cleaner&App Manager

Michael.Speed Tools ★★★★★ 4,534

3+

Contains Ads

You don't have any devices.

Super Clean-Phone Booster,Junk Cleaner&CPU Cooler

SuperClean Tools ★★★★½ 7,753

3+

Contains Ads

You don't have any devices.

LinkWorldVPN

linkworld Tools ★★★★★ 6

3+

Contains Ads

You don't have any devices.

Add to Wishlist

Shoot Clean-Junk Cleaner,Phone Booster,CPU Cooler

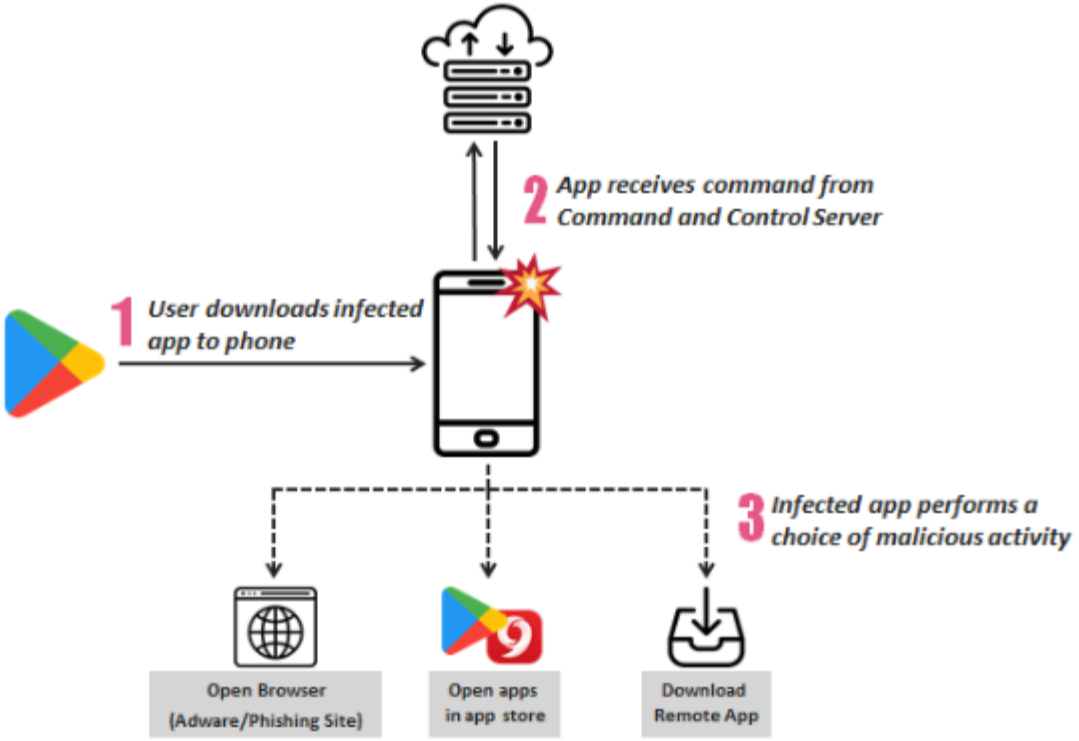
shootclean Tools ★★★★★ 614

3+

Contains Ads

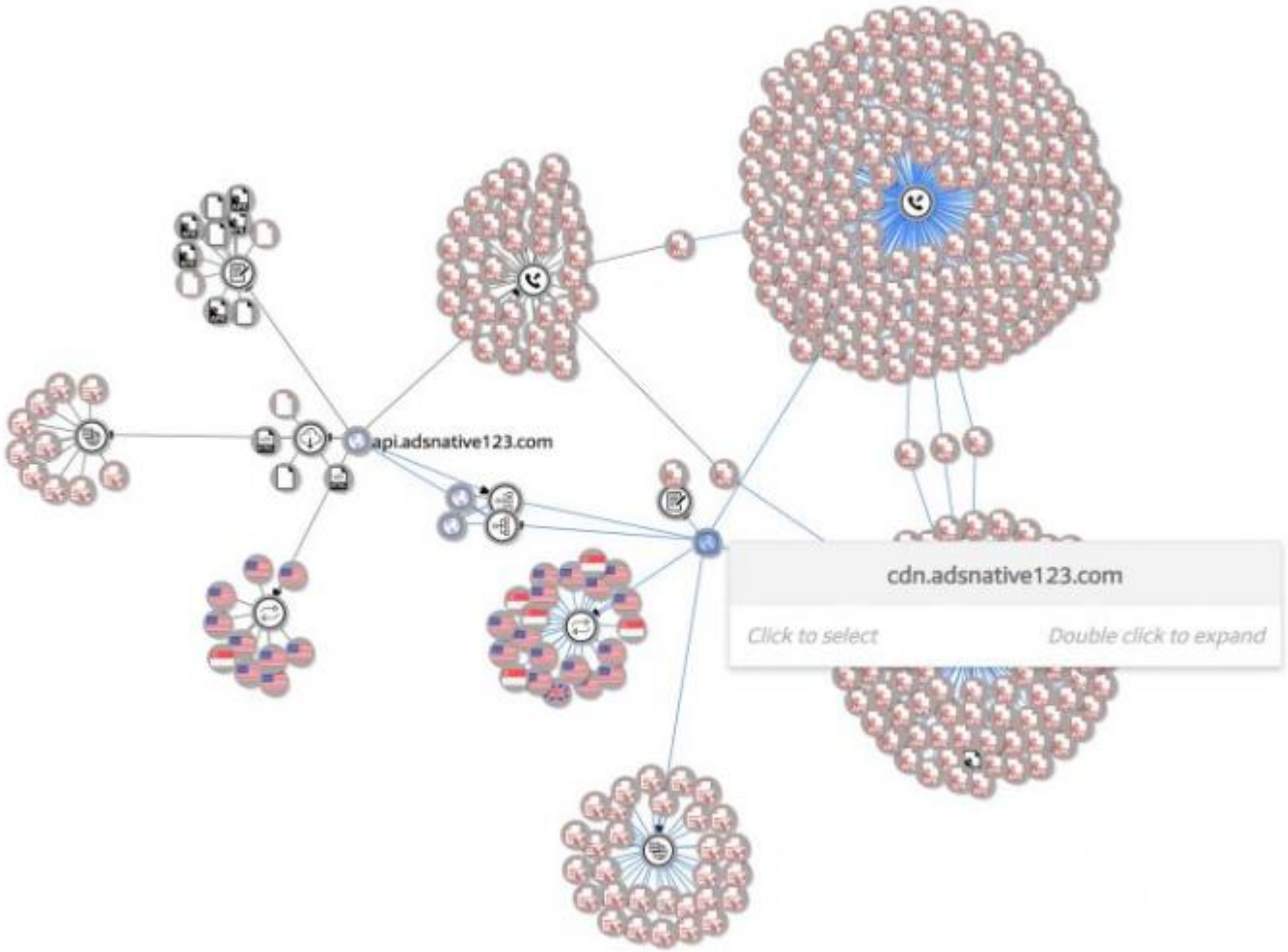
You don't have any devices.

