長庚學校財團法人
長庚科技大學
CHANG GUNG UNIVERSITY OF SCIENCE AND TECHNOLOGY

# 112年度資訊安全教育訓練

漢昕科技 蘇森堯

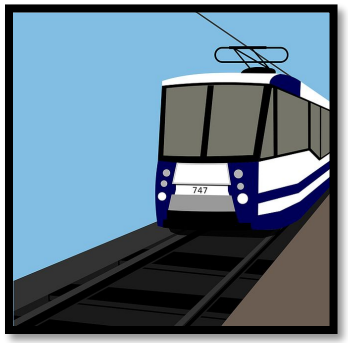
# 課程大綱

- 生活中所隱藏的資安風險
- 行動裝置安全
- 社交工程事件
- 雲端安全
- 熱門AI技術使用應注意事項

# 課程大綱

- 生活中所隱藏的資安風險
- 行動裝置安全
- 社交工程事件
- 雲端安全
- 熱門AI技術使用應注意事項

# 上班途中會隱藏哪些資安風險



1. 社群媒體
2. NFC
3. Air Drop
4. Deepfake

1. 釣魚郵件
2. 惡意網站
3. ChatGPT


1. 公用網路

1. 雲端安全

# 課程大綱

- 生活中所隱藏的資安風險
- 行動裝置安全
- 社交工程事件
- 雲端安全
- 熱門AI技術使用應注意事項

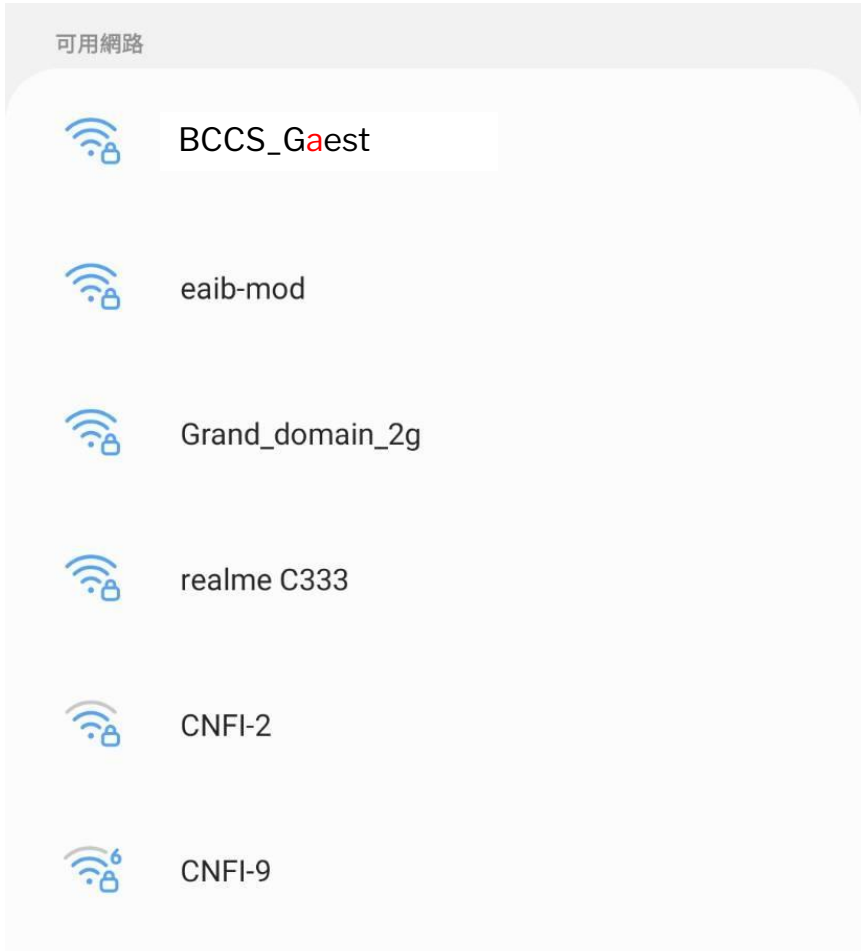
# 行動裝置安全

- 公用wifi
- 下載App
- 社群媒體
- 線上購物
- 網銀轉帳

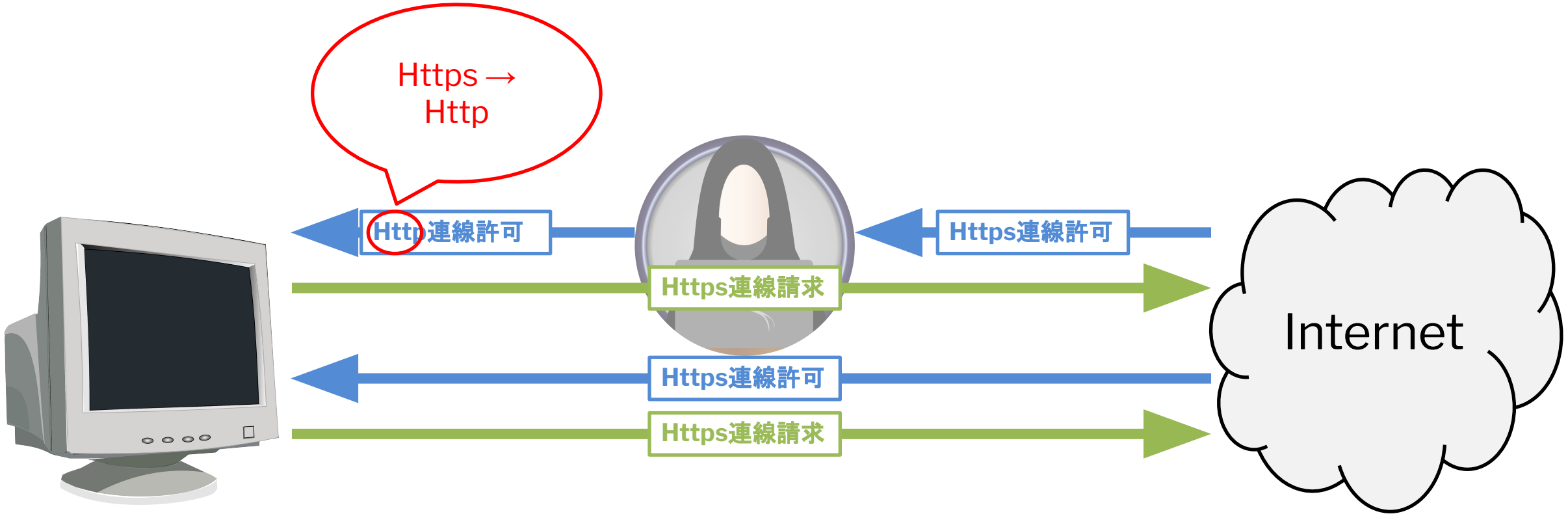
# 行動裝置安全

- 公用wifi
- 下載App
- 社群媒體
- 線上購物
- 網銀轉帳

# 駭客使用之手法


可用網路
BCCS_Gaest
eaib-mod
Grand_domain_2g
realme C333
CNFI-2
CNFI-9

# 當連上駭客的網路時....(一)


Https →
Http
Http連線許可
Https連線許可
Https連線請求
Https連線許可
Https連線請求
Internet

# Http與Https之差別

- Http:
  - 是網頁伺服器與你的電腦瀏覽器，以一般(非安全)模式在進行互動交談，所以內容有可能遭攔截竊聽；換句話說，你在此類網頁上填寫傳送的資料有可能被有心人士看到。

- Https:
  - 多了一個字母S的差別代表"安全(secure)"，基本上意謂著，你的電腦與伺服器間的資料傳遞是以加密的方式進行進行互動交談。

# 當連上駭客的網路時....(二)

# 行動裝置安全

- 公用wifi
- 下載App
- 社群媒體
- 線上購物
- 網銀轉帳

# 兩大平台藏有惡意程式

## 89款惡意APP藏兩大平台！全球恐超過1300萬人受害

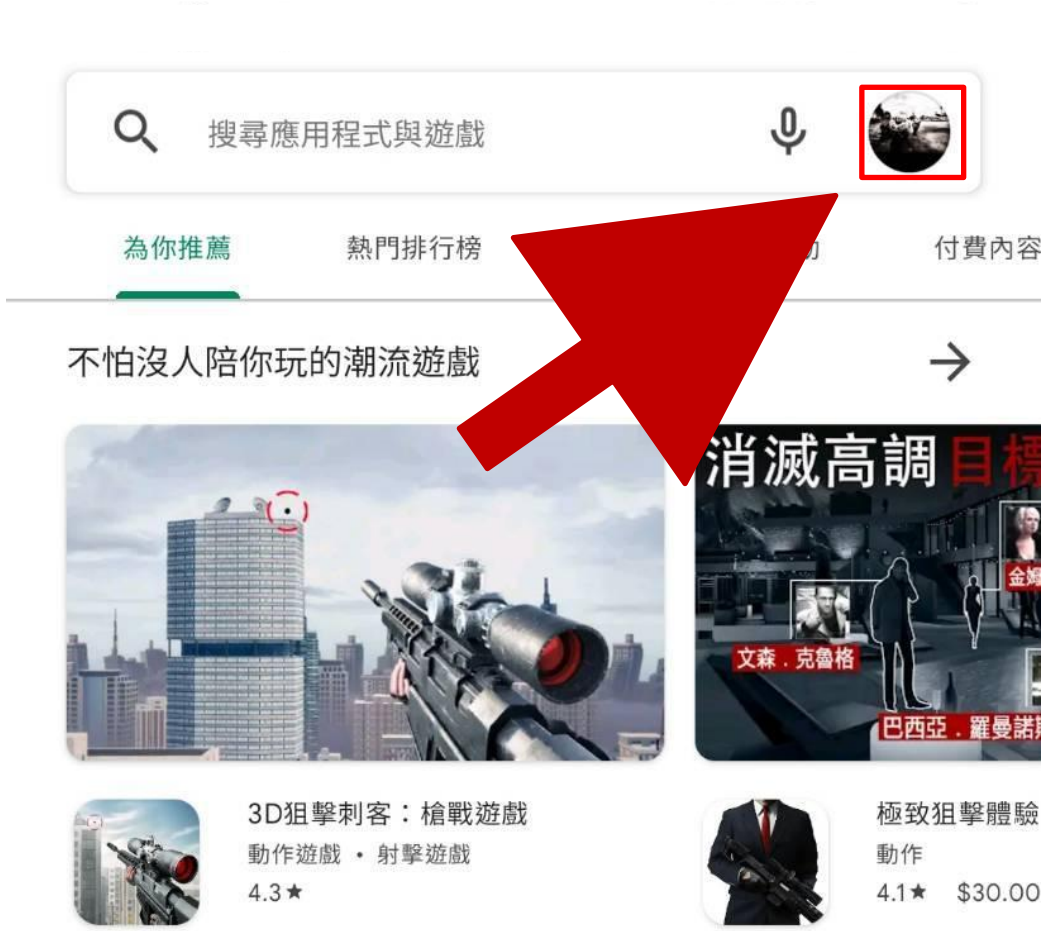
編輯 顏敏翔 報導
發佈時間：2022/09/27 18:11
最後更新時間：2022/09/27 18:11


89款藏有惡意程式的APP藏匿在App Store及Google Play Store中。（示意圖／shutterstock達志影像）

https://news.tvbs.com.tw/tech/1918149

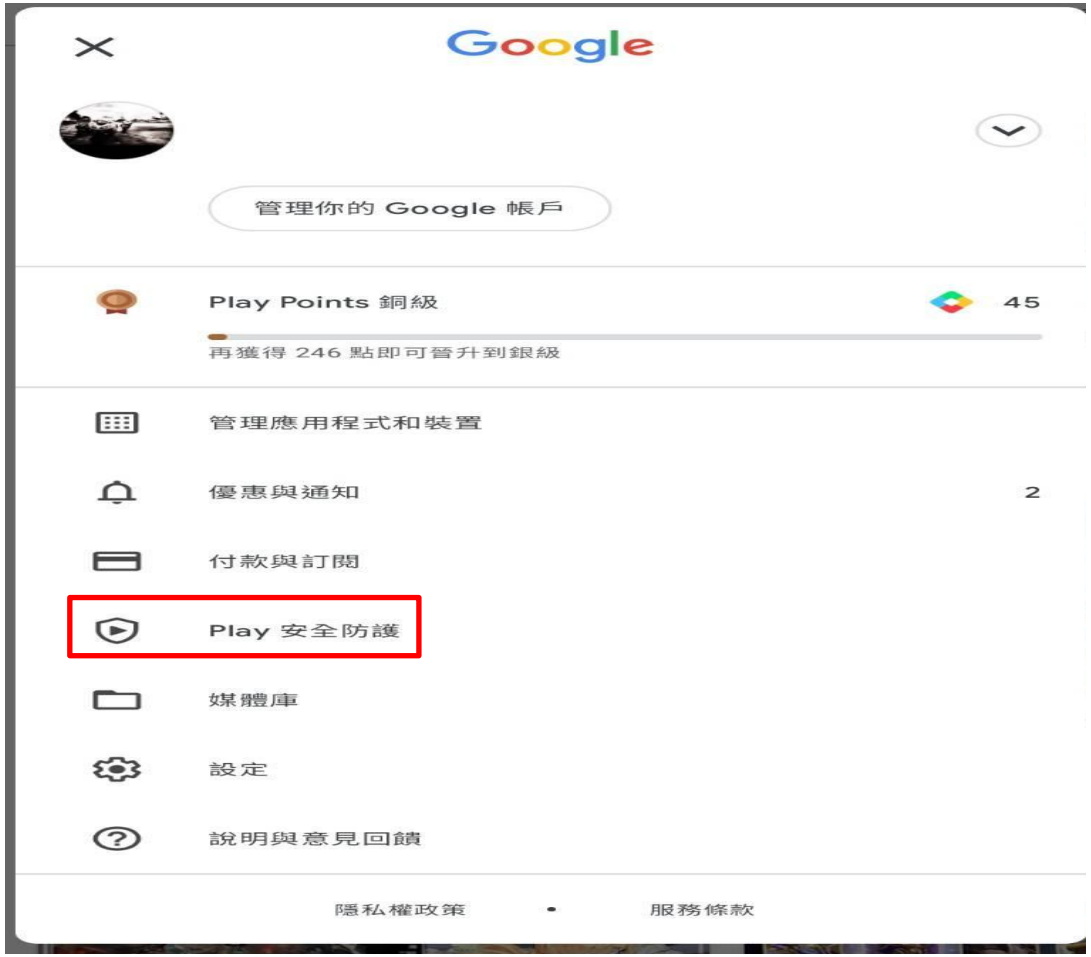
# Google Play 商店安全性設定(1/4)

- 第一步驟:
  點選右上角的
  個人資訊



# Google Play 商店安全性設定(2/4)

- 第二步驟:
  點選紅框內的
  Play安全防護



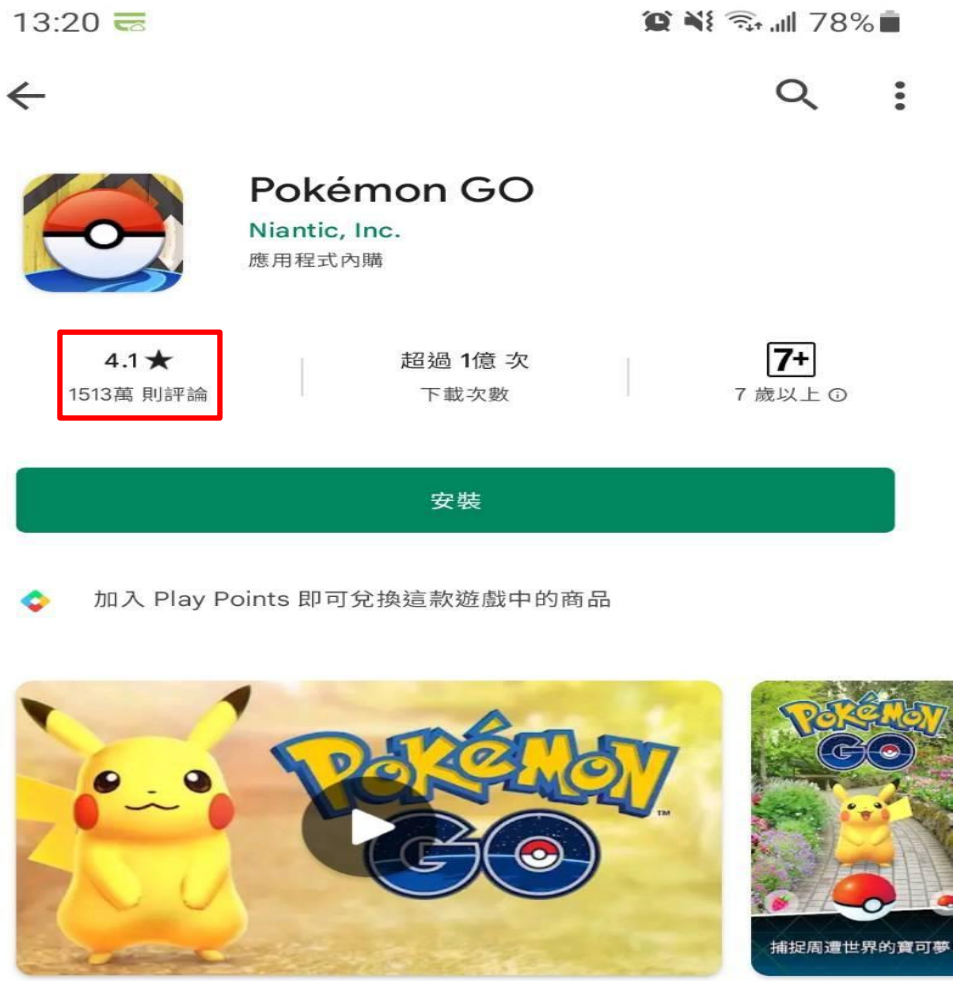
# Google Play 商店安全性設定(3/4)