SIMBAD 是種軟體開發套件病毒，下載被感染的 APP 就會被傳染

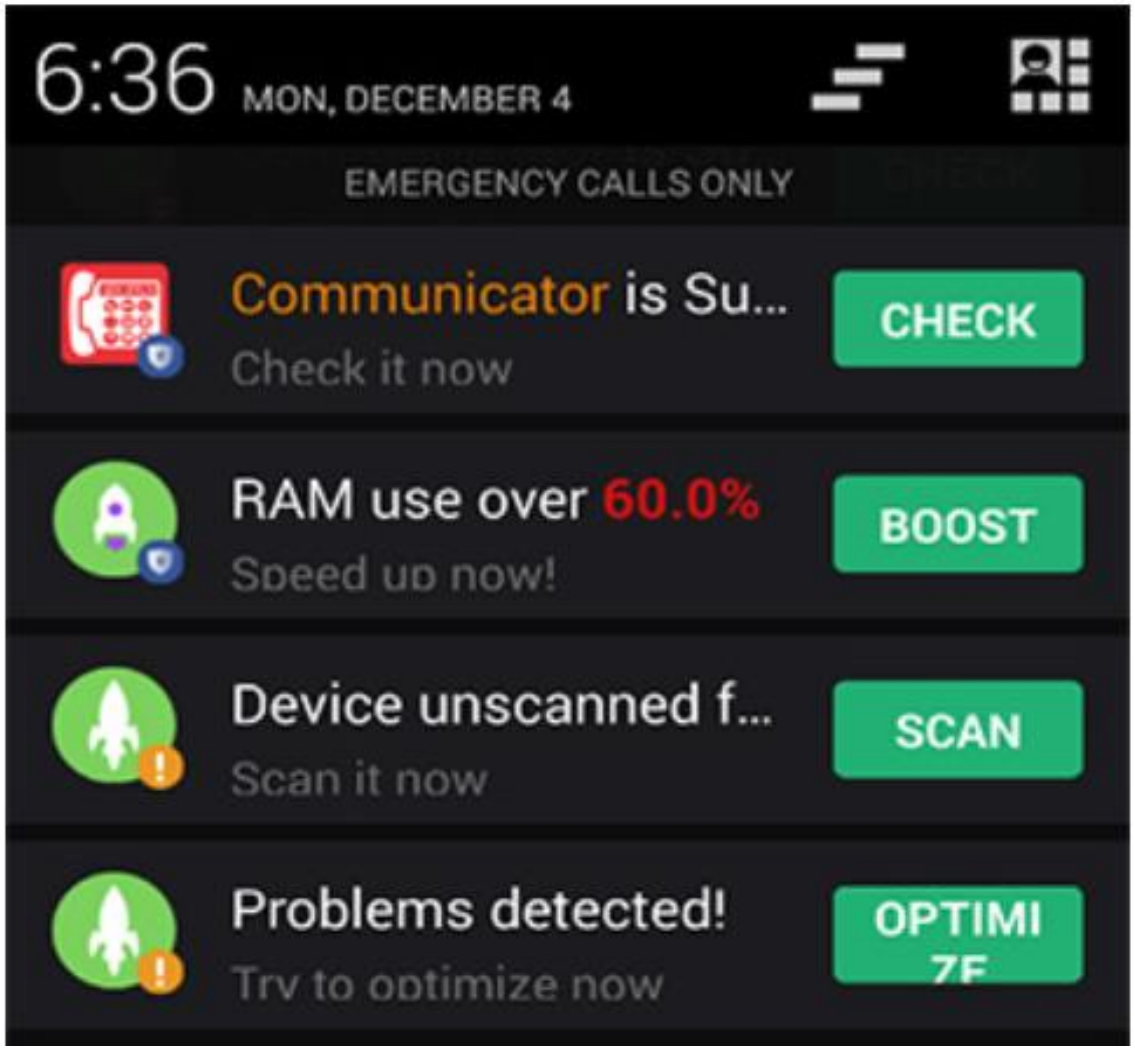


SimBad 攻擊流程圖。圖片來源：Check Point

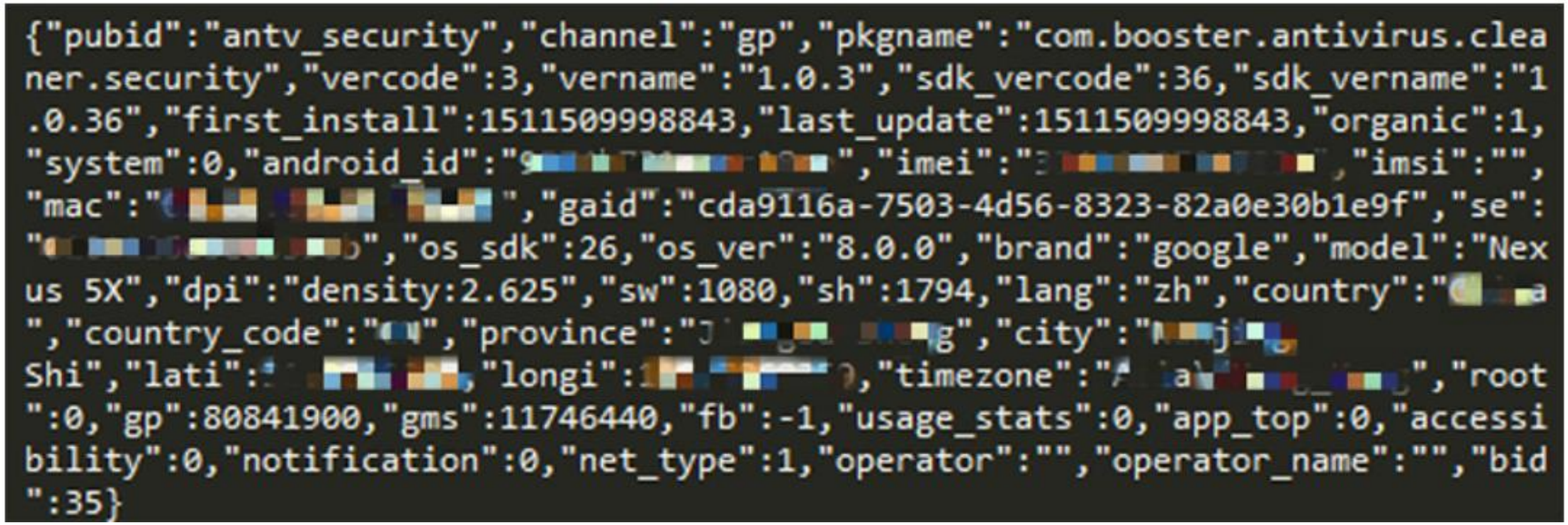
惡意廣告伺服器關聯示意圖



假防毒真騙點擊 的廣告應用程式

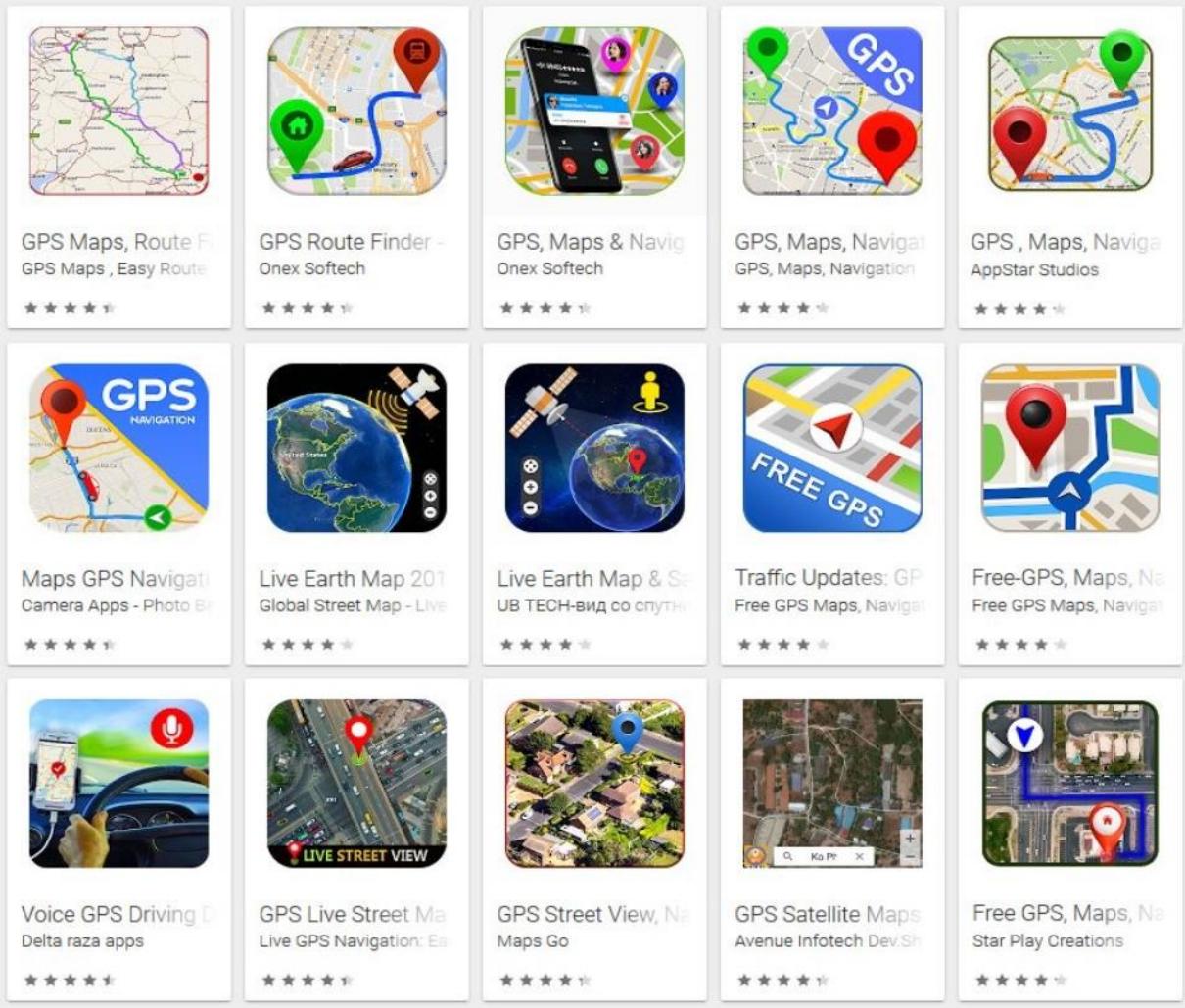


假防毒真騙點擊 的廣告應用程式

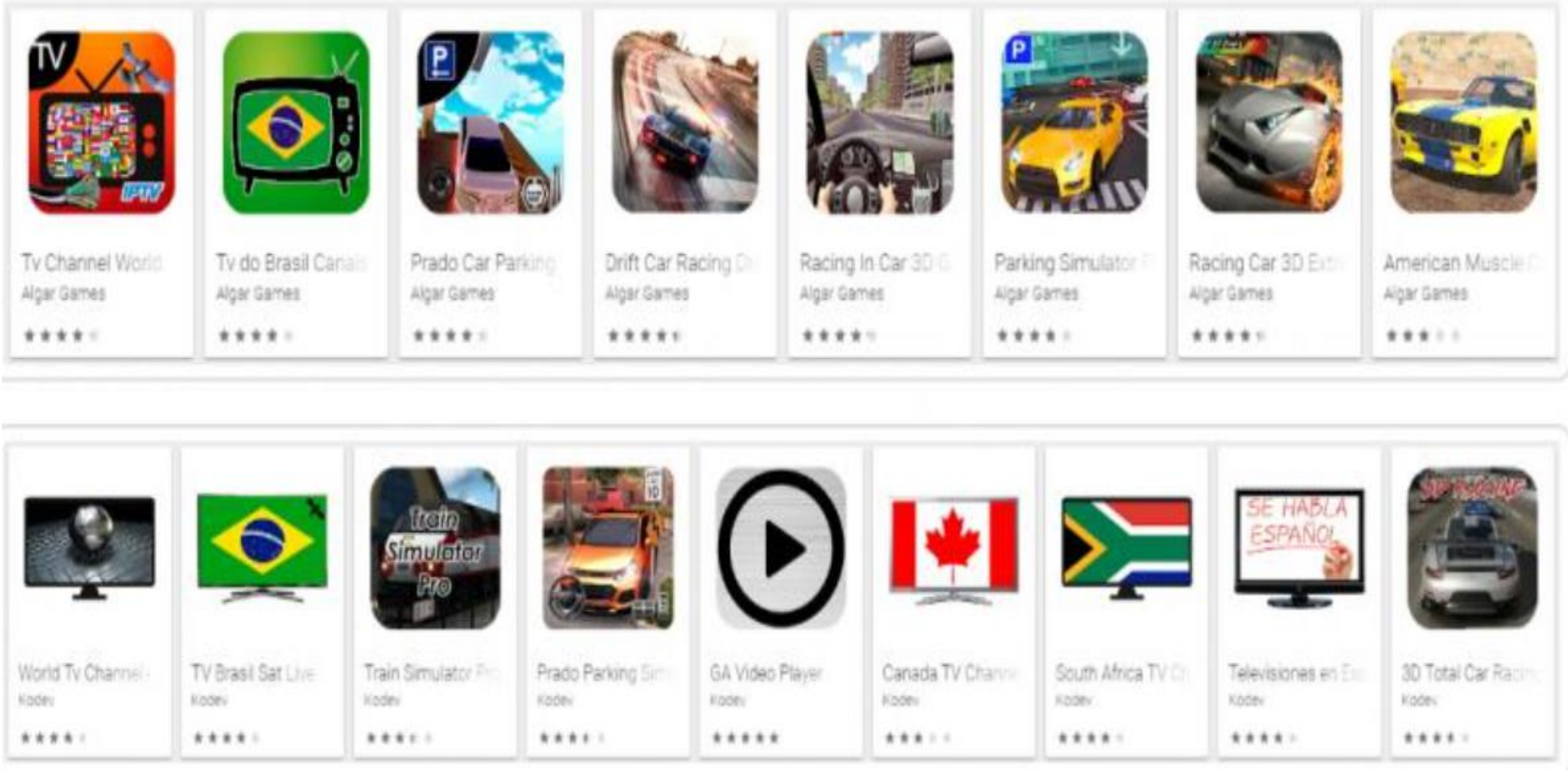


祕密收集使用者數據、所安裝的應用程式等資訊，追蹤使用者所在位置並大量推送各種廣告到手機上，沒錯！它的目的就是藉由現代人對於手機安全意識的模糊以廣告轟炸方式牟利。另一個有趣的事是下載和安裝這些應用程序之一的使用者都會被要求同意EULA（最終用戶許可協議），該協議描述了應用程序將收集和使用的信息傳送到遠端伺服器，不過大多數人應該都不會仔細閱讀就直接點選同意。