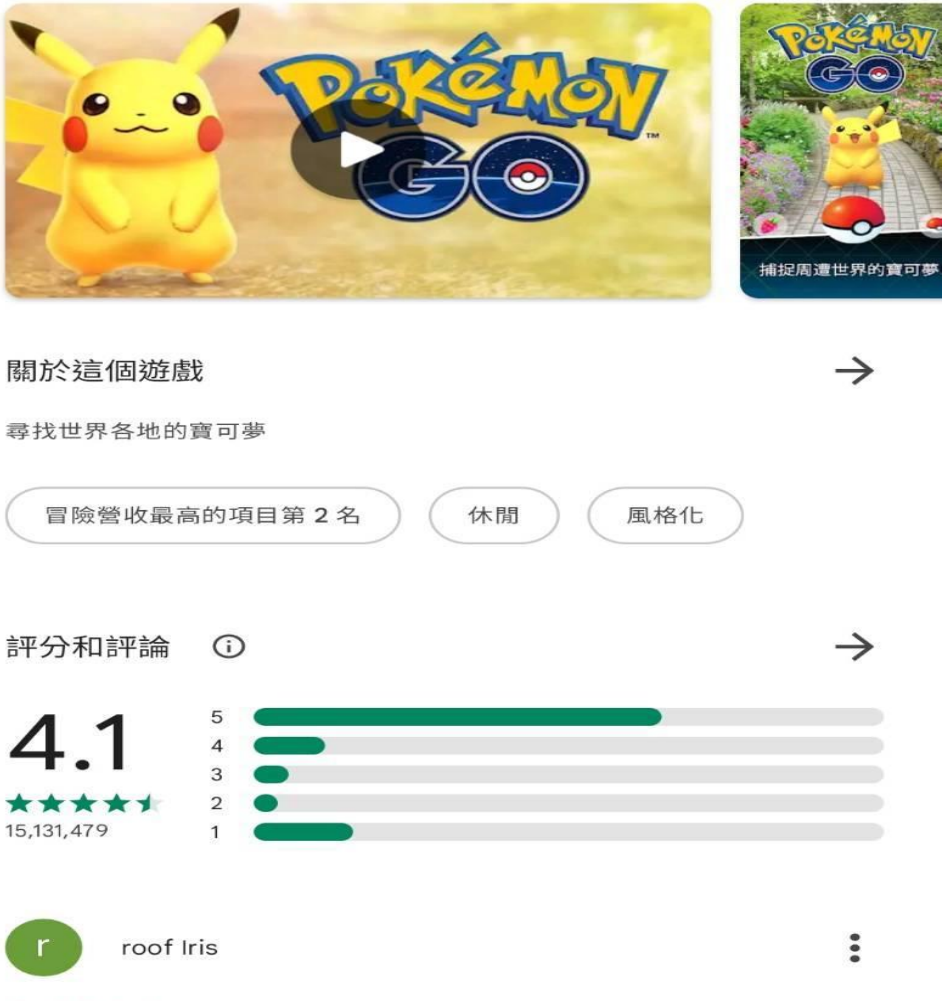
- 第三步驟:
  檢視紅框內的
  掃描時間

# Google Play 商店安全性設定(4/4)

- 第四步驟:
  檢視紅框內的
  功能是否開啟

# 查看App評論


13:20
78%
Pokémon GO
Niantic, Inc.
應用程式內購
4.1 ★
1513萬 則評論
超過 1億 次
下載次數
7+
7 歲以上
安裝
加入 Play Points 即可兌換這款遊戲中的商品
捕捉周遭世界的寶可夢


捕捉周遭世界的寶可夢
關於這個遊戲
尋找世界各地的寶可夢
冒險營收最高的項目第 2 名
休閒
風格化
評分和評論
4.1
15,131,479
5
4
3
2
1
roof Iris

# 查看遊戲開發商與更新日期(1/2)



關於這個遊戲 →

尋找世界各地的寶可夢

冒險營收最高的項目第 2 名 | 休閒 | 風格化

評分和評論 ⓘ →

4.1
★★★★½
15,131,479

5
4
3
2
1

r roof Iris ⋮

13:20 77%

← Pokémon GO
詳細資料

關於這個遊戲

尋找世界各地的寶可夢

現在可以和其他Pokémon GO訓練家在線上對戰了！馬上來試玩GO對戰聯盟吧。

加入世界各地訓練家的行列，一起探索周遭世界並尋找寶可夢吧。Pokémon GO是一款風靡全球的遊戲，下載次數超過10億次，榮獲Game Developers Choice Awards「最佳手機遊戲」獎，並獲選TechCrunch網站「年度最佳應用程式」。

————————————

隨時隨地探索寶可夢的世界！

捕捉更多的寶可夢，填滿寶可夢圖鑑！

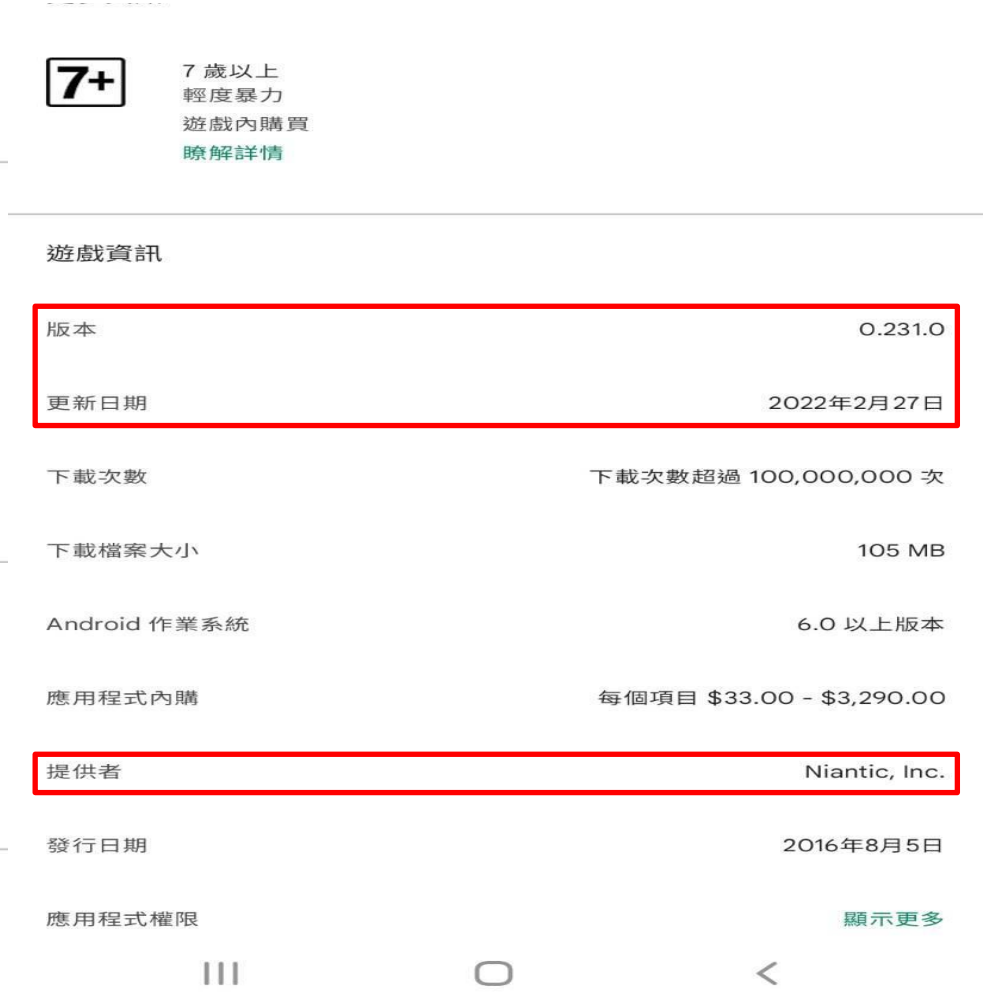
和你的夥伴寶可夢一起踏上冒險之旅，讓你的寶可夢變得更強大並獲得更多獎勵！

在道館對戰中一較高下，或是.....

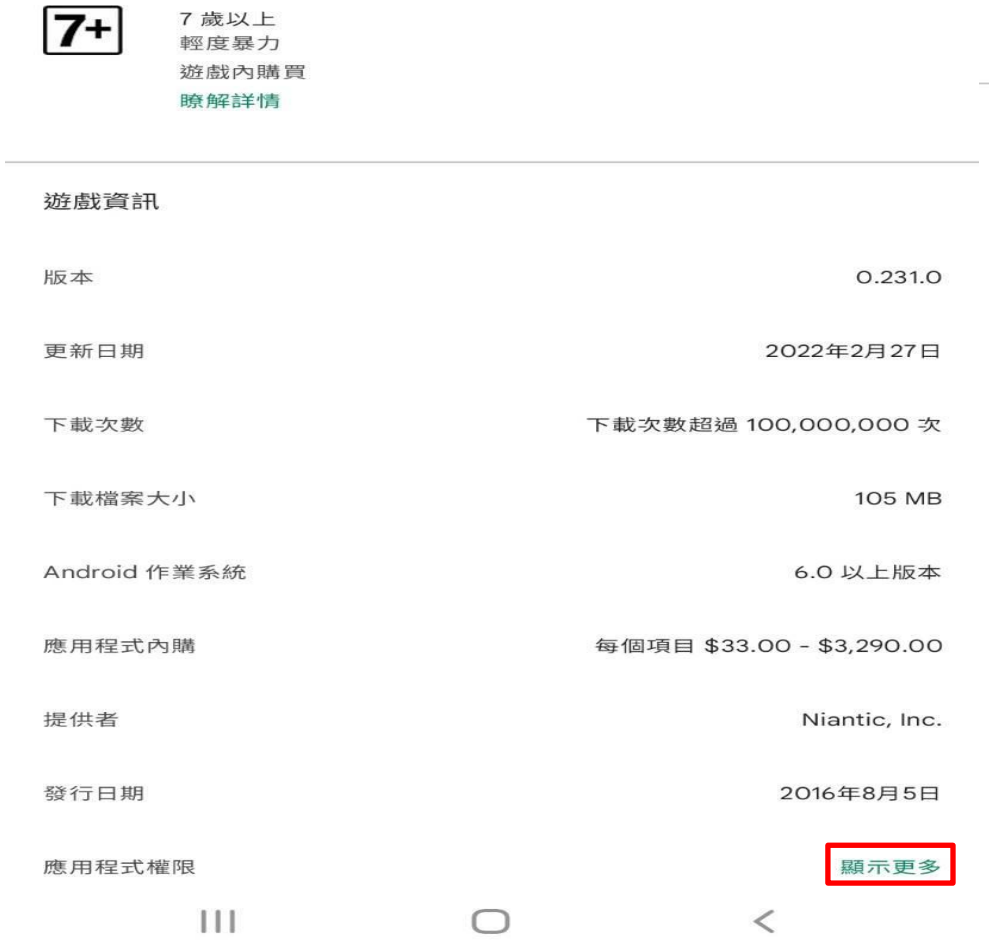
和其他訓練家在團體戰中聯手捕捉強大的寶可夢！

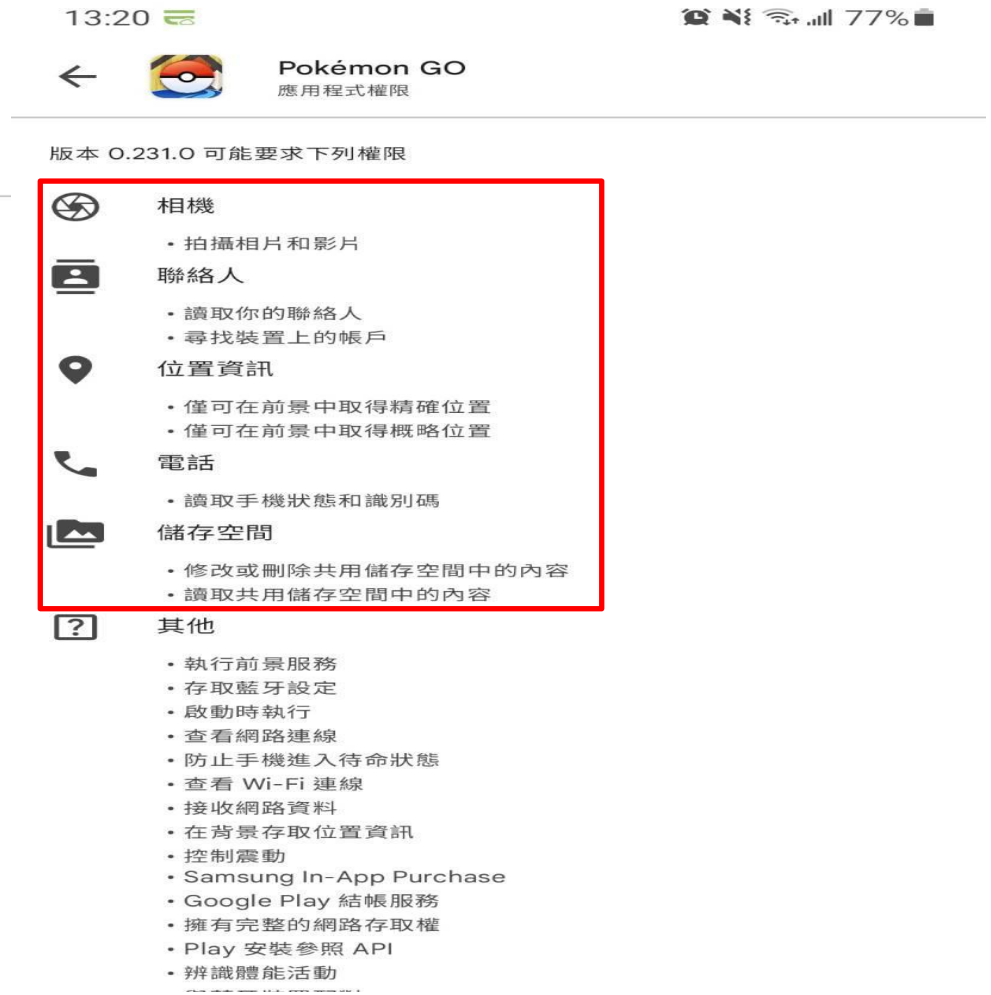
該出發了——現實世界的冒險正等著你踏上旅程！Let's GO！

# 查看遊戲開發商與更新日期(2/2)

# 查看App所需權限


7+
7 歲以上
輕度暴力
遊戲內購買
瞭解詳情
遊戲資訊
版本 0.231.0
更新日期 2022年2月27日
下載次數 下載次數超過 100,000,000 次
下載檔案大小 105 MB
Android 作業系統 6.0 以上版本
應用程式內購 每個項目 $33.00 - $3,290.00
提供者 Niantic, Inc.
發行日期 2016年8月5日
應用程式權限 顯示更多


13:20
77%
Pokémon GO
應用程式權限
版本 0.231.0 可能要求下列權限
相機
• 拍攝相片和影片
聯絡人
• 讀取你的聯絡人
• 尋找裝置上的帳戶
位置資訊
• 僅可在前景中取得精確位置
• 僅可在前景中取得概略位置
電話
• 讀取手機狀態和識別碼
儲存空間
• 修改或刪除共用儲存空間中的內容
• 讀取共用儲存空間中的內容
其他
• 執行前景服務
• 存取藍牙設定
• 啟動時執行
• 查看網路連線
• 防止手機進入待命狀態
• 查看 Wi-Fi 連線
• 接收網路資料
• 在背景存取位置資訊
• 控制震動
• Samsung In-App Purchase
• Google Play 結帳服務
• 擁有完整的網路存取權
• Play 安裝參照 API
• 辨識體能活動

# 行動裝置安全

- 公用wifi
- 下載App
- 社群媒體
- 線上購物
- 網銀轉帳

# Step 1. 謊稱使用者違反著作權

Hello, Dear Instagram User!

As the Instagram team, we have recently reviewed your account on complaints received by us and realized that you have violated our copyrights, we send you a warning message due to the problems this may cause.

Your Instagram account will be permanently deleted from our servers within 24 hours as you violate our copyrights, if you think this is an error, you can appeal, you can send us your account with the appeal form we will give you, otherwise your account will be closed within 24 hours.

**Step1.謊稱違反著作權帳號將被刪除，或宣稱提供驗證標章**

正如我們過去觀察到的一個案例，駭客的訊息會謊稱使用者違反著作權，或宣稱提供驗證標章來引起使用者注意。根據駭客的訊息，如果使用者沒有透過訊息內隨附的連結前往某個網頁輸入自己的帳號資料進行認證的話，使用者的帳號將會遭到刪除。事實上該連結會連上一個模仿 Instagram 官方頁面的網路釣魚網站。

https://blog.trendmicro.com.tw/?p=692

# Step 2. 引領受害者交出帳密

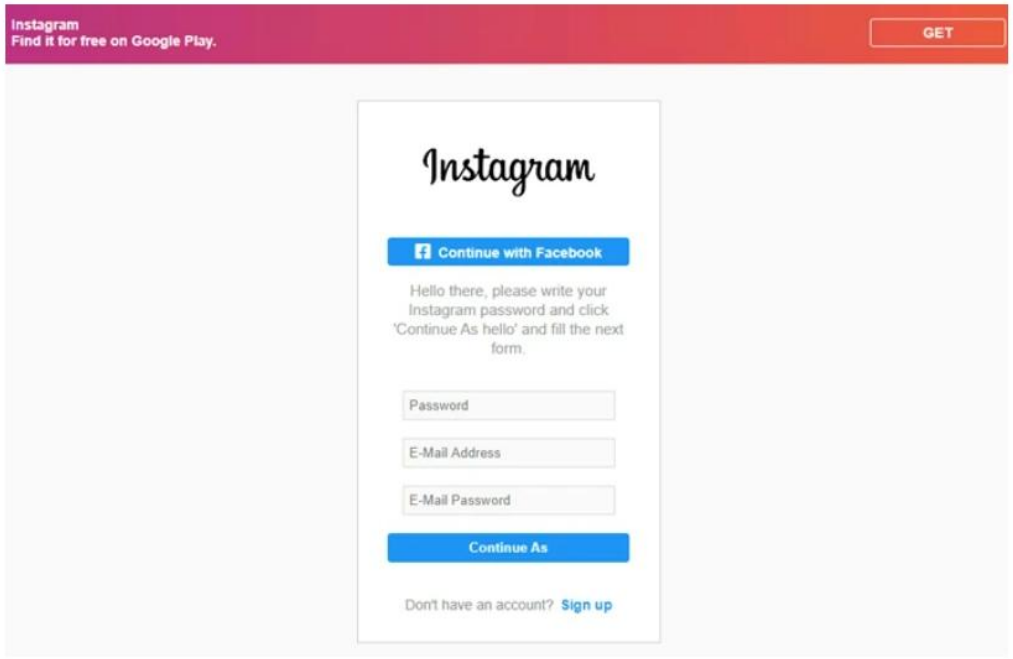
**Step2.釣魚網頁「下一步」按鈕,引領受害人一步步親手交出帳密**

當使用者按下網路釣魚網頁上的「Next」(下一步) 按鈕後，就會被要求輸入其 Instagram 帳號的使用者名稱。值得注意的是，這個網路釣魚網頁並不會確認您輸入的使用者帳號是否為有效的 Instagram 帳號。


https://blog.trendmicro.com.tw/?p=69221

# Step 3. 騙取Email帳密

接下來，使用者會被要求輸入 Instagram 帳號的密碼，以及該帳號連結的電子郵件地址，還有電子郵件的密碼。跟前面一樣，網路釣魚網頁並不會檢查您輸入的密碼是否有效，或是否正確。按一下「Continue with Facebook」(以 Facebook 帳號繼續) 按鈕其實也沒有作用。

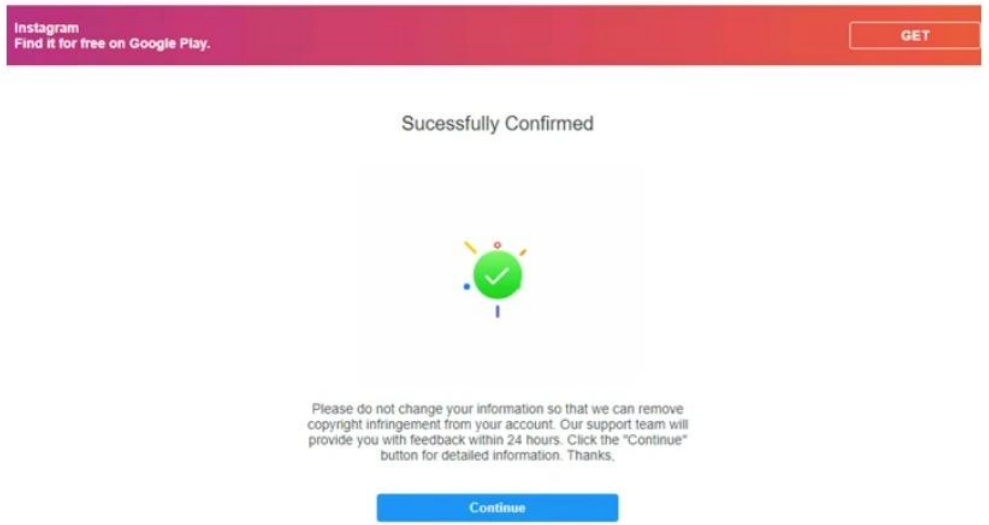



https://blog.trendmicro.com.tw/?p=69221

# Step 4. 提醒受害者不要更改密碼

**Step3.使用假好心拖延戰術, 以便爭取足夠時間登入受害者的帳號**

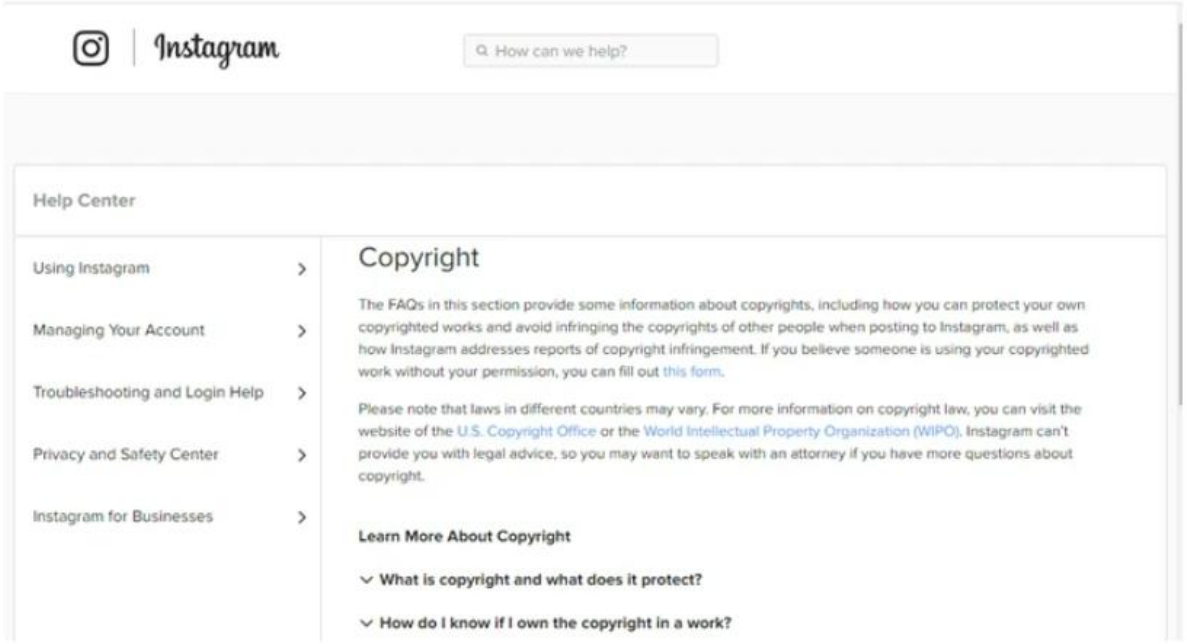
當使用者按下「Continue As」(以此身分繼續) 的按鈕時，接著會出現一個確認頁面。此頁面會請使用者不要再變更帳號資訊，而且還假好心地說，這樣他們才有足夠的時間幫您解決違反著作權的檢舉聲明。但其實駭客是為了爭取足夠的時間，好讓他們用使用者剛剛提供的資料來登入使用者的帳號。




https://blog.trendmicro.com.tw/?p=69221

# Step 5. 最後導向IG官方網站博取信任

當使用者在確認頁面上按下「Continue」(繼續) 按鈕，就會被帶到 Instagram 官方支援網站有關著作權資訊的頁面。駭客這麼做的用意是為了讓其詐騙手法看起來更有說服力。



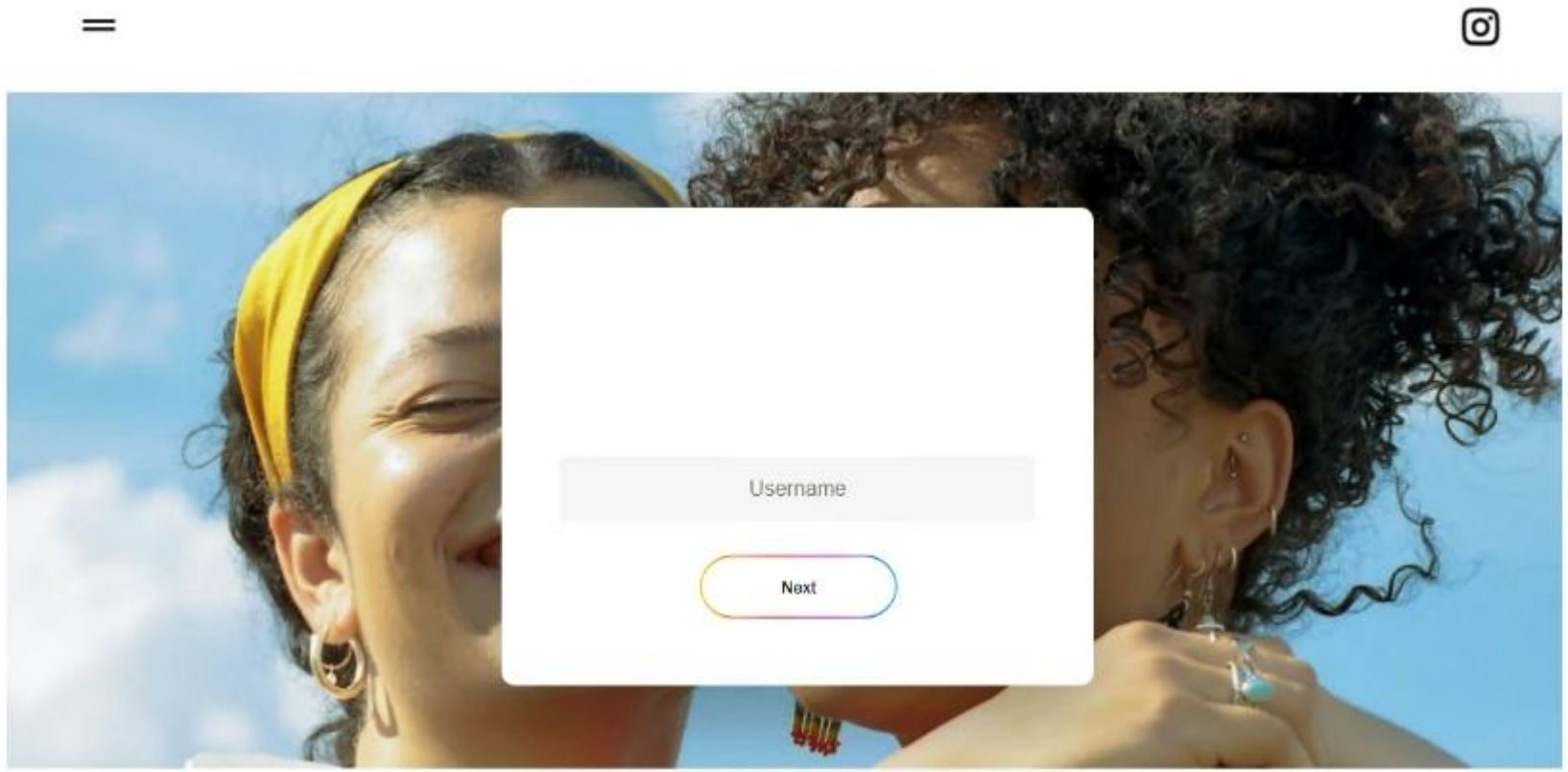

https://blog.trendmicro.com.tw/?p=69221

# Step 1. 以驗證標章當成誘餌

另一個版本的詐騙是駭客以假冒的 Instagram 驗證標章來當成誘餌。Instagram 驗證標章是顯示在帳號名稱旁邊的一個藍色打勾符號，許多網紅、名人、品牌、企業或其他 Instagram 上知名的帳號都有這個標章。此標章代表 Instagram 已驗證過該帳號的真實性。