假導航APP流竄使用免費的GOOGLE地圖



惡意廣告程式家族


Tv Channel World
Algar Games
Tv do Brasil Canais
Algar Games
Prado Car Parking
Algar Games
Drift Car Racing
Algar Games
Racing In Car 3D
Algar Games
Parking Simulator
Algar Games
Racing Car 3D
Algar Games
American Muscle
Algar Games
World Tv Channel
Kodev
TV Brasil Sat Live
Kodev
Train Simulator Pro
Kodev
Prado Parking
Kodev
GA Video Player
Kodev
Canada TV Channel
Kodev
South Africa TV
Kodev
Televisiones en
Kodev
3D Total Car Racing
Kodev

電信帳單無故暴增？美顏修圖 App 詐騙新手法

應用程式 App 下載後，確實也有提供相關攝影功能，但同時卻也夾帶暗藏有惡意軟體程式，不但可竊取識別用戶個人身份的資訊，甚至還可藉此進行網路詐騙。


陶板屋
陶板屋
今天
雙人份套餐禮卷點此領取
立即確認
下午4:13
請點擊上方【立即確認】
系統會自動發送給您西堤禮卷條碼
拿到條碼的人,可以自行去陶板屋享用哦
本平台不會向你索取個人資料
下午4:13
詐騙

選擇 3 個群組或 10 位好友

將自動套用至禮物盒即可使用

「分享」- 詐騙者常用技倆，迅速擴大受害範圍

Line的帳號有三種顏色:

灰色盾牌: 任何人可申請，Line@的普通帳號

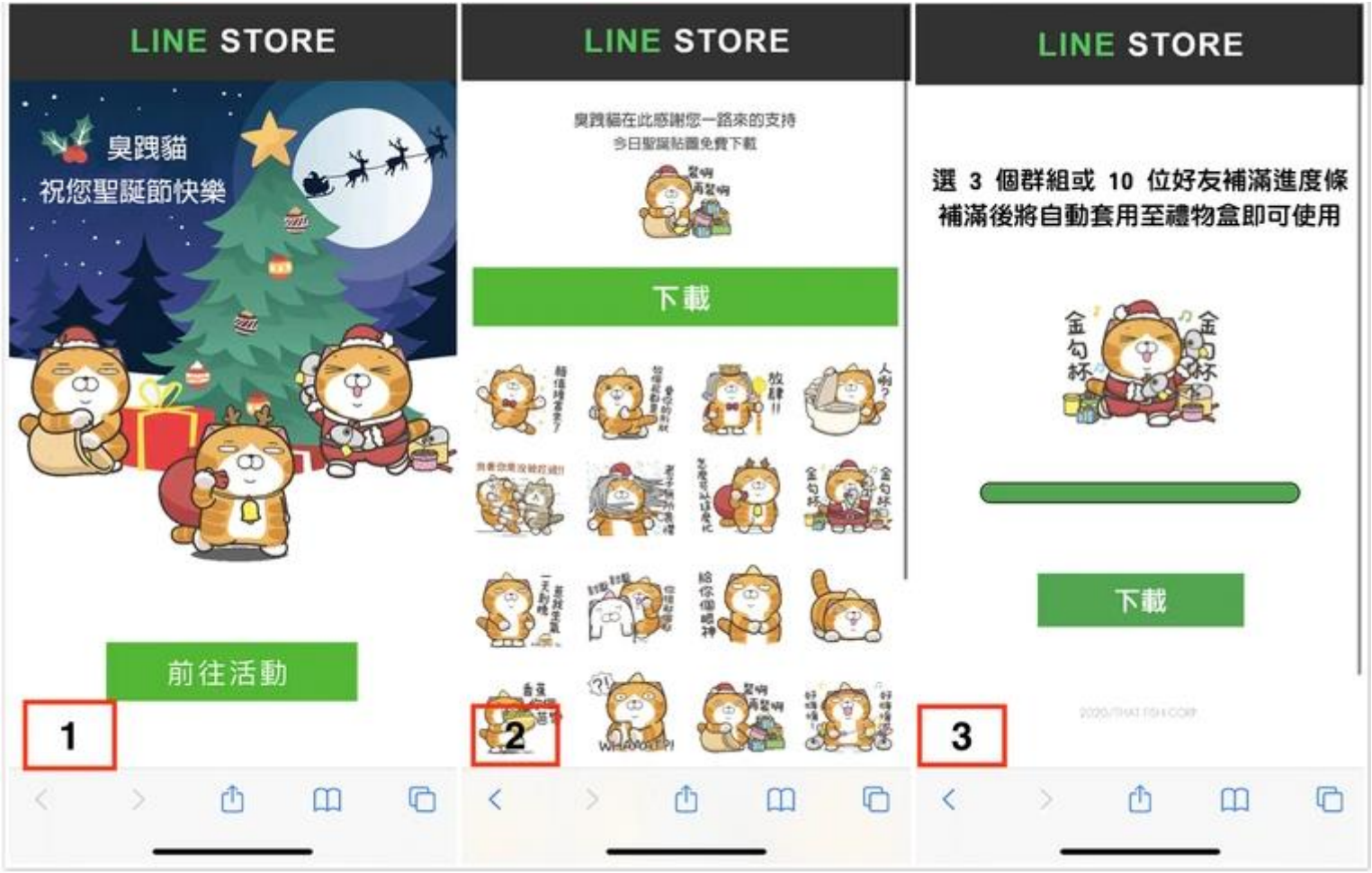
藍色盾牌: Line@的認證帳號

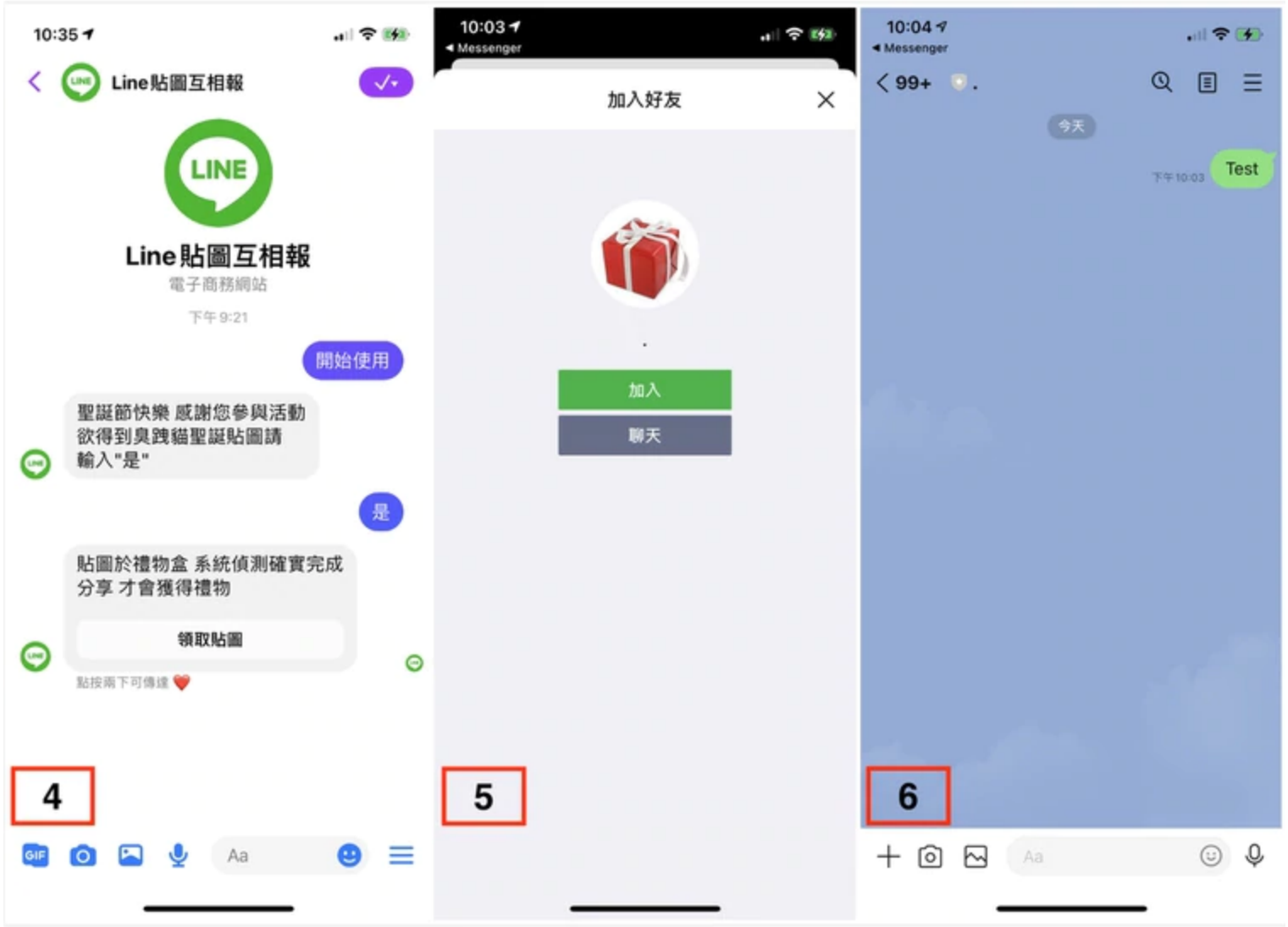
綠色盾牌: Line的官方帳號

LINE周年免費貼圖抽獎

開始抽貼圖


臭跩貓~陪你過聖誕
https://www.safesafe01.com/blank
LINE STORE
選 3 個群組或 10 位好友補滿
補滿後將自動套用至禮物
金勾杯
下載
2020/THAT FISH CORP
臭跩貓~陪你過聖誕
https://www.lineoutlet.org/
LINE STORE
臭跩貓
節快樂
前往活動
2020/THAT FISH CORP
詐騙
網站