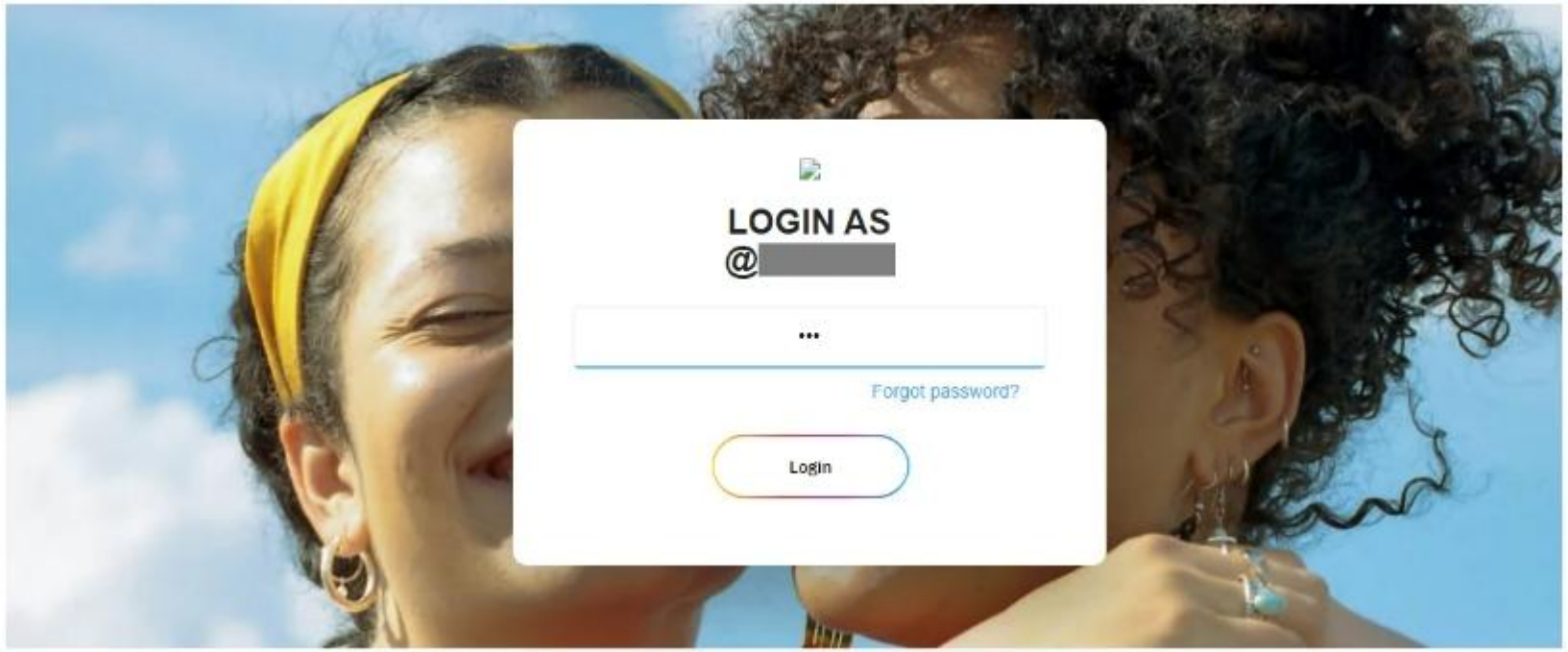

https://blog.trendmicro.com.tw/?p=69221

# Step 2. 導致假網頁輸入帳號



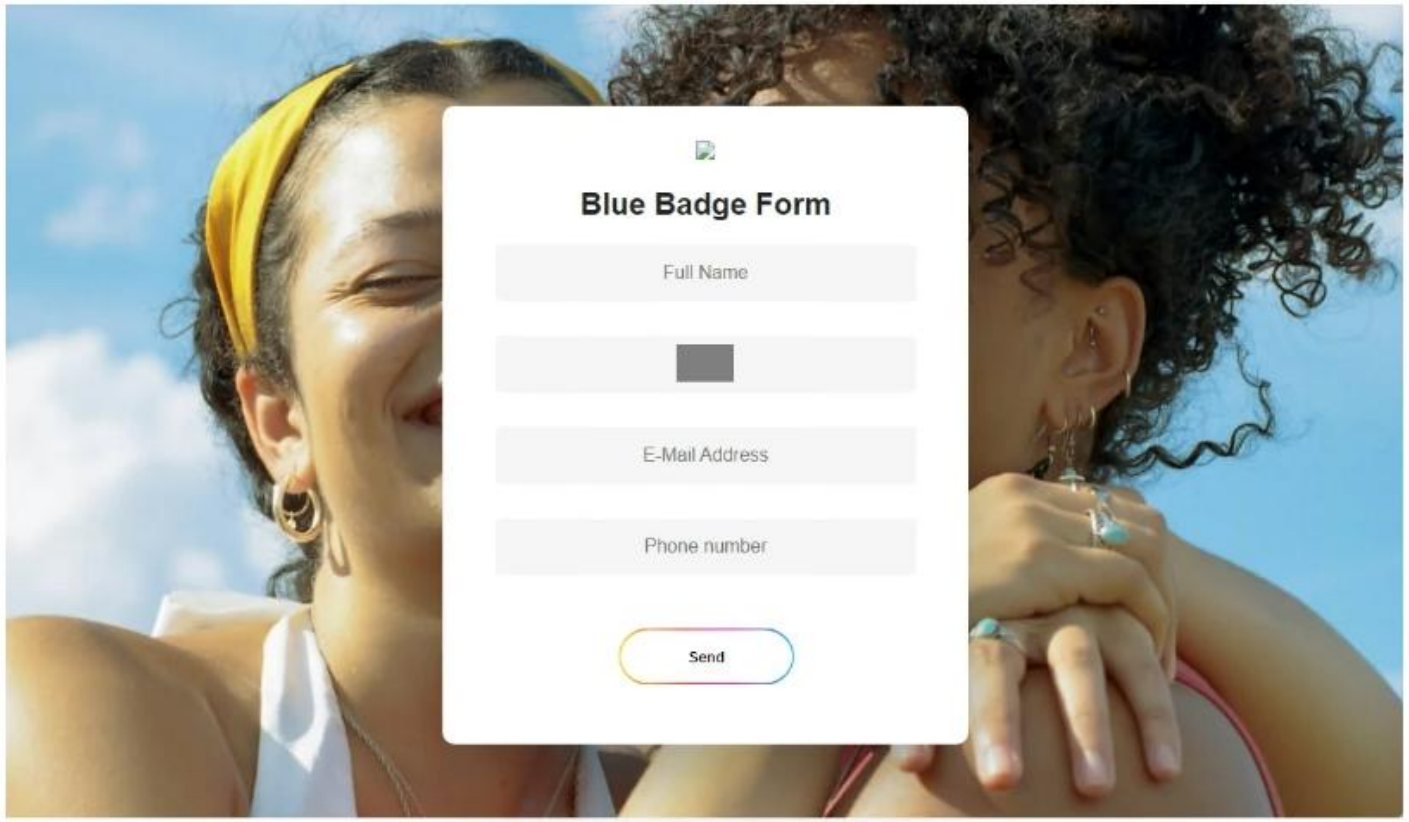

https://blog.trendmicro.com.tw/?p=69221

# Step 3. 導致假網頁輸入密碼



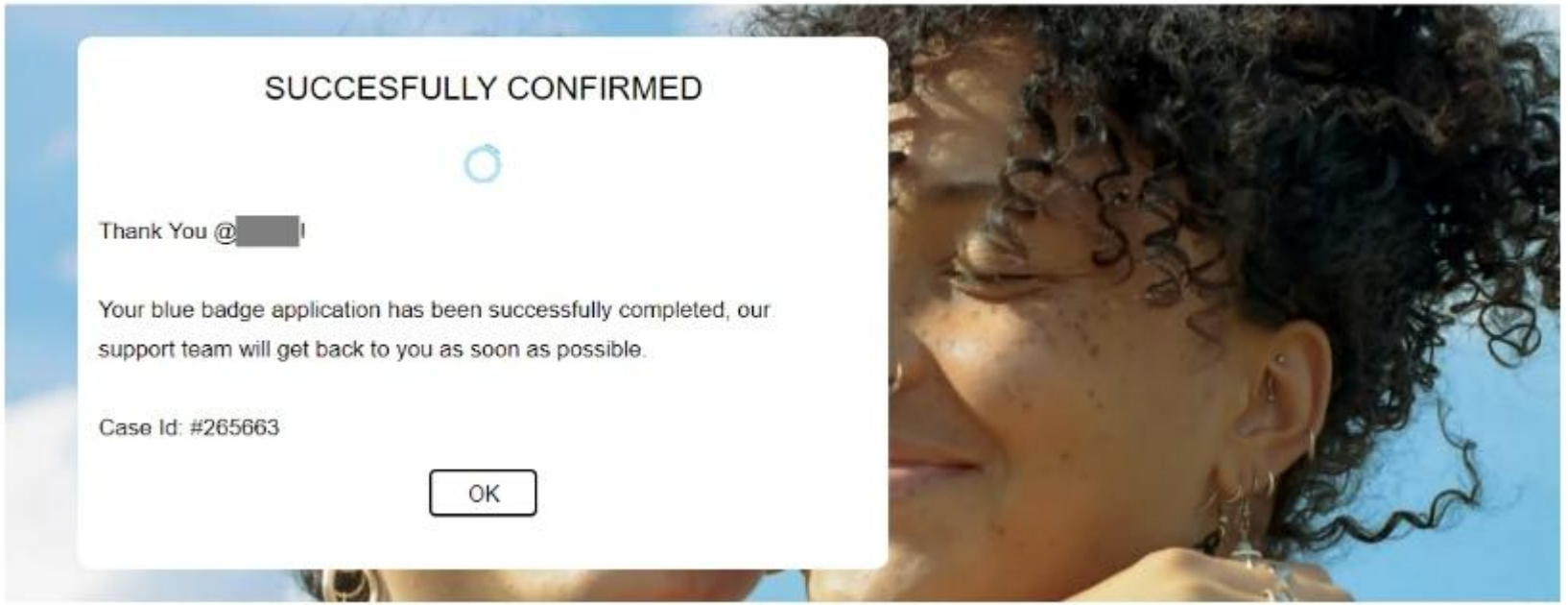

https://blog.trendmicro.com.tw/?p=69221

# Step 4. 輸入Email帳密




https://blog.trendmicro.com.tw/?p=69221

# Step 5. 告知申請已送出




https://blog.trendmicro.com.tw/?p=69221

# 如何確保帳號安全？

## 如何確保帳號安全?

駭客集團的詐騙伎倆從來就沒有用完的一天，所幸，許多平台已經開始導入更多的安全功能來保護使用者的帳號。例如 Instagram 最近推出了一項 Security Checkup (資安檢查) 功能，透過一系列的引導步驟協助使用者保護自己的帳號。這些步驟包括檢查自己的：登入活動、個人檔案資訊、共用登入資訊的帳號以及帳號回復資訊。

除了應用程式與網站開發團隊所做的努力之外，使用者自己也可以透過一些基本的資安原則來保護自己的帳號。

首先，建議使用者最好啟用雙重驗證/兩步驟驗證 (2FA)。啟用之後，駭客就算拿到使用者的密碼也無法登入使用者的帳號。Instagram 及許多其他網站都提供了這項功能設定。

此外，最好不要點選不明來源的郵件或訊息中的連結，因為這很可能是網路釣魚網站的連結。

當帳號遭駭或遭到停用時，可上服務業者或官方網站的支援頁面來查詢該如何處理。

建議使用者採用可偵測電子郵件內容和附件檔案當中暗藏惡意網址 (如網路釣魚網站)的防毒軟體來讓自己多一層保障,如趨勢科技PC-cillin 可保護家庭使用者，防範電子郵件、檔案與網站威脅。

# 行動裝置安全

- 公用wifi
- 下載App
- 社群媒體
- 線上購物
- 網銀轉帳

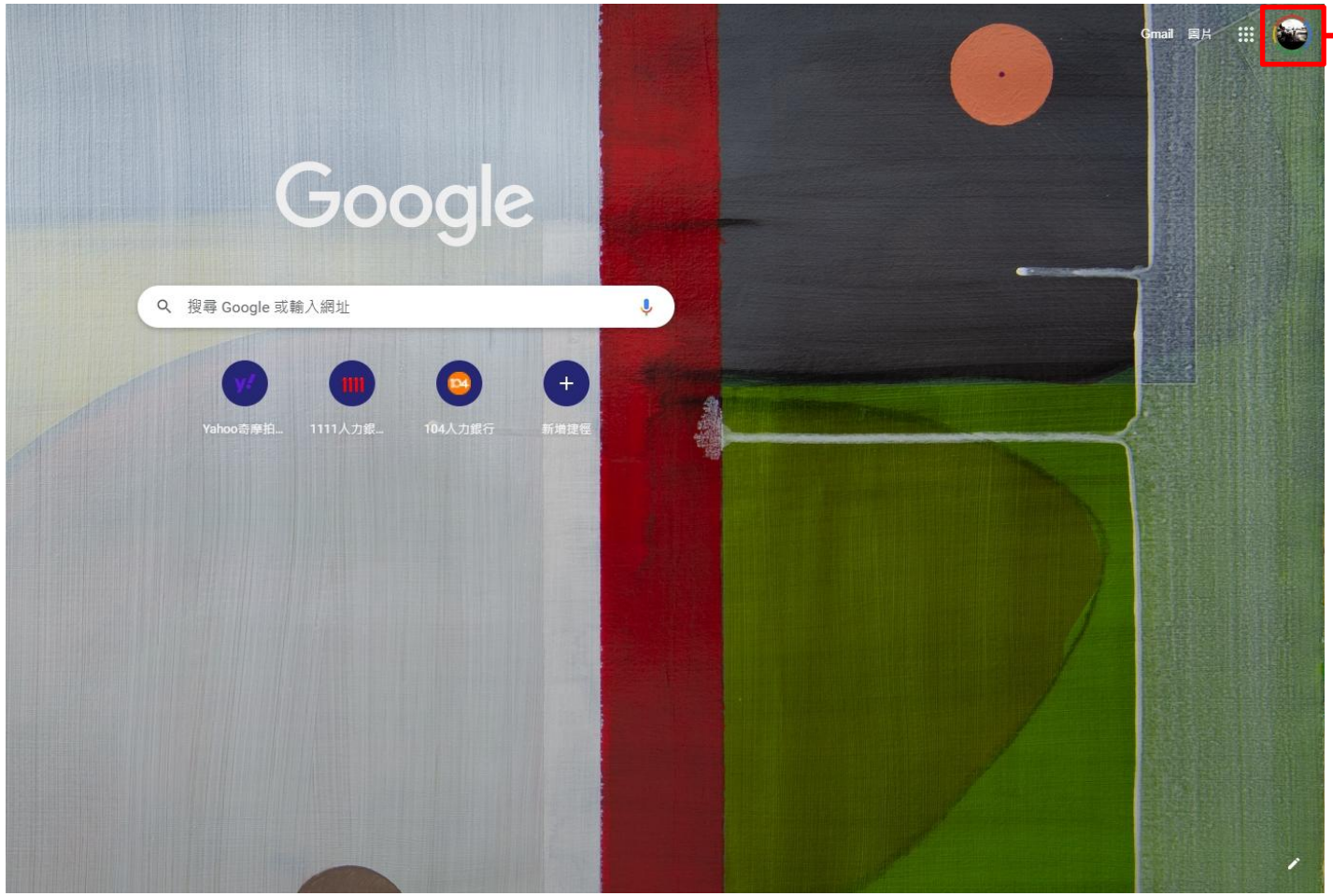
# 所隱藏之資安風險

- 個資外洩
- 信用卡資訊外洩

# 網路購物與網銀轉帳注意事項

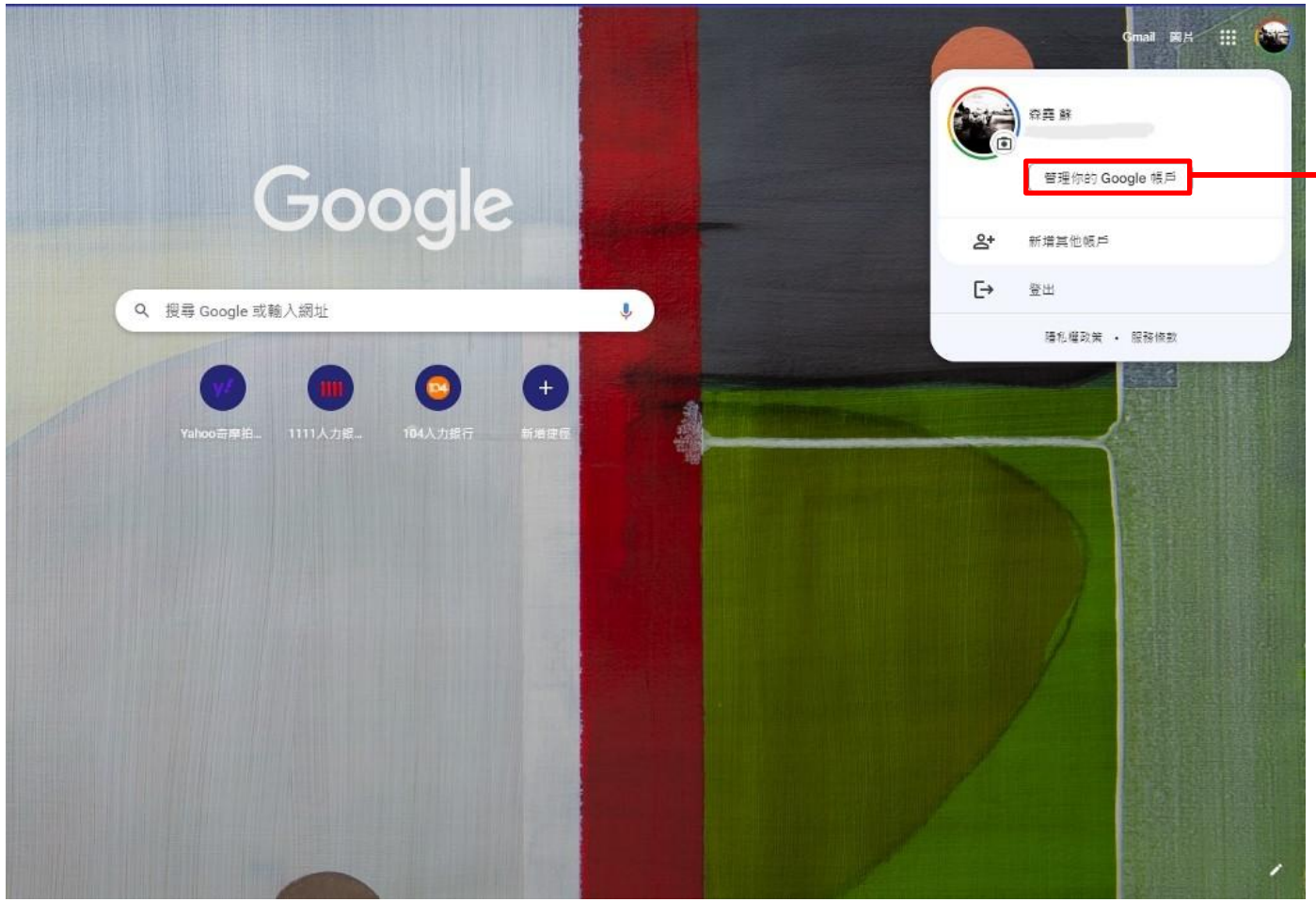
- 網站安全性
  - Http、Https
- 多重驗證機制
- 密碼勿儲存於瀏覽器中
- 密碼勿儲存於行動裝置中
- 信用卡資訊勿儲存於行動裝置中

# Chrome刪除已儲存之密碼(1/8)




點擊右上角的頭像

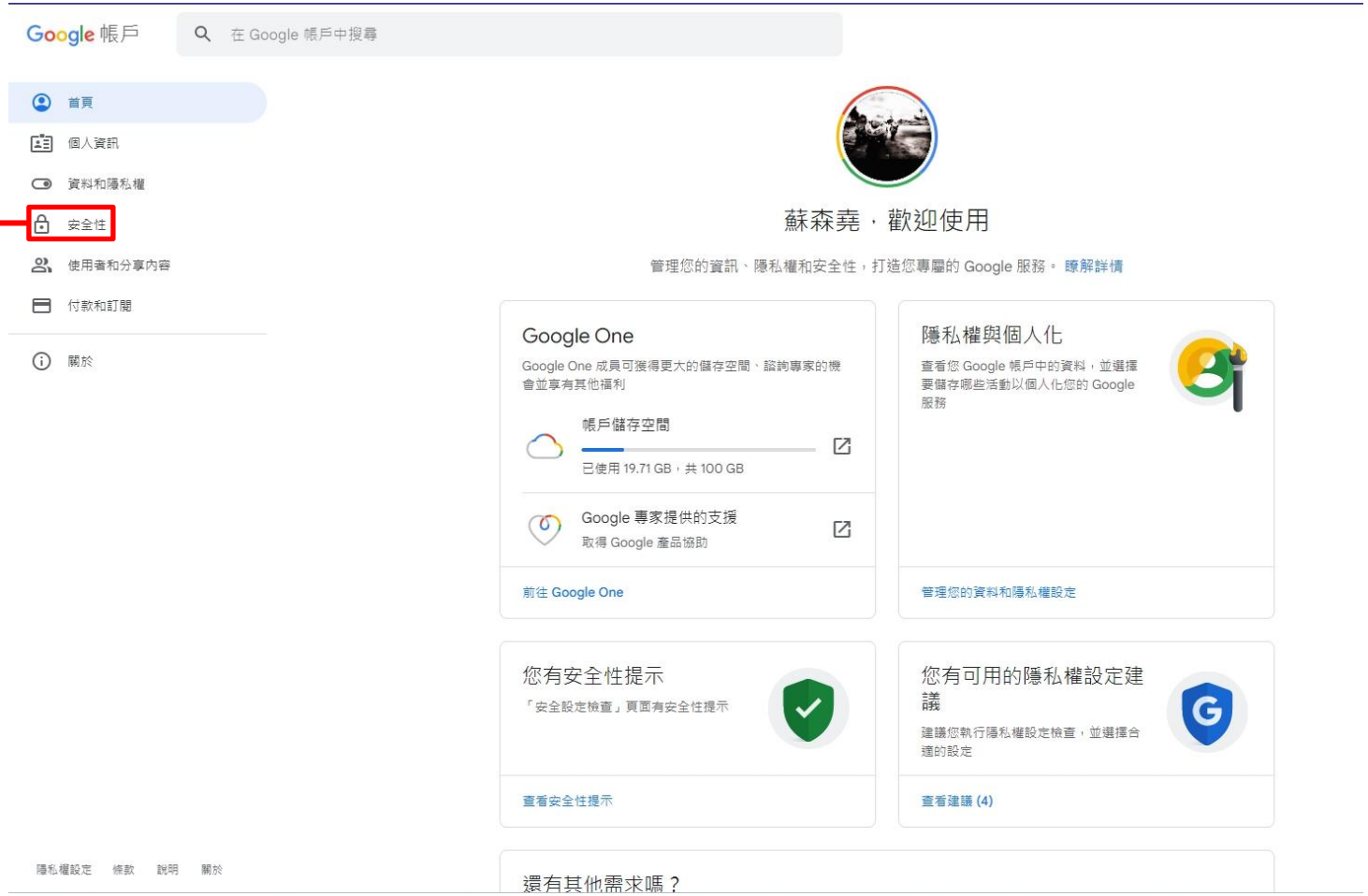
# Chrome刪除已儲存之密碼(2/8)



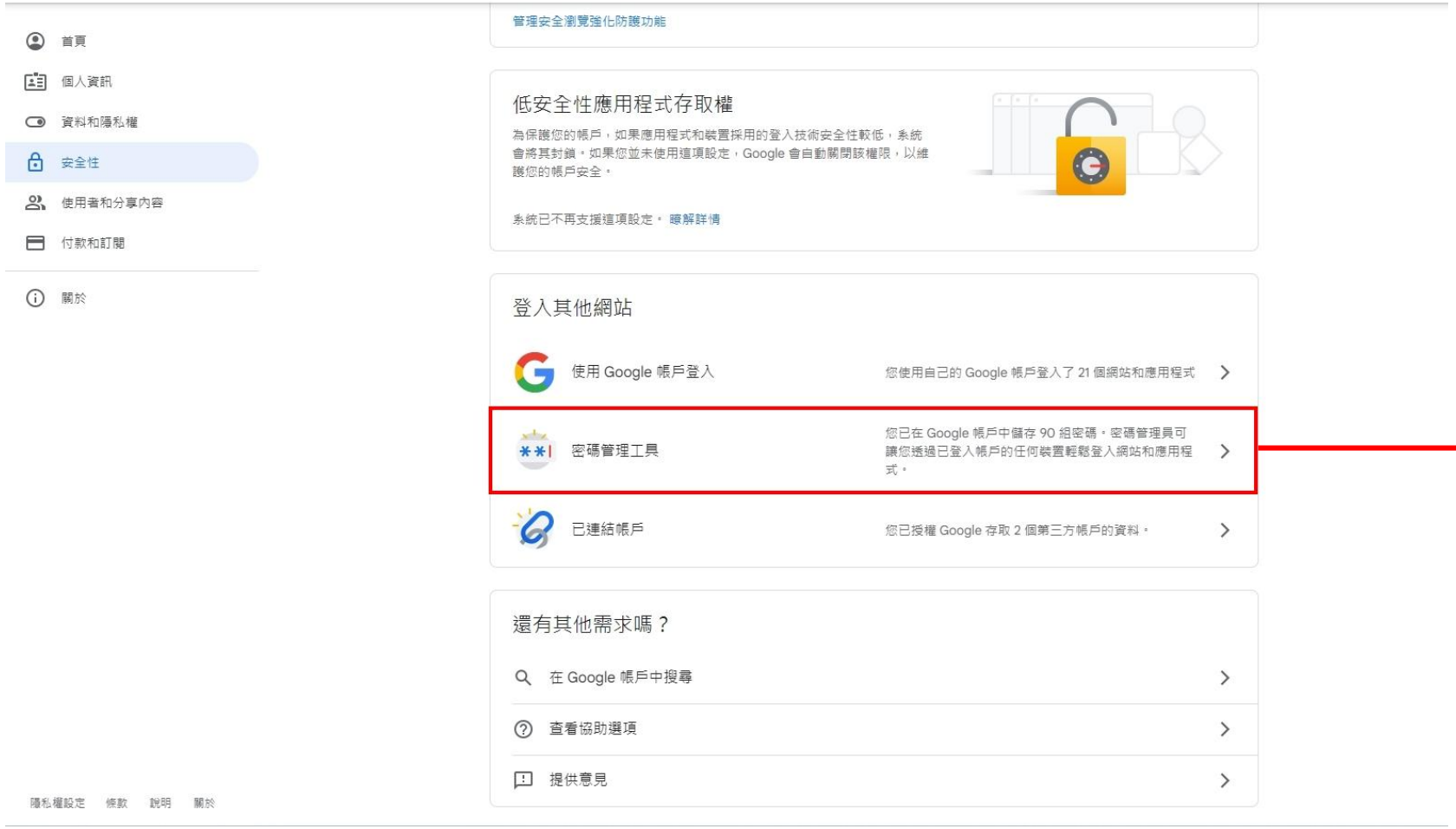

管理你的Google帳戶

# Chrome刪除已儲存之密碼(3/8)

點擊左上角的安全性

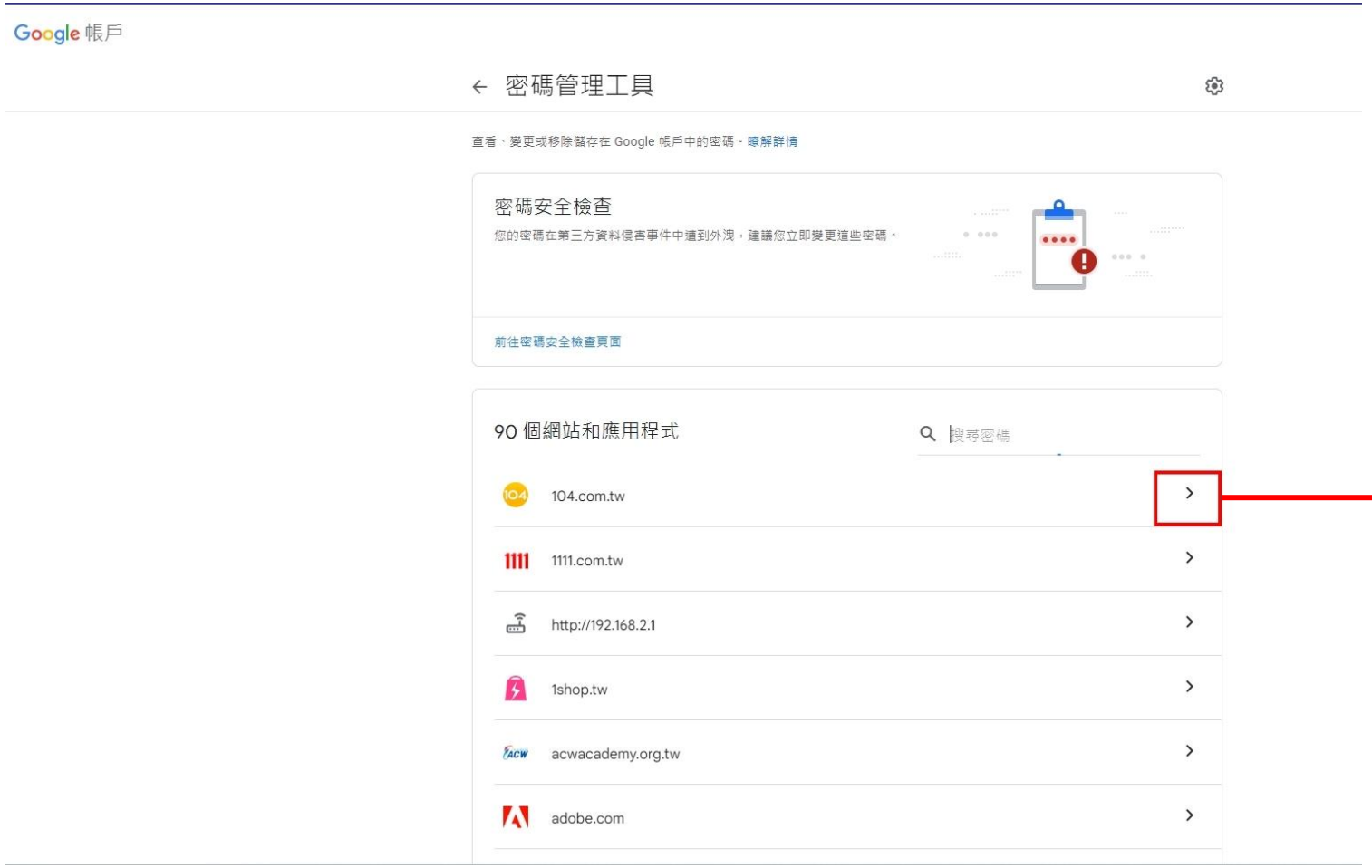


# Chrome刪除已儲存之密碼(4/8)




密碼管理工具

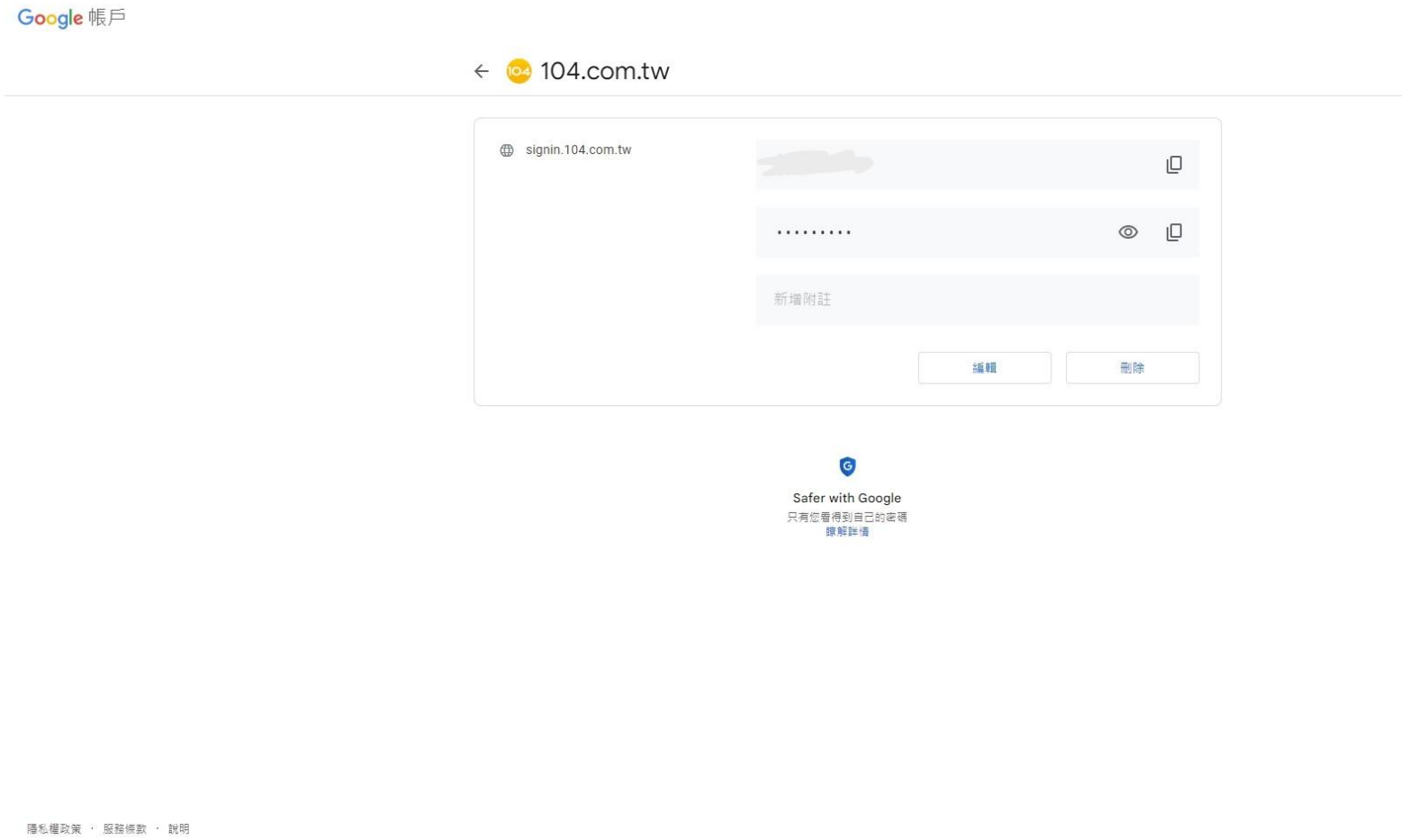
# Chrome刪除已儲存之密碼(5/8)