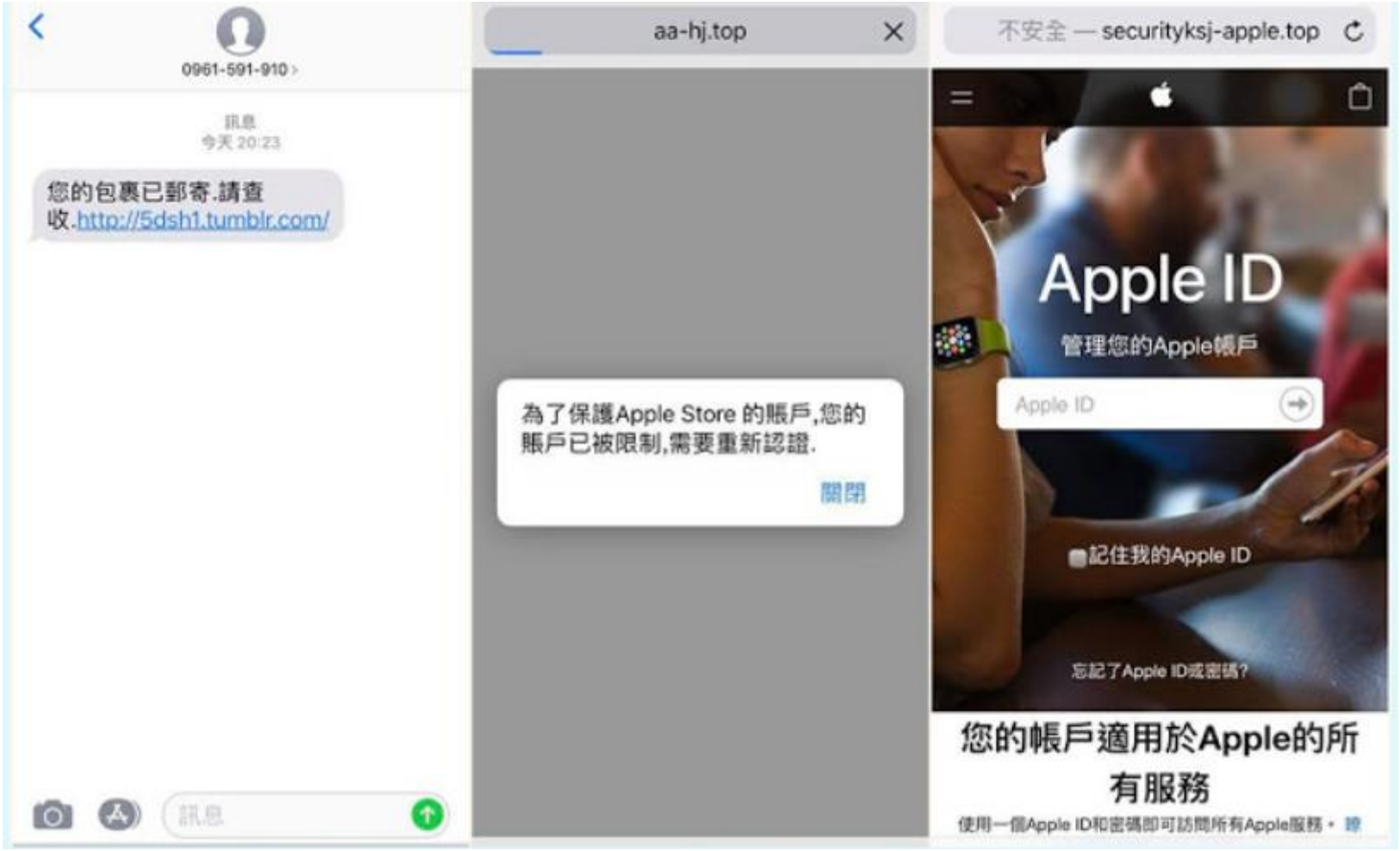

LINE STORE
臭賤貓
祝您聖誕節快樂
前往活動
1
LINE STORE
臭賤貓在此感謝您一路來的支持
今日聖誕貼圖免費下載
下載
2
LINE STORE
選 3 個群組或 10 位好友補滿進度條
補滿後將自動套用至禮物盒即可使用
下載
3


10:35
Line貼圖互相報
LINE
Line貼圖互相報
電子商務網站
下午 9:21
開始使用
聖誕節快樂 感謝您參與活動
欲得到臭賤貓聖誕貼圖請
輸入"是"
是
貼圖於禮物盒 系統偵測確實完成
分享 才會獲得禮物
領取貼圖
點按兩下可傳遞
4
Aa
10:03
Messenger
加入好友
加入
聊天
5
10:04
Messenger
99+
今天
Test
下午 10:03
6
Aa

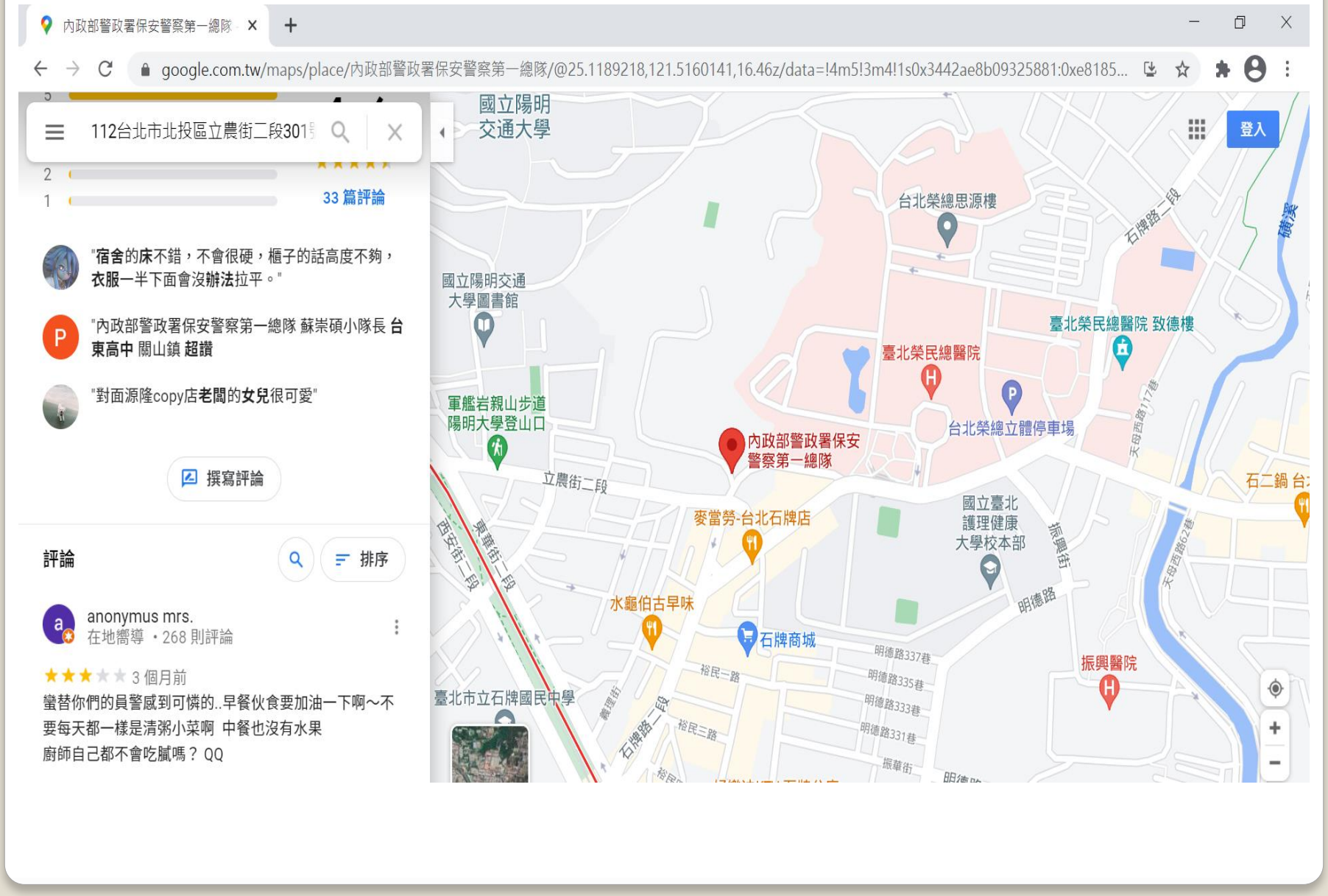
▼假帳號4大特徵。（圖／LINE@生活圈提供）

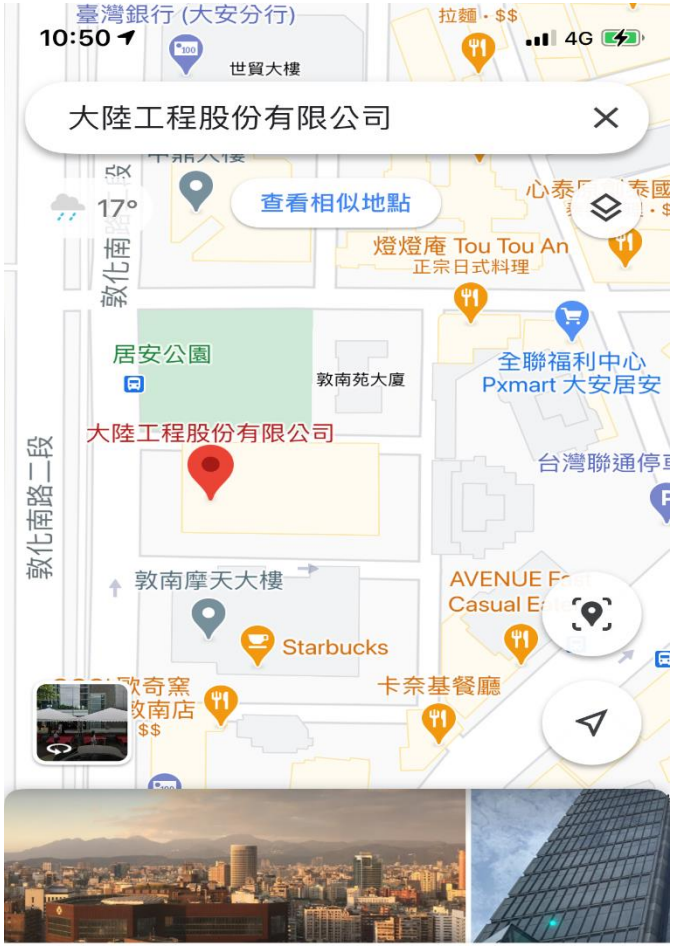
原始詐騙訊息版本：

> 預計送貨日期：04月08日（星期三）請確認地址 https://bit＊ly/34hVLXn


0961-591-910
訊息
今天 20:23
您的包裹已郵寄,請查收.http://5dsh1.tumblr.com/
訊息
aa-hj.top
為了保護Apple Store 的賬戶,您的賬戶已被限制,需要重新認證.
關閉
不安全 — securityksj-apple.top
Apple ID
管理您的Apple帳戶
Apple ID
記住我的Apple ID
忘記了Apple ID或密碼?
您的帳戶適用於Apple的所有服務
使用一個Apple ID和密碼即可訪問所有Apple服務。