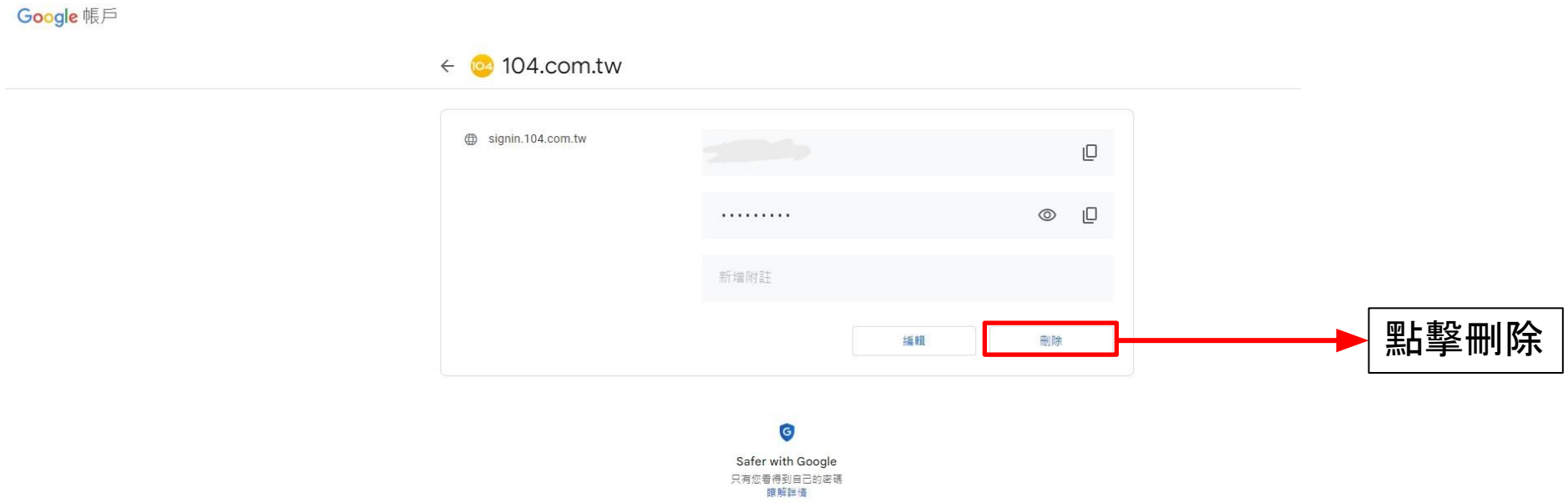

選擇預刪除之密碼的網站或是應用程式

# Chrome刪除已儲存之密碼(6/8)

# Chrome刪除已儲存之密碼(7/8)



# Chrome刪除已儲存之密碼(8/8)




點擊刪除

# 課程大綱

- 生活中所隱藏的資安風險
- 行動裝置安全
- 社交工程事件
- 雲端安全
- 熱門AI技術使用應注意事項

# 統計2022年釣魚郵件激增569%

## 2022年釣魚郵件激增569%

2023 / 04 / 07 - 編輯部

Facebook LinkedIn Twitter 新增至最愛文章

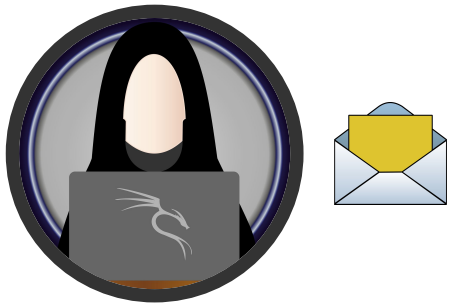

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10398

# 駭客寄出釣魚郵件之目的

- 竊取機敏資料
  - 冒充金融或網路服務通知信，主要騙取金融相關服務的登入帳號及密碼，可能也是為了後續騙取金錢財物目的;其次是電子郵件或其它網路服務的登入帳密
- 騙取金錢財物
  - 多半在郵件內容中聲稱有不錯的財務合作方案，或是通知受害人中了大獎，以誘騙受害人匯款
- 誘導執行惡意程式
  - 通常在釣魚郵件中放置惡意程式、惡意連結，並誘騙受害人開啟，目的在取得受害者電腦的控制權

https://www.softnext.com.tw/solution_01.html

# 社交工程入侵過程



**主旨：**普發6000元再加碼6000元！

**內容：**
行政院會報告「全民共享普發現金規劃」將再抽出10000個名額加碼6000元，請至下方連結登記資格，報名資格將於5月底截止，千萬別錯過！
https://6000.gou.tw

v → u

植入木馬程式、鍵盤側錄程式等等，竊取點擊連結者的電腦內資料以及帳號密碼等等

# 寄件人

- 確認該寄件人是否為機關內部同仁
- 是否曾經跟該電郵件聯繫過
- 確認電子郵件地址
  - @Microsoft.com
  - @Micorsoft.com

駭客可能會用拼寫錯誤的假網域來騙你

https://www.epochtimes.com/b5/22/12/26/n13891994.htm

# 收件人

- 確認電子郵件中的其他收件人

駭客有時候會同時寄給多個收件人，且若是其他郵件的收件者名字首字母都跟你一樣，那這封電子郵件有可能是詐騙分子寄的。

https://www.epochtimes.com/b5/22/12/26/n13891994.htm

# 超連結

- 確認郵件中的超連結是否有拼錯

把滑鼠移到超連結上，看看它指向那裡(網址會顯示在螢幕左下方)。如果這個網址跟你的電子郵件中所陳述的不同，或它的拼寫類似一個已知網站但拼寫錯誤，這很明顯就是詐騙分子寄的。

https://www.epochtimes.com/b5/22/12/26/n13891994.htm

# 附件

- 確認附件是否與郵件有關係

如果你的電子郵件中含有意想不到的附件，或是附件看起來與郵件內容無關，這時候就不要點擊超連結或下載附件，除非你確定它們是安全的。

https://www.epochtimes.com/b5/22/12/26/n13891994.htm

# 日期

- 確認收到信件的時間

如果你工作使用的電子信箱在正常的上班時間之外收到電子郵件，例如凌晨3點，而這不是你在其他時區的某個熟人寄的，那你就得留意了。

https://www.epochtimes.com/b5/22/12/26/n13891994.htm

# 主旨

- 確認主旨與內文之關係

如果電子郵件的主旨與內文不相關，或看起來像是在回覆先前的電子郵件，但你並未寄過這樣的電子郵件，你在處理時要特別小心。

https://www.epochtimes.com/b5/22/12/26/n13891994.htm

# 內文

駭客通常會營造「迫切感」，讓你忽略了其他可疑的跡象，而且配合他們的要求。

如果你意外收到一封電子郵件，而寄件人的文筆很差而且有拼字錯誤，你也應該懷疑。一般公司或金融機構的代表所寄的電子郵件，其內文應該都經過潤飾，不太可能出錯。

https://www.epochtimes.com/b5/22/12/26/n13891994.htm

# 釣魚郵件範例

寄件: 重要消息 <e394021@yahoucrabdance.com>
收件: 008560@customs.gov.tw
時間: 2023-02-09 11:13
主旨: [外部郵件]印度神童預言「明年5月前有3大災難」 全球都要注意

印度神童阿南德（Abhigya Anand）近日拍攝新影片表示，
今年12月10日以後至明年5月之間會發生許多事情，提醒大家要特別注意。
今年12月的第二周起因木星逆行...完整預言就在中時新聞網

1 個附件 • Gmail 已掃描檢查


印度神童預言「明年5月前有3大災難 全球都要注意

新冠肺炎席捲全球近2年，不少人盼能趕緊回到過去的生活。對此，印度神童阿南德表示，今年12月起至明年5月會發生許多事情，包括12月可能再爆發更大規模的傳染，特別是在疫苗接種率高的國家。到了3、4月恐有一場震驚世界的災難，提醒投資人注意。另今年冬天至明年5月則要小心極端氣候，大寒大雨的狀況恐會對亞洲、歐洲等地區造成影響，預估要到明年下半年才有好日子可過。

印度神童阿南德（Abhigya Anand）近日拍攝新影片表示，今年12月10日以後至明年5月之間會發生許多事情，提醒大家要特別注意。今年12月的第二周起，可能會出現更大規模的疫情危機或是病毒傳染的範圍會擴大。且因木星逆行，許多疫苗接種率較高的國家感染率將提升，像是英國、美國、新加坡與以色列。

明年5月前3大災難....

是否為認識的電子郵件
yahoo → yahou
是否有其他不認識的收件者或副件
收到信件的時間是否正常
是否與自身業務有關

# 釣魚郵件防範手法

- 釣魚郵件:
  - 關閉電子郵件系統的預覽功能
  - 不開啟與自身業務無關的郵件
  - 注意電子郵件中的超連結
  - 若信件中有簡體字、亂碼或是大量英文等，務必要提高警覺
  - 遣詞用字較特別
  - 主旨及內容過於聳動或緊急
  - 確認郵件中內容的真偽

# 簡訊詐騙新聞

## 收到逾期汽燃費催繳簡訊 假的！勿點連結留信用卡個資

中廣新聞網

2023年4月11日 週二 上午7:24


https://tw.yahoo.com/

# 簡訊詐騙

【汽燃費逾期徵收通知】
您的111年度汽燃費逾期金額2880元，請於112/04/10前繳納，https://pmmde1.vip/ 回復1開始連結查詢

【汽燃費逾期徵收通知】
您的111年度汽燃費逾期金額2880元，請於112/04/10前繳納，https://foiurn3.vip/ 回復1開始連結查詢

1. 確認超連結是否為官方的網址
   - 政府機關網址結尾為「gov.tw」
   - 直接搜尋官網比對兩網址是否一致

2. 致電至監理所詢問

3. 使用監理所之App查詢

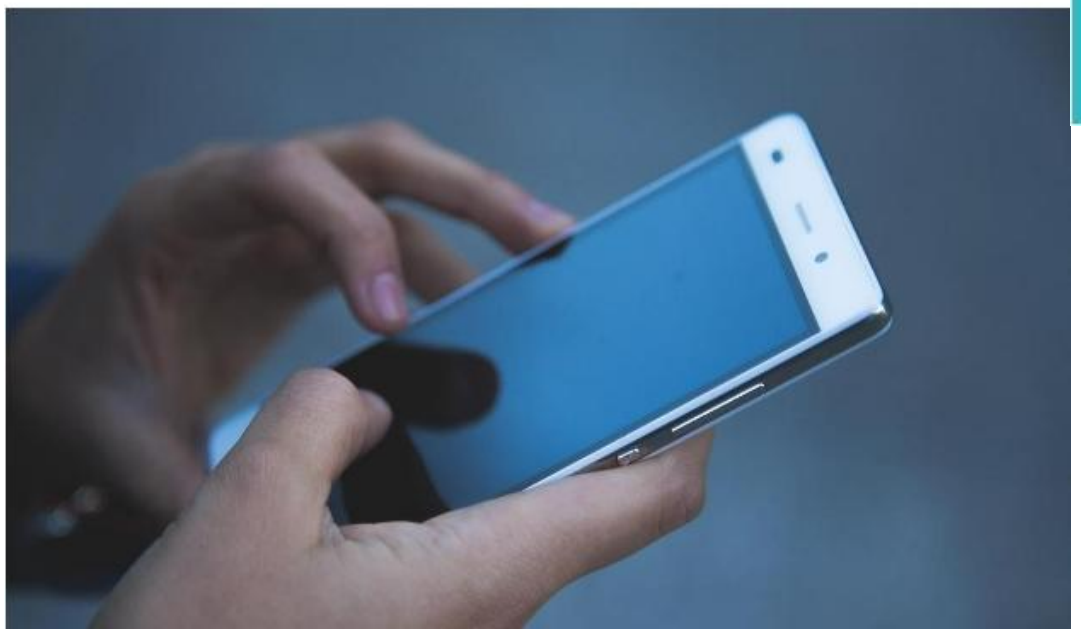
https://tw.yahoo.com/

# 簡訊騙取帳號密碼

## 手機簡訊附釣魚網站　小心帳號密碼被偷窺

文｜劉文淵

鏡 | f LINE | $ 贊助本文



1位家住台中從事服務業、年約35歲的伍姓小姐，日前收到一則手機簡訊，內容表示「您所在地區帳戶將在近期中止」，並附上一則短網址連結。伍小姐不疑有他點擊該網址查看，發現是虛擬通貨交易所「幣安」網站，依據網頁指示填寫輸入個人登入帳號、密碼，沒想到她輸入的網頁，竟是歹徒架設釣魚網站。

https://www.mirrormedia.mg/story/20220424soc013/

# 詐騙簡訊手法

## 一、詐騙簡訊手法

- **Step 1.假簡訊吸引注意**

詐騙集團會假冒政府單位、銀行、郵局或快遞公司傳送訊息。

- **Step 2.要求點擊詐騙網址**

再以申請或查詢名義，要求受害人點擊惡意網址。

- **Step 3.竊取個資**

假網站要求受害人輸入個資，或是直接在手機上安裝惡意程式APK

- **Step 4.詐騙成功**

成功竊取受害人帳號資訊後，再盜領存款、盜刷信用卡或用受害人帳號來詐騙他人。

https://houseloan.tw/spam-message/

# 常見詐騙簡訊內容(1/2)

(1)【衛生福利部】恭喜您符合條件，可提領防疫補貼，複製鏈結到瀏覽器領取。

(2) 恭喜您，您的防疫補助請綫上領取，點hxxp:// xx.com 領（複製網址到瀏覽器打開）

(3) 因應「COVID-19」疫情影響 我國（109）年1月成立【XX金融】疫情補助貸款中心 在2月公佈（嚴重特殊傳染性肺炎防治及救援補助）行政號依特別條例450億新台幣貸款救援 8月正式開啟 台灣公民憑本人身分證即可獲取10到300萬新台幣的貸款額度 一萬塊每月只需支付60塊利息 最高還可分期36期 讓民眾（更好領 更好用 更方便）盡快帶動消費 讓國泰金融跟民眾一起對抗疫情 添加信貸專員免費咨詢疫情救濟貸 信貸專員LINE：xx

(4)【xx貸】提醒您已獲50-100萬新台幣借款資格。每一萬塊月利息只需60塊。月繳無壓力！無需照會，無需保人，沒有手續費。當天辦理當天入帳！21年網路口碑第一貸款公司。添加信貸專員免費咨詢改善財務問題。添加信貸專員 LINE：xx

(5) 幫我LINE好友輔助認證！

(6) 我是xx銀行的xxxx，剛剛有與你聯絡，麻煩你聯繫我LINE：xx！

# 常見詐騙簡訊內容(2/2)

(7) 【xx銀行】您的銀行賬戶顯示異常，請立即登入榜定用戶資料，否則賬戶將凍結使用：hxxp:// xx.com

(8) Hi！我是XX證券投信的XXX ，請儘快加我赖，我傳些檔案，自營商有牌导師免費三檔報牌送給你,我的ID：xxxx ！

(9) 跟上新時代炒股模式，逆勢中把握機遇，明天你也是市場的贏家！LINE：xxxx 前來領取飆股，逆風起飛！

(10) 8月股市橫盤走勢不穩定，添加LINE：xxxx免費領取書籍，九月即將開啟免費講解課程，名額有限！告訴你如何在動盪的市場中運用135均線技術分析準確判斷未來趨勢，帶你研判九月風險行情！