內政部警政署保安警察第一總隊
google.com.tw/maps/place/內政部警政署保安警察第一總隊/@25.1189315,121.5148799,17z/data=!4m5!3m4!1s0x3442ae8b09325881:0xe8185f9...
112台北市北投區立農街二段301號
內政部警政署保安警察第一總隊
The First Special Police Corps National Police Agency Ministry of the Interior
內政部警政署保安警察第一總隊
4.6 33 則評論
警察局
規劃路線
儲存
附近
傳送到你的手機
分享
112台北市北投區立農街二段301號
02 2821 8137
4G98+HR 北投區 台北市
運動場
登入
台北榮總思源樓
臺北榮總急診部
臺北榮民總醫院
台北榮總立體停
全家便利商店 北榮店
便利商店
明曜清潔服務社
國立陽明交通大學圖書館
國立陽明大學停車場
衛生福利部國家中醫藥研究所
軍艦岩親山步道陽明大學登山口
日日文創舖
文具店
好日子咖啡
內政部警政署保安警察第一總隊
臺北榮民總醫院第一門診
台北榮民總醫院二號門地下室停車場
石牌路二段
立農街二段
客來海鮮庭園餐廳
海鮮料理 • $$
Panmills studio
7-ELEVEN 安遠門市
便利商店
潤聖影印店
麥當勞-台北石牌店
速食 • $
幸福養心站
親仁樓
北投石牌郵局
台中無障礙計程車
國立臺北護理健康大學校本部
石牌商城
水龜伯古早味
雲鼎阿二麻辣食堂石牌店
開立醫療器材股份有限公司
明德路
裕民一路
明德路335巷
明德路333巷
東華街二段
西安街二段
衛星
Google
財鍋貼水餃專賣店


內政部警政署保安警察第一總隊
google.com.tw/maps/place/內政部警政署保安警察第一總隊/@25.1189218,121.5160141,16.46z/data=!4m5!3m4!1s0x3442ae8b09325881:0xe8185...
112台北市北投區立農街二段301
2
1
33 篇評論
"宿舍的床不錯，不會很硬，櫃子的話高度不夠，衣服一半下面會沒辦法拉平。"
"內政部警政署保安警察第一總隊 蘇崇碩小隊長 台東高中 關山鎮 超讚
"對面源隆copy店老闆的女兒很可愛"
撰寫評論
評論
排序
anonymus mrs.
在地嚮導 • 268 則評論
3 個月前
蠻替你們的員警感到可憐的..早餐伙食要加油一下啊～不要每天都一樣是清粥小菜啊 中餐也沒有水果
廚師自己都不會吃膩嗎？ QQ
國立陽明交通大學
登入
台北榮總思源樓
國立陽明交通大學圖書館
臺北榮民總醫院 致德樓
臺北榮民總醫院
台北榮總立體停車場
軍艦岩親山步道
陽明大學登山口
內政部警政署保安警察第一總隊
立農街二段
麥當勞-台北石牌店
國立臺北護理健康大學校本部
水龜伯古早味
石牌商城
振興醫院
臺北市立石牌國民中學
石牌路二段
裕民二路
裕民三路
明德路
明德路337巷
明德路335巷
明德路333巷
明德路331巷
振華街
振興街
西安街二段
東華街二段
天母西路117巷
天母西路62巷
石二鍋 台
橫溪


臺灣銀行 (大安分行)
10:50
4G
世貿大樓
拉麵 · $$
大陸工程股份有限公司
查看相似地點
17°
燈燈庵 Tou Tou An
正宗日式料理
敦化南
居安公園
敦南苑大廈
全聯福利中心
Pxmart 大安居安
大陸工程股份有限公司
台灣聯通停
敦化南路二段
敦南摩天大樓
AVENUE F
Casual E
Starbucks
卡奈基餐廳
大陸工程股份有限公司
4.2 (100)
建築公司 · 14 分鐘
營業中 · 將於下午 5:30 結束營業
路線
開始
致電
儲存


10:50
4G
大陸工程股份有限...
總覽
評論
相片
相片
全部
街景服務和 360 度相片
新增相片
大陸工程股份有限公司
敦化南路二段
評論摘要
4.2
(100)
"高級且氣派的環境，唯獨洽公時附近車位難找，前往之前須注意"

狂被盜照！苦主曝「319個假帳號」都詐騙 網傻眼：有看過你

2021-04-12 11:02 聯合新聞網 / 綜合報導

+ 詐騙集團


dob Studio의 AI 기술로 만들어진 가상얼굴입니다.
Her face is AI-made virtual face by dob Studio.

一頁式詐騙廣告夾帶在 Yahoo 首頁熱門新聞中!

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

TREND MICRO 趨勢科技

一頁式詐騙廣告穿插在Yahoo 熱門新聞中,受害者難以分辨

Fan Cold
5月16日上午10:29

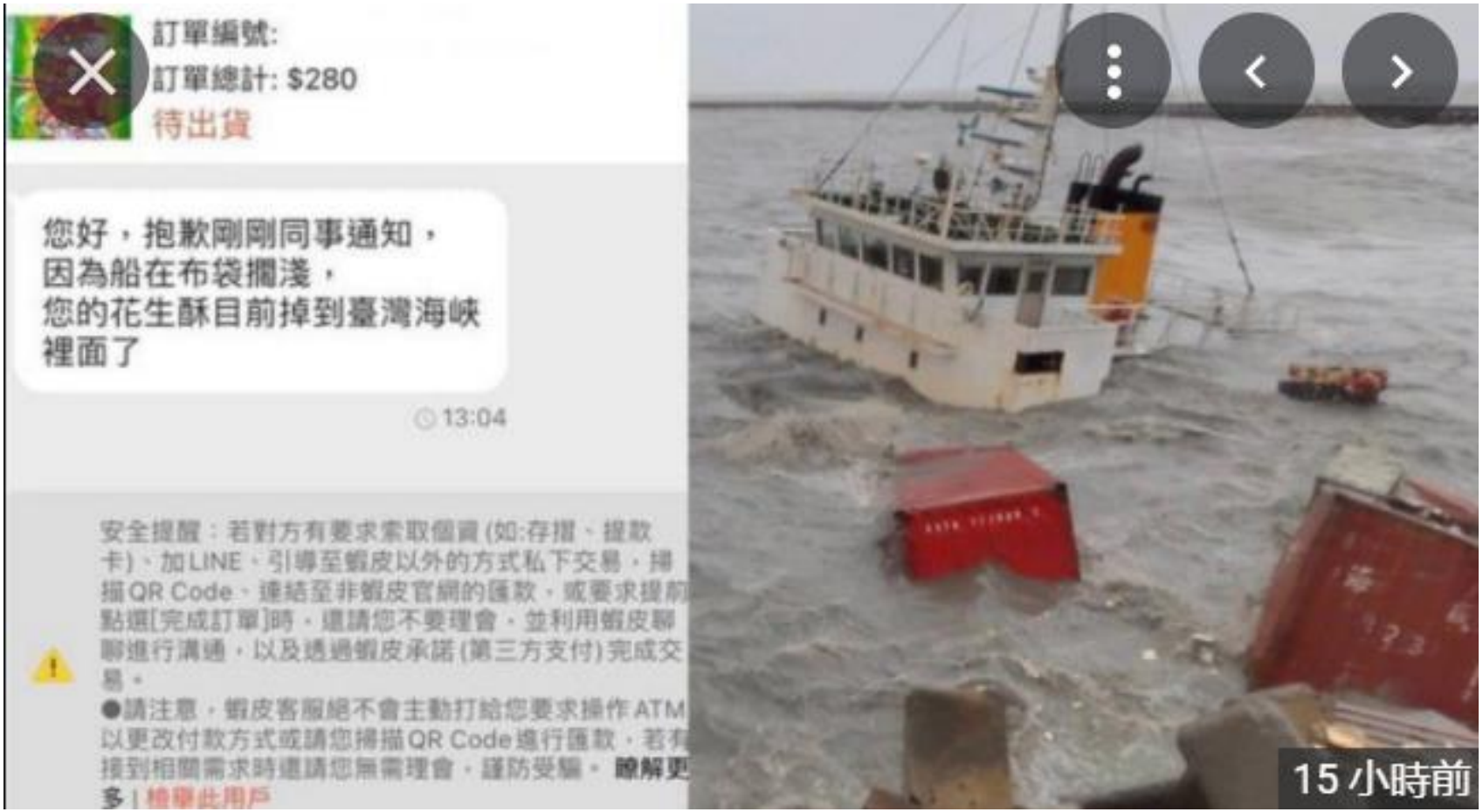
【專櫃豪華彈潤保養精華組合】限時出清大特價！

～知名女星代言限量專櫃保養品精華禮盒～
‼️原價NT$10588【限時下殺】只要NT$2588‼️

👇內容物誠意滿滿👇
玫瑰經典化妝水300ml x1
玫瑰萃取淨白乳液200ml x1
毛孔緊緻精華液100ml x1
水光保濕面膜1盒（6入）
美白透亮洗面乳200ml x1
潤澤卸妝凝露150ml x1

你還在等什麼？限量300組要搶要快！
購買連結：fancold2.shop.com


4大疑點揭穿網購詐騙！
單一商品
網站為單一網頁，而且只販賣一種商品？
小心可能是「一頁式詐騙網站」！
名人推薦
盜取名人照片並 P 圖偽冒的詐騙層出不
窮，務必去本人的社群帳號查證！
限時特價
以「高價品、低價賣」的手法吸引目光，
以聳動標題、活動倒數計時等引誘上鉤！
強調保障
強調「貨到付款有保障」或有「七天鑑賞期」
，民眾發現包裹內容物不符後卻求償無門！
whoscall


訂單編號:
訂單總計: $280
待出貨
您好，抱歉剛剛同事通知，
因為船在布袋擱淺，
您的花生酥目前掉到臺灣海峽
裡面了
13:04
安全提醒：若對方有要求索取個資(如:存摺、提款
卡)、加LINE、引導至蝦皮以外的方式私下交易，掃
描QR Code、連結至非蝦皮官網的匯款，或要求提前
點選[完成訂單]時，還請您不要理會，並利用蝦皮聊
聊進行溝通，以及透過蝦皮承諾(第三方支付)完成交
易。
●請注意，蝦皮客服絕不會主動打給您要求操作ATM
以更改付款方式或請您掃描QR Code進行匯款，若有
接到相關需求時還請您無需理會，謹防受騙。 瞭解更
多 | 檢舉此用戶
15 小時前

假訊息查證參考資訊

TFC 台灣事實查核中心
官方網站：https://www.facebook.com/taiwantfc
點我直接加Line：http://line.me/ti/p/%40rqd9861a

Line 訊息查證
官方網站：https://fact-checker.line.me/
點我直接加Line：http://line.me/ti/p/@linefactchecker

蘭姆酒吐司
官方網站：https://www.rumtoast.com/
點我直接加Line：https://line.me/R/ti/p/1q14ZZ8yjb

MyGoPen
官方網站：https://www.mygopen.com

遠端工作潮 居家網路風險提升

在疫情下成為辦公空間的家庭，聯網設備也越來越多，如今也可能成為駭客的攻擊對象，尤其在家庭路由器。
趨勢科技預測家用路由器將成為駭客入侵家庭網路的首要目標，同時出售路由器家庭網路訪問權限的新興商業模式也將出現，尤其是企業高層或是 IT 管理人員的網路權限更有價值，可能存在更高的風險，大家應該特別將家庭網路納入資安防護重點。


中保無限 智慧宅
9大功能
方案介紹
操作介面
申裝流程
我有興趣
AI智能安檢
智慧連動 | 月租只要2,000元 起
智慧電子門鎖
溫濕度顯示
家電控制
燈光控制
※本方案為預設之基本標準配備 您可依據您的實際需求額
dormakaba
方案介紹
我有興趣

飛利浦智能居家
2019年6月24日 ·

#飛利浦智能鎖 #教學

設定 #藍牙開鎖 及使用 #app分享權限 聽起來很困難？
沒關係，我們準備了詳細的手把手教學影片！
兩分鐘內馬上學會藍牙及app操作 😊

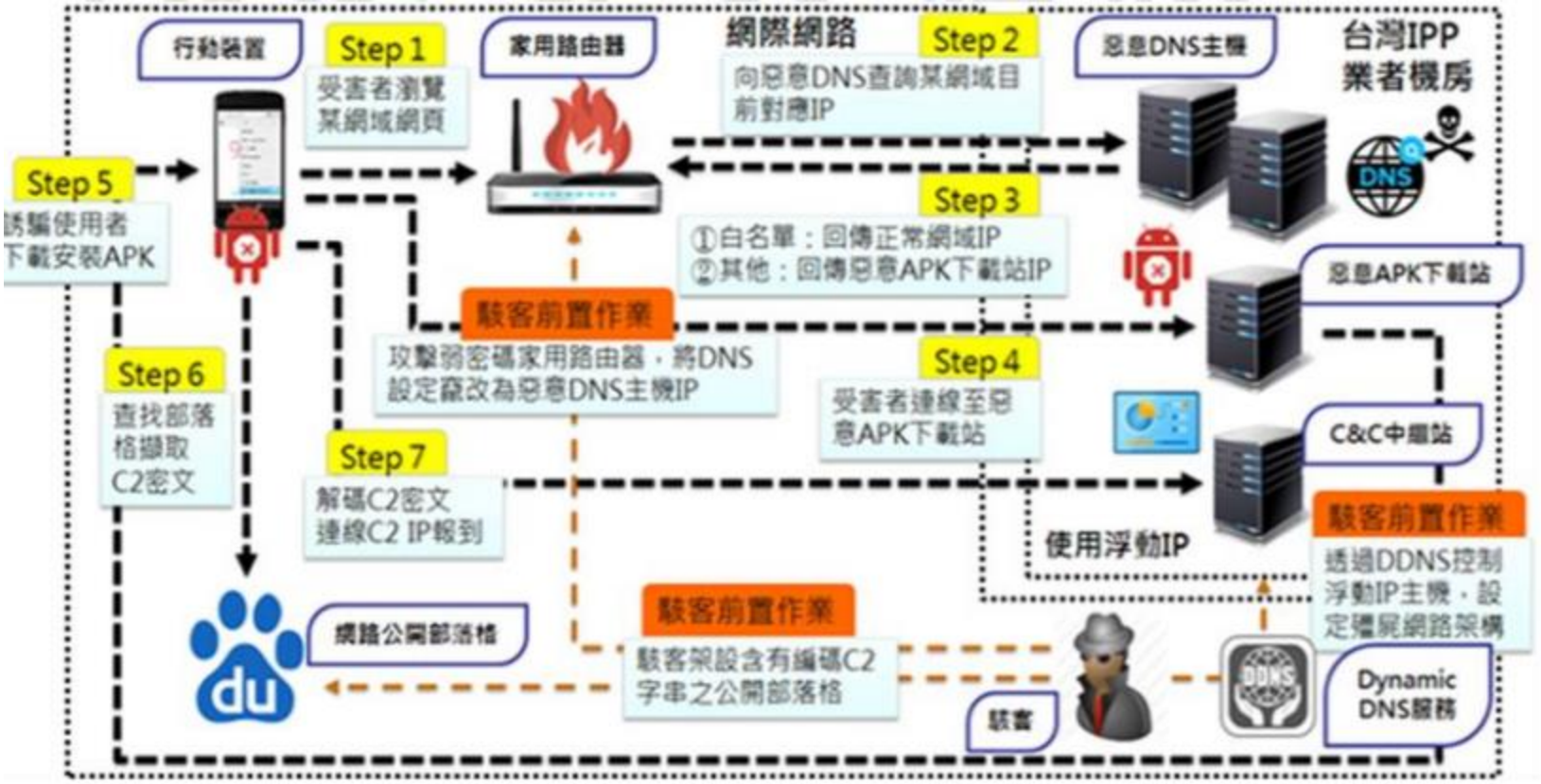
哪些型號可以使用這些便利功能呢：
👉旗艦款：9200
👉最新款：Alpha

飛利浦全自動IOT智能鎖

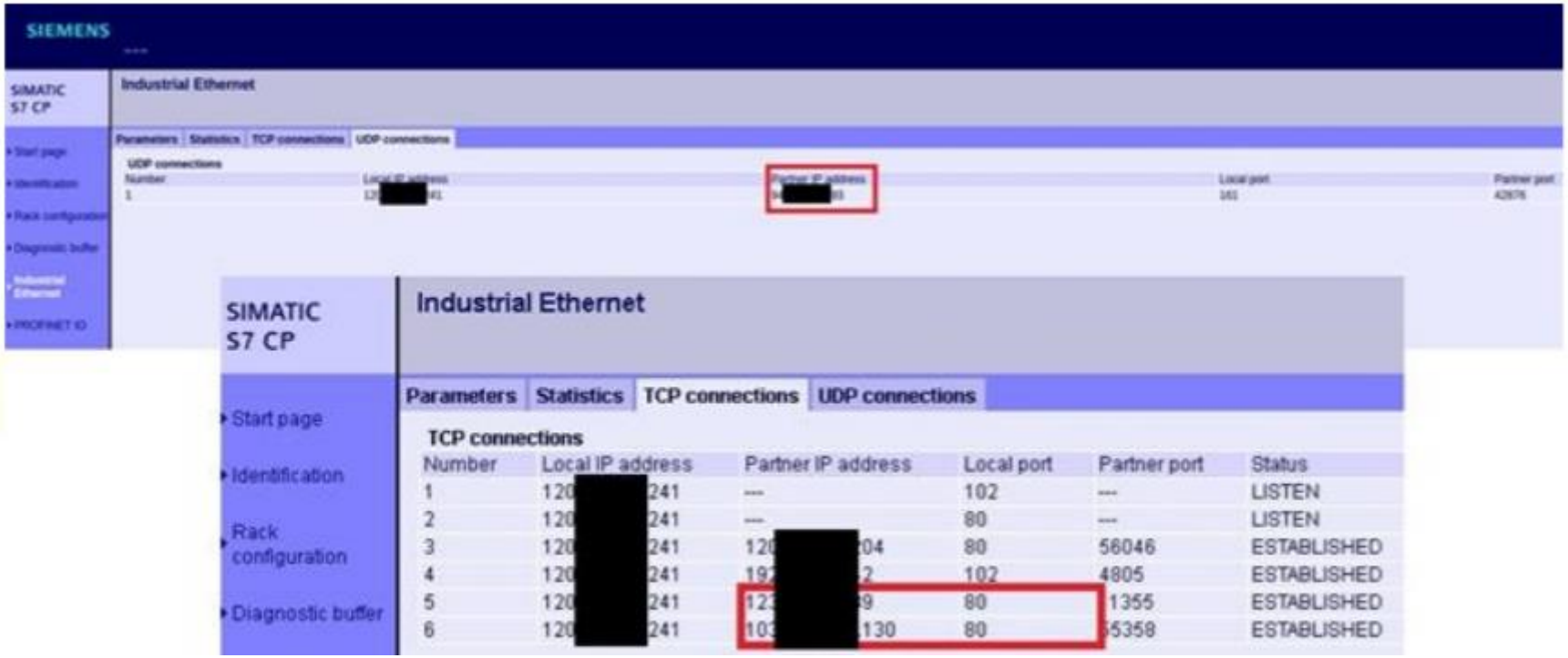
EASYKEY 9300

連接網路，管理門鎖不受限；IOT全新技術，定格全智能

了解更多


行動裝置
Step 1
受害者瀏覽某網域網頁
家用路由器
網際網路
Step 2
向惡意DNS查詢某網域目前對應IP
惡意DNS主機
台灣IPP業者機房
DNS
Step 5
誘騙使用者下載安裝APK
Step 3
①白名單：回傳正常網域IP
②其他：回傳惡意APK下載站IP
駭客前置作業
攻擊弱密碼家用路由器，將DNS設定竄改為惡意DNS主機IP
惡意APK下載站
Step 6
查找部落格擷取C2密文
Step 4
受害者連線至惡意APK下載站
C&C中繼站
Step 7
解碼C2密文
連線C2 IP報到
使用浮動IP
駭客前置作業
透過DDNS控制浮動IP主機，設定殭屍網路架構
網路公開部落格
駭客前置作業
駭客架設含有編碼C2字串之公開部落格
駭客
DDNS
Dynamic DNS服務