(11) 快遞包裹已發，請您查收：xxxx。

(12) 您的貨運單號是70****76，請透過hxxp:// xx.com查詢

(13) 可以跟你交個朋友嗎？LINE：xxxx。

# 詐騙簡訊防範手法

Step 1. 內容是否為熱門時事或是緊急事件

Step 2. 確認簡訊中的超連結是否與官網一致

Step 3. 致電至相關單位詢問

# 課程大綱

- 生活中所隱藏的資安風險
- 行動裝置安全
- 社交工程事件
- 雲端安全
- 熱門AI技術使用應注意事項

# 資料上傳至雲端最大隱憂？

1. 雲端平台遭駭客入侵
2. 遭雲端平台內部員工竊取資料

# 雲端服務供應商遭駭

## Puma因軟體商被勒索軟體攻擊外洩逾6千員工資料

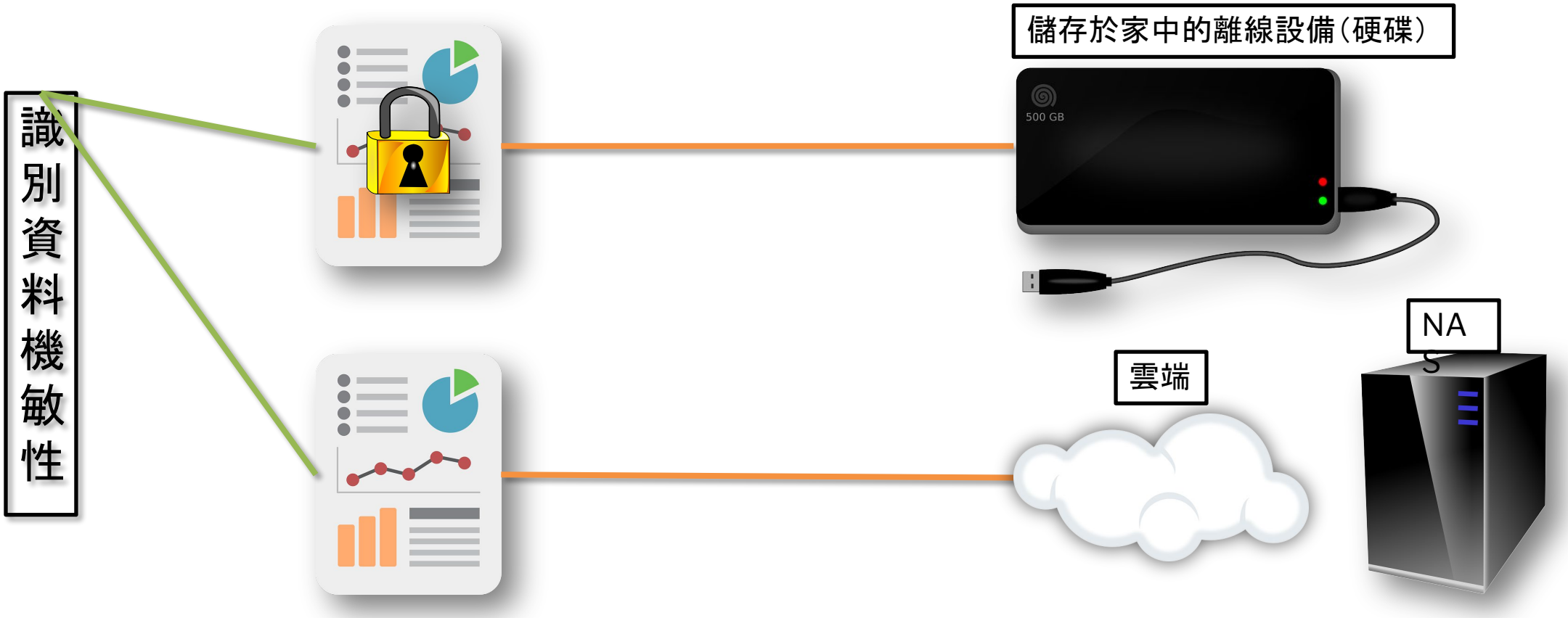
運動品牌Puma使用的人力管理雲端服務業者遭勒索軟體攻擊，駭客盜走6千多名Puma員工個資

文/ 林妍溱 | 2022-02-10 發表

讚 66 分享


https://www.ithome.com.tw/news/149288

# 資料如何保存？



# 提升密碼強度

1. 符合密碼複雜度
   - 英文字母大小寫、數字、特殊符號
2. 至少8碼以上(建議12碼)
   - 密碼越長，破解時間越久
3. 勿使用與個人資料相關之資訊作為密碼
   - 身份證字號、生日、手機號碼、車牌、家裡電話、員工編號等
4. 勿將所有密碼接設定為同一組
   - Line、Facebook、IG、Gmail、手機密碼、資料夾加密密碼、網銀密碼等
5. 開啟多因子驗證機制
   - 如 OTP(單次驗證密碼)、生物辨識功能
6. 避免使用常見的密碼

# 駭客破解密碼需要多久？

一、駭客可在低於2秒內瞬間破解的密碼

4個到11個數字組合。

4個到8個的英文字母小寫組合。

4個到6個的英文字母大小寫組合。

4個到6個的數字與英文字母大小寫組合。

4個到6個的數字混合英文字母大小寫與符號的組合。

二、駭客可在低於一分鐘內破解的密碼

12個數字組合2秒內破解。

13個數字組合19秒內破解。

9個英文小寫字母組合10秒內破解。

7個英文字母大小寫組合2秒內破解。

7個數字與英文字母大小寫組合7秒內破解。

7個數字混合英文字母大小寫與符號的組合31秒內破解。

https://3c.ltn.com.tw/news/48218

# 密碼添加特殊字元有用嗎？

**不過，若用戶在基本密碼中添加像是「@#_」1個特殊字符，會增加90分鐘的破解時間；若添加2個特殊字符，破解時間則延長到2天4小時**。對此，研究機構以「London1984」、「London_1984」、「@London_1984」三組不同的密碼展開實測，發現在暴力破解的情況下，「London1984」需要 3.6 萬次暴力破解；「London_1984」只加了1個特殊字符就飆升至5316 萬次；添加2個特殊字符的「@London_1984」則需要 18 億次。

雖然增添特殊字符能大幅延長破解時間，但研究機構指出，若使用更高級的破解工具，也可能會達到秒破解，因此建議用戶設置密碼時還是越複雜越好，至少使用 12-15 個字元，且組合包含數字、大小字母與特殊符號，或使用雙重驗證或是密碼管理器保護帳號安全。

https://tw.news.yahoo.com/news/10%E7%B5%84%E5%AF%86%E7%A2%BC-%E5%85%8D%E8%B2%BB%E5%B7%A5%E5%85%B7%E5%8F%AF%E7%A7%92%E7%A0%B4%E8%A7%A3-1%E6%8B%9B%E6%8F%90%E9%AB%98%E5%AE%89%E5%85%A8%E5%BA%A6-071455781.html

# 駭客破解密碼需要多久？

若改換一個角度來看，怎樣的密碼組合，會讓駭客得花上至少3年的時間才會破解？從 Hive Systems 釋出研究報告的圖表可以看出，基本上需要符合兩個條件，就是密碼字元長度至少要在10個以上，且密碼需採數字混合英文大小寫字母。

另，若密碼組合還有參雜符號，相對地駭客要破解的難度與時間也越高。例如：10個數字與英文字母大小寫組合，需花3年破解；11個數字混合英文字母大小寫與符號的組合，則需花長達34年破解。

https://3c.ltn.com.tw/news/48218

# 個資在暗網中的價格

# 信用卡價格

| | | |
|---|---|---|
| **Credit Card Data** | Credit card details, account balance up to 5,000 | $120 |
| | Credit card details, account balance up to 1,000 | $80 |

# 社群媒體價格

| | | |
|---|---|---|
| **Social Media** | Hacked Facebook account | $45 |
| | Hacked Instagram account | $40 |
| | Hacked Twitter account | $25 |
| | Hacked Gmail account | $65 |
| | Instagram followers x 1000 | $4 |

# 平台價格

| | | |
|---|---|---|
| **Hacked Services** | Netflix account, 1-year subscription | $25 |
| | Bet365 account | $40 |
| | Kaspersky account | $5 |
| | NBA League Pass | $7 |
| | Various adult site accounts | $5 |
| | Canva Pro yearly | $6 |
| | CNBC Pro | $3 |

# 課程大綱

- 生活中所隱藏的資安風險
- 行動裝置安全
- 社交工程事件
- 雲端安全
- 熱門AI技術使用應注意事項

# ChatGPT

# ChatGPT 製作釣魚郵件

## 騙徒ChatGPT製釣魚郵件

更新時間：03:14 2023-03-08

https://www.stheadline.com/article/3206751/%E9%A8%99%E5%BE%92ChatGPT%E8%A3%BD%E9%87%A3%E9%AD%9A%E9%83%B5%E4%BB%B6

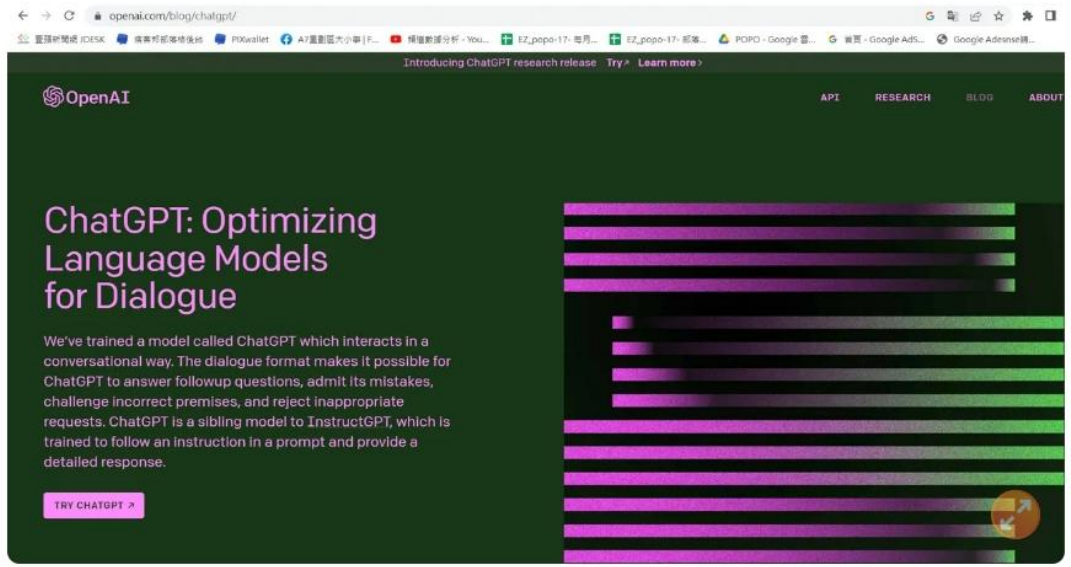
# 山寨版 ChatGPT

## ChatGPT怎麼笨笨的？竟下載到山寨版「慘被盜刷1200」　他崩潰喊要剪卡

財經地產 2023/02/26 15:09

分享 分享 加入好友

【即時中心／綜合報導】當心！ChatGPT APP是山寨版，還會盜刷你的錢！OpenAI開發的一個人工智慧聊天機器人程式ChatGPT在全球引發熱潮，不過有網友在網路上PO文呼籲大家要小心，因為已經有「山寨版ChatGPT APP」專門詐騙信用卡號盜刷無辜民眾荷包！

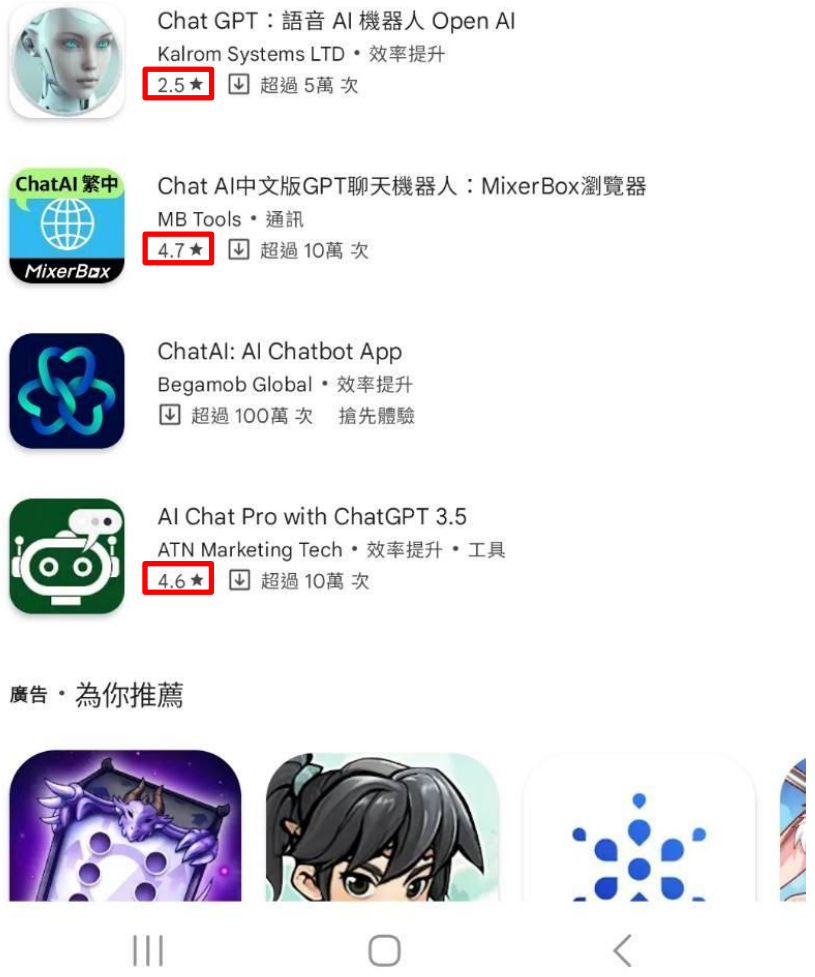



OpenAI開發的人工智慧聊天機器人程式ChatGPT，目前僅有網頁版。翻攝《OpenAI》網頁

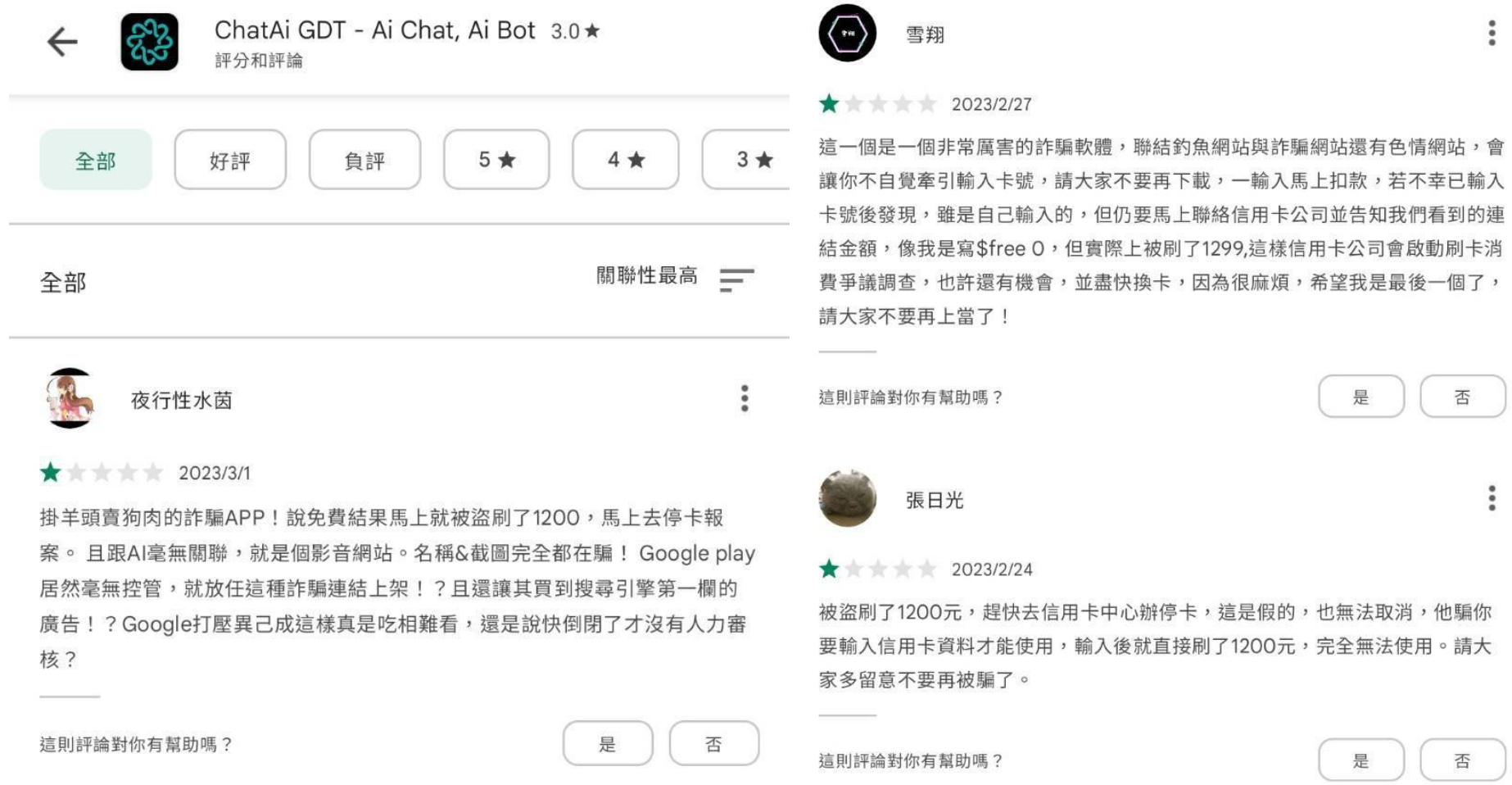
https://tw.nextapple.com/life/20230226/5B9BE16284A7A1CEB93E6F0D3118791E