假冒 Facebook 更新檔中文視窗畫面



環境控制系統 IP 連線紀錄

無線網路防護措施

家用與企業無線Wi-Fi的管理方式與建議，改善無線網路安全的事項。

1.需妥善設定SSID:變更過SSID與密碼不要使用原廠預設資訊

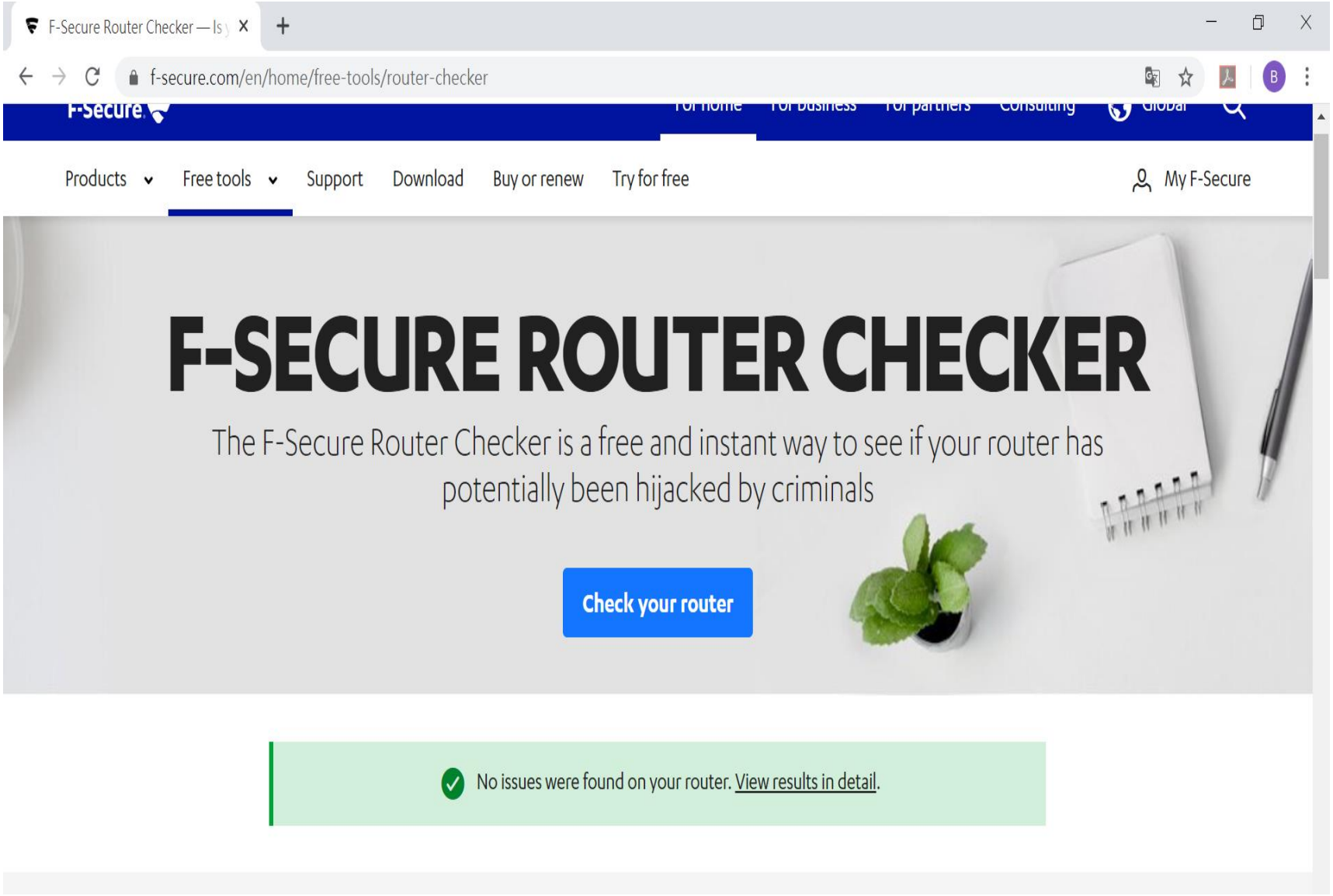
2.請將無線網路設定為WPA2加密

3.切記Wi-Fi密碼設定不可過於簡單

4.管理介面的密碼修改也很重要

5.注意韌體更新，減少設備漏洞威脅

6.藉助其他工具或服務(https://campaigns.f-secure.com/router-checker/en_global/)


F-Secure Router Checker — Is
f-secure.com/en/home/free-tools/router-checker
F-Secure
For home
For business
For partners
Consulting
Global
Products
Free tools
Support
Download
Buy or renew
Try for free
My F-Secure
F-SECURE ROUTER CHECKER
The F-Secure Router Checker is a free and instant way to see if your router has potentially been hijacked by criminals
Check your router
No issues were found on your router. View results in detail.

快確認品項！風險極高 Wi-Fi 分享器爆資安漏洞

資安業者「Tenable」揭露的報告，由於韌體出現漏洞，有跨 20 個品牌、共 37 款 Wi-Fi 分享器可能有資安風險，且相關漏洞的 CVSS 風險評級還達到 9.8 分（滿分 10 分），已達不可忽視的程度。

廠牌	路由器機種
ADB	ADSL wireless IAD router
Arcadyan	ARV7519
Arcadyan	VRV9517
Arcadyan	VGV7519
Arcadyan	VRV9518
ASMAX	BBR-4MG / SMC7908 ADSL
ASUS	DSL-AC88U (Arc VRV9517)
ASUS	DSL-AC87VG (Arc VRV9510)
ASUS	DSL-AC3100
ASUS	DSL-AC68VG
Beeline	Smart Box Flash
British Telecom	WE410443-SA
Buffalo	WSR-2533DHPL2
Buffalo	WSR-2533DHP3
Buffalo	BBR-4HG
Buffalo	BBR-4MG
Buffalo	WSR-3200AX4S
Buffalo	WSR-1166DHP2
Buffalo	WXR-5700AX7S
Deutsche Telekom	Speedport Smart 3
HughesNet	HT2000W
KPN	ExperiaBox V10A (Arcadyan VRV9517)
KPN	VGV7519
O2	HomeBox 6441
Orange	LiveBox Fibra (PRV3399)
Skinny	Smart Modem (Arcadyan VRV9517)
SparkNZ	Smart Modem (Arcadyan VRV9517)

中國政府自己都點名「不安全」！這 11 款軟體別再用了

中國江蘇省消費者權益保護委員會稍早公布了一名「PC軟體」調查報告，並認定有 11 款在資安上有風險。被點名不安全的軟體亦不乏知名選擇，包括騰訊視頻、QQ、迅雷都在列。其他被點名的，還有 360 安全瀏覽器、360 安全衛士、暴風影音、小鳥壁紙、酷我音樂、愛剪輯、ACDsee、2345看圖王，總有 11 款。近年累積不少資安和強迫安裝爭議的 360 產品，本次亦有兩款軟體「入選」。

可以防堵的惡意行為

檢視你的手機是否有App可以執行這八種動作的程式：

1.在Android通知欄中顯示廣告。
2.修改瀏覽器預設的首頁或書籤。
3.在手機桌面上新增icon圖示。
4.可以存取手機電話、簡訊、相機功能。
5.收集個人資訊。
6.收集位置資訊。
7.收集裝置或是行動網路資訊。
8.用廣告取代播放鈴聲。

不給多餘的權限，危險不上身

您的位置：程式會透過手機GPS或是LBS基地台的方式來取得你的位置。一般來說，只有與地圖相關的應用才會用到這個權限。

需要額外費用：這個權限可以讓應用程式直接用手機撥打電話、簡訊給特定對象。理論上很少有遊戲會用到這個權限。

您的帳戶：應用程式會存取這台手機上的Google帳戶、密碼。一般來說，除了Google本身的App之外，其他程式應該不會用到。

您的個人資訊：很多應用程式都會要求這個權限，這個權限的要求可大可小，透過這個授權可以讀取手機中的聯絡人資料。

系統工具：這個授權可以讓應用程式設定為在開機的時候，自動將程式載入到背景。如果是應用程式要求這個授權還算合理，如果是遊戲的話則很奇怪。

免費手機防毒軟體


CM Security - 免
KS Mobile Inc. 免費
免費 防毒防盜安
Lookout Mobil 免費
avast! 手機安全
AVAST Softwa 免費
免費杀毒 - AVG
AVG Mobile 免費
Dr.Web v.7 Anti-
Doctor Web, Lt 免費
台灣360手機衛士
Hope Joy 免費
安全達人(趨勢科
Trend Micro 免費
行動安全防護與
Trend Micro 免費
McAfee Antivirus
McAfee Mobile 免費
Avira Antivirus S
AVIRA 免費
Clean Master (
KS Mobile 免費
Trustlook安全衛
Trustlook Hea 免費
行動防毒 Antivir
NQ Mobile Sec 免費
視頻防毒審查
PashaYakushe 免費
遠傳防毒工具
AegisLab 免費
諾頓行動安全軟
NortonMobile 免費
G-Protector 防毒
Gpc 免費
Dr.Web v.9 Anti-
Doctor Web, Lt 免費
LINE Antivirus
LINE Corporati 免費
行動安全防護-全
Trend Micro 免費
Kaspersky Intern
Kaspersky Lab 免費
Heartbleed 全面
KS Mobile Inc. 免費
防毒面具
mstore365 免費
Antivirus & Mobi
TrustGo Inc. 免費


遠傳電信 3G 下午3:53
附近地標
取消
搜尋或新增地標
“Facebook”要使用您的目前位置
不允許
好
定位中.....

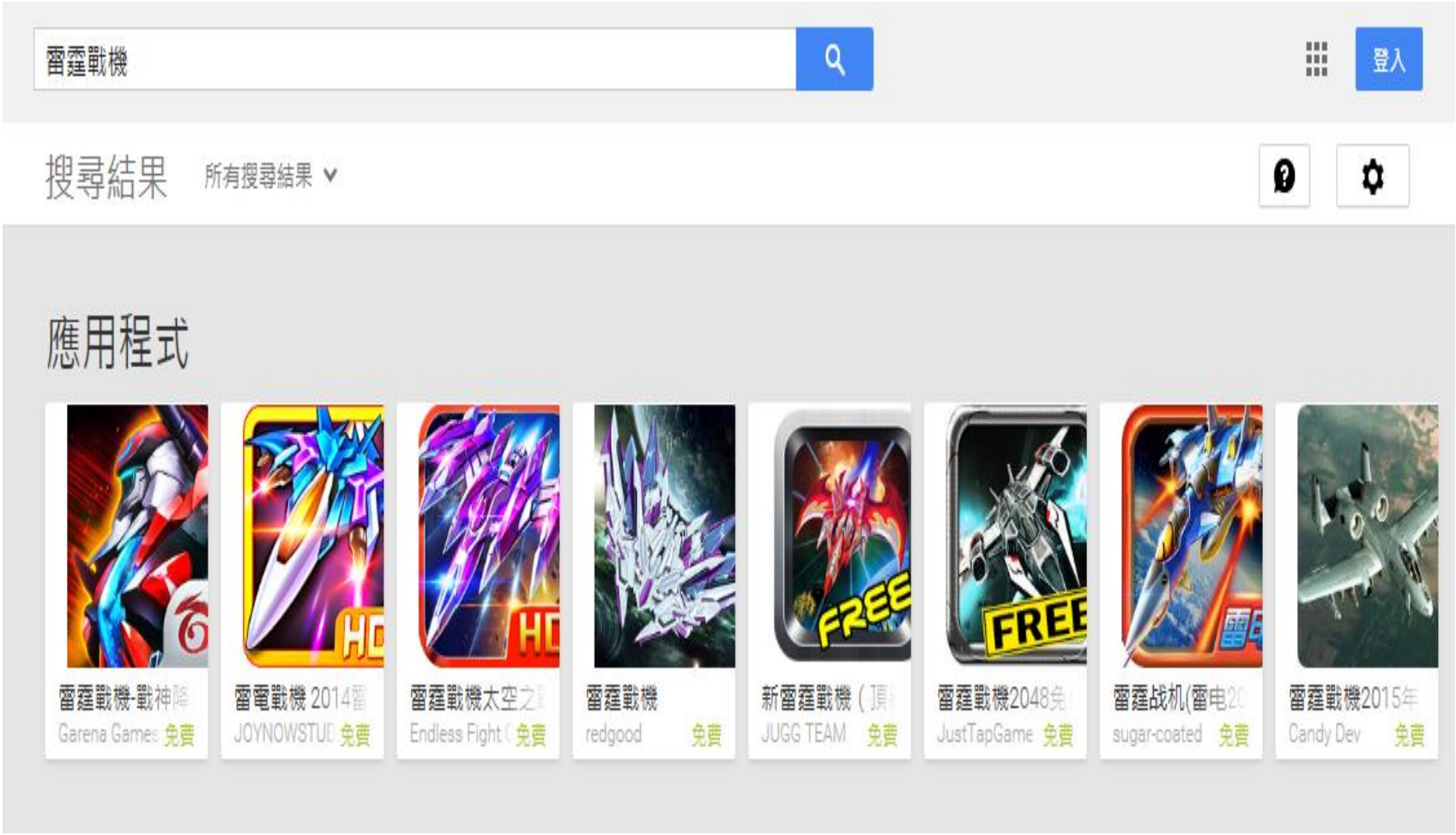

17:03
Checkins
Map
淡水區
基隆市
新莊區
新店區
新北市
烏來區
員山鄉
宜蘭
My dates
Friends
地標
張香腸
打卡
朋友
20:40
20:38
19:53
19:35
19:21

請小心假的手機病毒警告訊息，千萬不要隨便安裝來路不明的 APP!

點選 OK 後，跳轉到了「**你的手機已經中毒**」的頁面，聲稱你的個人相片及密碼已經有風險，要你「**立刻移除病毒**」


81% 10:35
www.ye[redacted]
警告:檢測到Android木馬攻擊
檢測到兩次來自遠程主機的未經授權訪問，發生兩次木馬攻擊。
掃描報告詳情
1.檢測到未經授權的訪問，來自阿爾巴尼亞的IP地址(212.156.312.23)。
2. 木馬程序隱藏在“trojan.droid3x”的垃圾文件。
警告:病毒會破壞你的SIM卡,刪除聯繫人信息，盜取你的密碼和電子郵件。
如果你想消除這一威脅，請點擊“立即清理”。
立即清理

官方版本&非官方版本

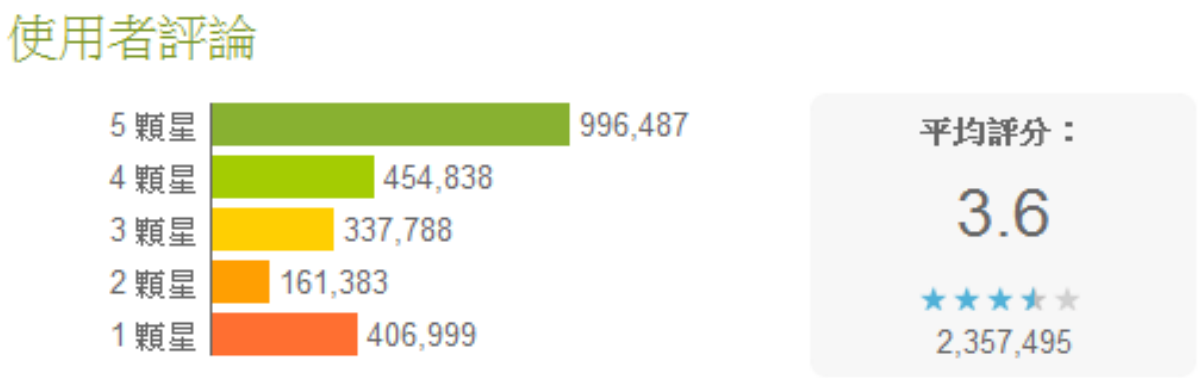

雷霆戰機
登入
搜尋結果
所有搜尋結果
應用程式
雷霆戰機-戰神降
Garena Games 免費
雷電戰機 2014雷
JOYNOWSTUD 免費
雷霆戰機太空之
Endless Fight (免費
雷霆戰機
redgood 免費
新雷霆戰機 (頂
JUGG TEAM 免費
雷霆戰機2048免
JustTapGame 免費
雷霆战机(雷电20
sugar-coated 免費
雷霆戰機2015年
Candy Dev 免費

如何判定Android App是否為惡意軟體

下載前:

1.使用者評價

誰說都不公平，使用者說最公平，看評價，是4星或5星就可以下載?不，等一下，請確定評價人數至少要500到1000人，因為10人可能是灌水



如何判定Android App是否為惡意軟體

如何判定Android App是否為惡意軟體

看完軟體，來看看開發員，建議只下載頂尖開發員的軟體，因為大部分知名品牌都有頂尖開發員資格，所以這樣可以避免被騙

如何判定Android App是否為惡意軟體

下載後:

1.手機耗電量

當駭客到你的手機抓檔案，耗電量當然會增加，所以隨時注意耗電量是否異常

2.背景運作軟體

駭客不可能在你用軟體時才來抓檔案，一定是讓軟體背景運作，隨時都可以抓，所以可以到設定→應用程式→正在運作的服務，確定裡面沒有沒看過的程式在跑，如果有，請強制停止(通常叫作MonitorService)

移動式個人裝置應用與安全

安裝了最新的手機惡意程式嗎!!

最新危險Android應用：


超级玛丽经典怀旧


Pocket Basketball

美食Walker


Jewels Dash

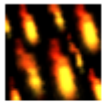
老黃曆通勝


Moon+ Reader Pro


Camera360


Pocket Basketball


Uninstall Master


Fire Rain


TheEpiphanyV3


Ice Galaxy


卡牌交換牧场


皇帝


Lightning Storm

aTorrent Pro


家人定位


Strata


SoundHound ∞

Real Racing 3


WIFI破解


伪装地理位置


Sys Config

十大手機病毒

這部份就僅供參考，但如果你是常去大陸亂下載 APK 安裝的朋友可能就要檢查一下你自己的手機了。

TOP 1：Msm
危害級別：★★
病毒特性：該病毒安裝後，會監聽使用者簡訊接收，並上傳到雲端伺服器，造成隱私洩漏。

TOP 2：Android Defender
危害級別：★★★
病毒特性：該病毒安裝後，彈出釣魚訊息，騙取使用者支付費用，造成資費消耗，如果不支付的話會讓你無法使用其它軟體，讓手機安全遭受嚴重的影響。

TOP 3：轟炸彊屍
危害級別：★★★
病毒特性：該病毒安裝後，後台會常駐惡意服務，以通知欄或對話框形式匿名推送推廣訊息，無法取消，而且一點擊就下載，造成使用者大量流量消耗，並存在安全疑慮。

十大手機病毒(續)

TOP 4：100tv 播放器
危害級別：★★★★
病毒特性：該病毒特性同上「轟炸彊屍」。
TOP 5：水果派對
危害級別：★★★★
病毒特性：該軟體會私自發送簡訊定制 SP 服務，並屏蔽回傳的訊息，造成資費增加。
TOP 6：競技摩托
危害級別：★★★★
病毒特性：該病毒安裝後，會強制執行，從遠端伺服器自動下載惡意腳本代碼，私自下未知的軟體，消耗使用者流量，造成資費增加。。
TOP 7：KM Home
危害級別：★★★★
病毒特性：該病毒經常捆綁在一些主題類的軟體，啟動後就會自動安裝特定目錄下的軟體，每隔一秒向指定目標發送簡訊，並且在背景自動上網，同時這病毒也會攔截以「10」開頭的簡訊及特定類型的信息，會大量增加資費。

十大手機病毒(續)

TOP 8：萬能查詢
危害級別：★★★★
病毒特性：該病毒安裝後，誘導使用者申請 Root 權限，一但獲取 Root 權限則會破壞系統，同時會在背景私自下載並安裝未知軟體，收集使用者 IMEI 等相關訊息，造成嚴重安全問題。

TOP 9：手機也能變魔術
危害級別：★★★★
病毒特性：該病毒啟用後，未經使用者允許自動上網下載推廣安裝包，增加使用流量，造成資費增加。

TOP 10：Google Service
危害級別：★★★★
病毒特性：該病毒安裝後，私自監聽收發簡訊及通話記錄，並隱藏指定簡訊接收，將監控到的訊息上傳到伺服器，造成隱私洩漏。

Google play

太陽能充電

登入

應用程式

搜尋結果 Android 應用程式 所有價格

我的應用程式

購物

遊戲

編輯精選

應用程式

太陽能充電器免費
MHedia.de 免費

太陽能充電器
Ponyrocket.com 免費

太陽能充電器
inventor 免費

太陽能充電器
Joaquim Marii 免費

太陽能充電器
mz50 免費

新的太陽能充電器
DROID PRANK 免費

太陽能電池充電器
SEMSIX 免費

太陽能電池充電器
andrivax 免費

太陽能電池充電器
Mafooly 免費

太陽能電池充電器
capzlock 免費

太陽能電池充電器
A1 Designer Ap 免費

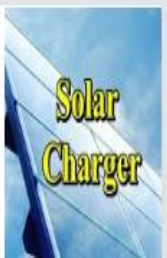
太陽能充電加速器
Folus Wen 免費

Solar Charger
AppGeniusWor 免費

聲音手機充電器
KALUM FERNA 免費

風光互補免費
ThinkChange 免費

cargador bateria
tunegocioapp 免費



蚊子驅趕 - Google Play

https://play.google.com/store/search?q=蚊子驅趕

Google play

電子蚊香

Benny

商店

應用程式

電影

圖書

書報攤

裝置

我的 Play 動態

我的願望清單

兌換

搜尋結果 所有搜尋結果

應用程式

驅蚊王
Viclands Workshop
免費

anti mosquitoes 20
mawika
免費

擊退蚊子
senigo
免費

Anti Mosquito simu
gonsai
NT$30.00

Ultrasonic Sounds
Medasoft
免費

控制蚊蟲
S3ym0ur Birkhoff
免費

防疫app - Google Play Android

play.google.com/store/search?q=防疫app&c=apps&hl=zh-TW

Google Play

防疫app

登入

應用程式

搜尋 Android 應用程式 不限價格

我的應用程式

購物

遊戲

家庭

編輯精選

帳戶

付款方式

我的訂閱內容

兌換

我的願望清單

我的 Play 動態

家長指南

應用程式

台灣口罩庫存查詢

Taiwan Innovation App

全民健保行動快易

衛生福利部中央健康保

台灣口罩地圖(藥局

Mark App Design

口罩地圖[APrevent]

APrevent

即時口罩地圖

Mosil Studio

第一招：不點擊來路不明的鏈結，關閉「從未知的來源」安裝應用程式權限

Android 的安全性設定裡，有一個「**未知的來源**」選項，勾選後**會允許安裝非 Market 線上應用程式商店的軟體**，請記得要把這個選項「取消勾選」，可以降低不小心安裝到 APK 程式所造成的風險。

第二招：中毒請恢復原廠設定，還原最乾淨系統

如果你真的不幸點擊到簡訊、LINE 裡的惡意鏈結，也確定下載、安裝了不乾淨的 APK 檔，那最好的方法不是找到它，或者把它刪除（如果有這麼容易被刪除，那它也不用玩了），而是**把手機「恢復原廠設定」，將所有的資料都刪除掉，重新開始**，以免夜長夢多。

結論

- 網路處處是陷井小心處處有駭客存在網路上，不要輕易相信網路上提供資訊，請勿瀏覽看似好康資料的下載網站。
- 網路平台處處都會留下使用者個人資訊及使用者記錄，凡不必要的資料勿留於網際網路上，千萬不要相信重要資料設有密碼就是安全不會造成資料外洩
- 凡走過必留下足跡，可以透過一些簡檢測電腦輕鬆判斷是否中毒，並可收集系統記錄檔分析追蹤入侵駭客或是惡意使用者，並可以結合搜尋引擎功能找出惡意使用者相關資訊。


THE
END