# 檢視APP評論(1/2)


chatgpt app中文
評分
家庭
新功能
AI Chat - AI 聊天機器人 AI 朋友 & 專家
廣告 • Open companion & AI assistant GP tech ...
含廣告內容 • 應用程式內購
安裝
4.3 ★
9萬 則評論
超過 500萬 次
下載次數
3+
3 歲以上
畅爽交流，让你的聊天更智能
ChatGPT中文版-AI聊天
AppStation Studio • 工具
2.7 ★ 超過 10萬 次
ChatAi GDT - Ai Chat, Ai Bot
Now Tech • 工具
3.0 ★ 超過 100萬 次


Chat GPT：語音 AI 機器人 Open AI
Kalrom Systems LTD • 效率提升
2.5 ★ 超過 5萬 次
Chat AI中文版GPT聊天機器人：MixerBox瀏覽器
MB Tools • 通訊
4.7 ★ 超過 10萬 次
ChatAI: AI Chatbot App
Begamob Global • 效率提升
超過 100萬 次 搶先體驗
AI Chat Pro with ChatGPT 3.5
ATN Marketing Tech • 效率提升 • 工具
4.6 ★ 超過 10萬 次
廣告 • 為你推薦

# 檢視APP評論(2/2)


ChatAi GDT - Ai Chat, Ai Bot 3.0★
評分和評論
全部
好評
負評
5★
4★
3★
全部
關聯性最高
夜行性水茵
2023/3/1
掛羊頭賣狗肉的詐騙APP！說免費結果馬上就被盜刷了1200，馬上去停卡報案。 且跟AI毫無關聯，就是個影音網站。名稱&截圖完全都在騙！ Google play居然毫無控管，就放任這種詐騙連結上架！？且還讓其買到搜尋引擎第一欄的廣告！？Google打壓異己成這樣真是吃相難看，還是說快倒閉了才沒有人力審核？
這則評論對你有幫助嗎？
是
否
雪翔
2023/2/27
這一個是一個非常厲害的詐騙軟體，聯結釣魚網站與詐騙網站還有色情網站，會讓你不自覺牽引輸入卡號，請大家不要再下載，一輸入馬上扣款，若不幸已輸入卡號後發現，雖是自己輸入的，但仍要馬上聯絡信用卡公司並告知我們看到的連結金額，像我是寫$free 0，但實際上被刷了1299,這樣信用卡公司會啟動刷卡消費爭議調查，也許還有機會，並盡快換卡，因為很麻煩，希望我是最後一個了，請大家不要再上當了！
這則評論對你有幫助嗎？
是
否
張日光
2023/2/24
被盜刷了1200元，趕快去信用卡中心辦停卡，這是假的，也無法取消，他騙你要輸入信用卡資料才能使用，輸入後就直接刷了1200元，完全無法使用。請大家多留意不要再被騙了。
這則評論對你有幫助嗎？
是
否

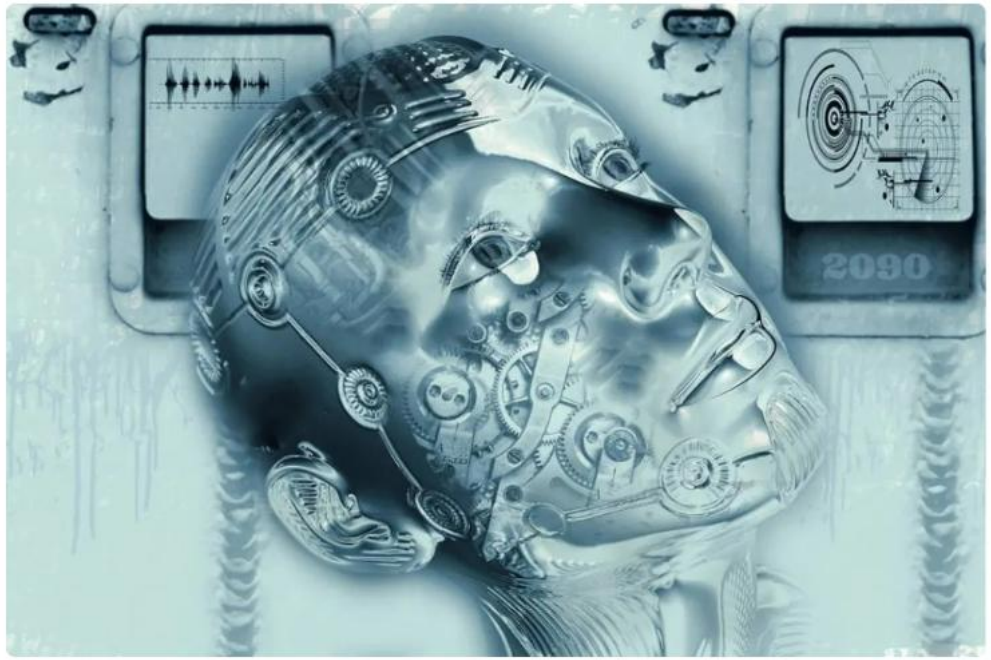
# Deepfake 深偽技術

# Deepfake技術模仿聲音

## 駭客用AI仿冒英國能源公司CEO 語音命令員工匯款22萬歐元

王 佐銘

2020年8月29日 · 3 分鐘 (閱讀時間)



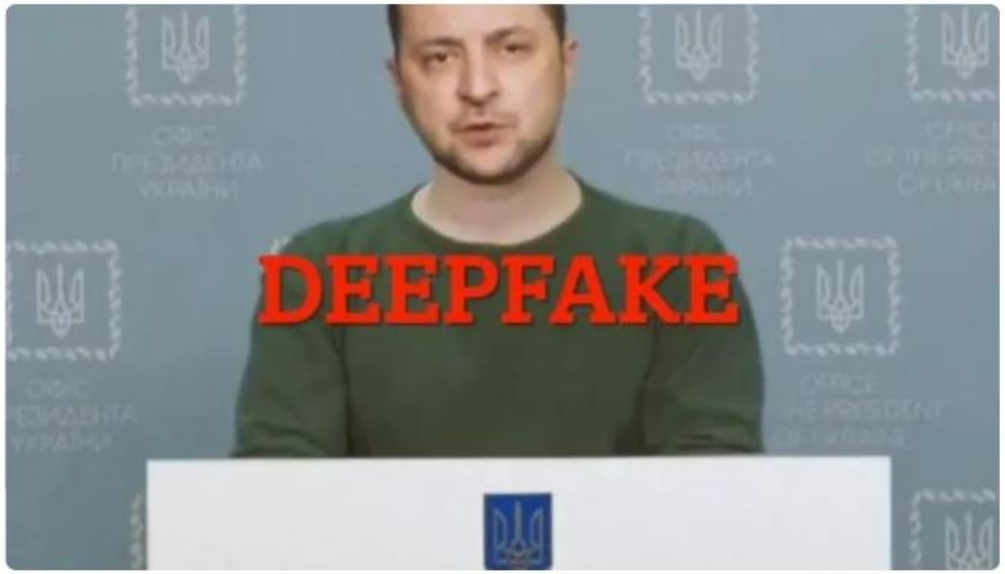

https://tw.news.yahoo.com/news/%E9%A7%AD%E5%AE%A2%E7%94%A8ai%E4%BB%BF%E5%86%92%E8%8B%B1%E5%9C%8B%E8%83%BD%E6%BA%90%E5%85%AC%E5%8F%B8ceo-%E8%AA%9E%E9%9F%B3%E5%91%BD%E4%BB%A4%E5%93%A1%E5%B7%A5%E5%8C%AF%E6%AC%BE770%E8%90%AC%E6%AD%90%E5%85%83%E8%A9%90%E9%A8%99%E6%88%B0%E5%8A%9F-103107244.html

# Deepfake技術模仿影像

【烏克蘭成戰場】俄網瘋傳澤倫斯基投降片 全是Deepfake假造「恐僅冰山一角」

陳凱俊

2022年3月18日 · 3 分鐘 (閱讀時間)




澤倫斯基的投降影片被抓包是用deepfake技術假造的。（翻攝自推特@MikaelThalen）

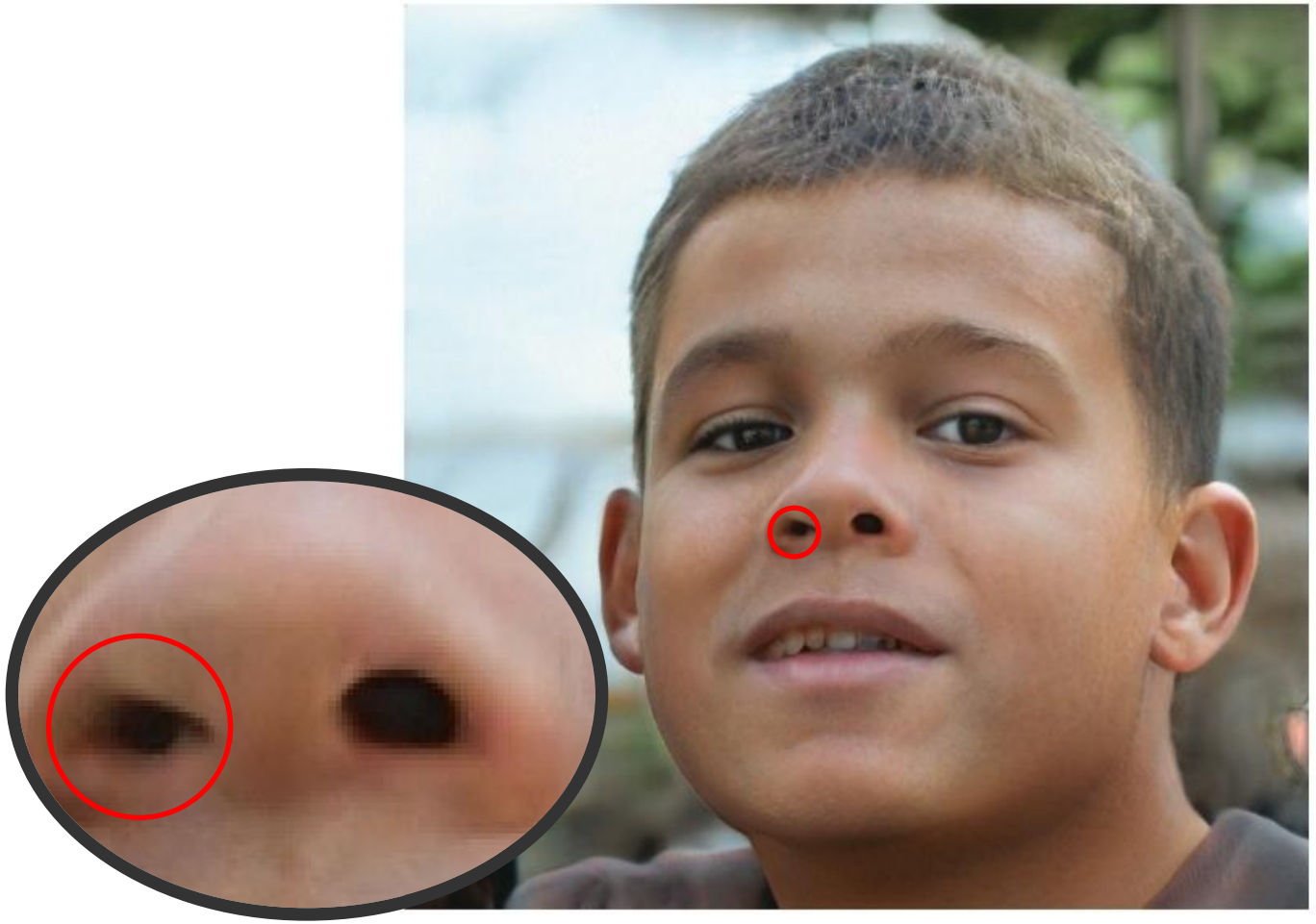
https://tw.news.yahoo.com/news/%E7%83%8F%E5%85%8B%E8%98%AD%E6%88%90%E6%88%B0%E5%A0%B4-%E4%BF%84%E7%B6%B2%E7%98%8B%E5%82%B3%E6%BE%A4%E5%80%AB%E6%96%AF%E5%9F%BA%E6%8A%95%E9%99%8D%E7%89%87-%E5%85%A8%E6%98%AFdeepfake%E5%81%87%E9%80%A0-%E6%81%90%E5%83%85%E5%86%B0%E5%B1%B1-%E8%A7%92-232526539.html

# Deepfake 影像辨識方法

- 眨眼率；Deepfake製作對象的眨眼率少於正常人
- 語音和嘴唇運動的同步狀況
- 臉部輪廓
- 模糊的痕跡、畫面停頓或變色

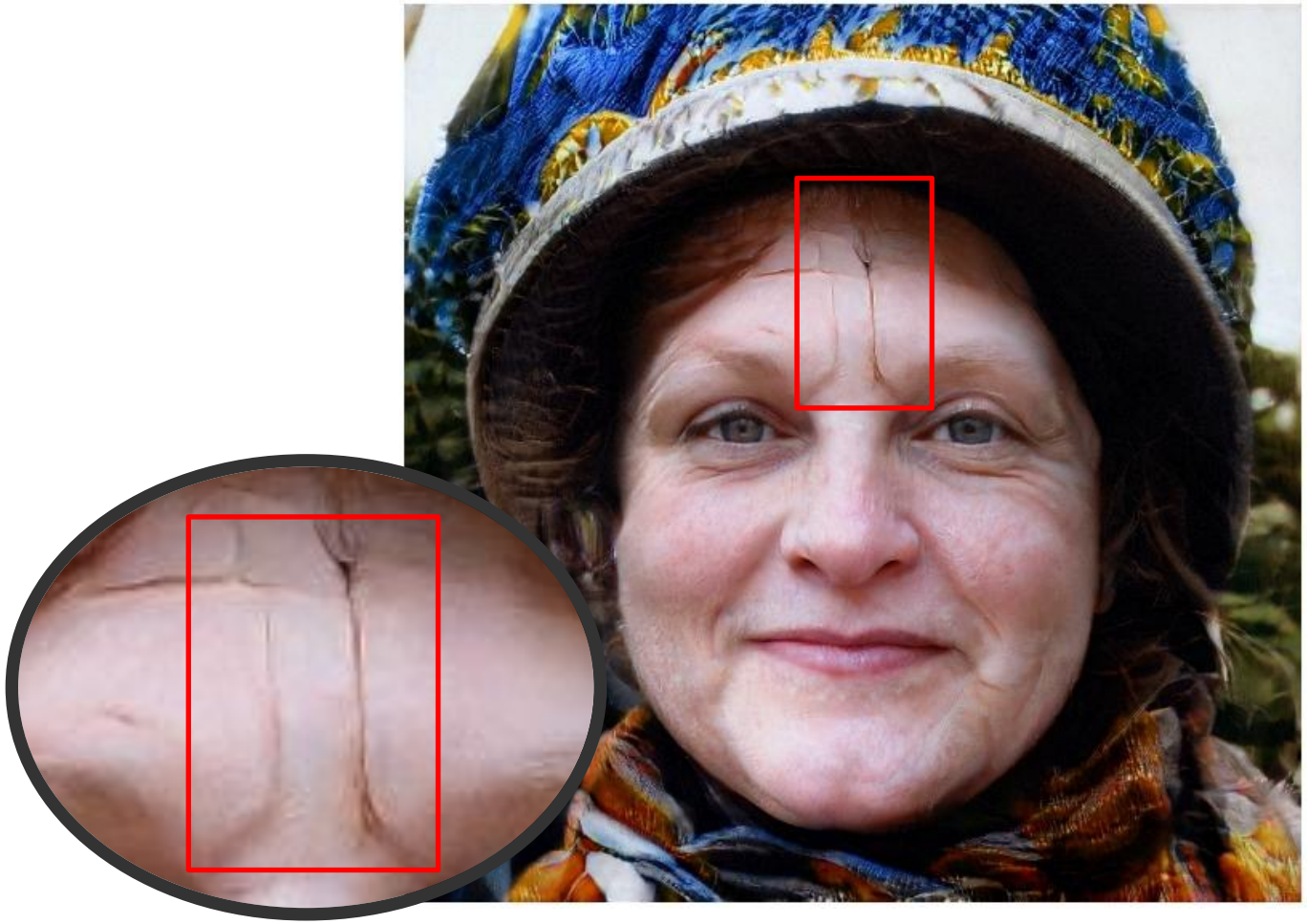
https://blog.trendmicro.com.tw/?p=63452

# Deepfake技術模仿圖像範例 1



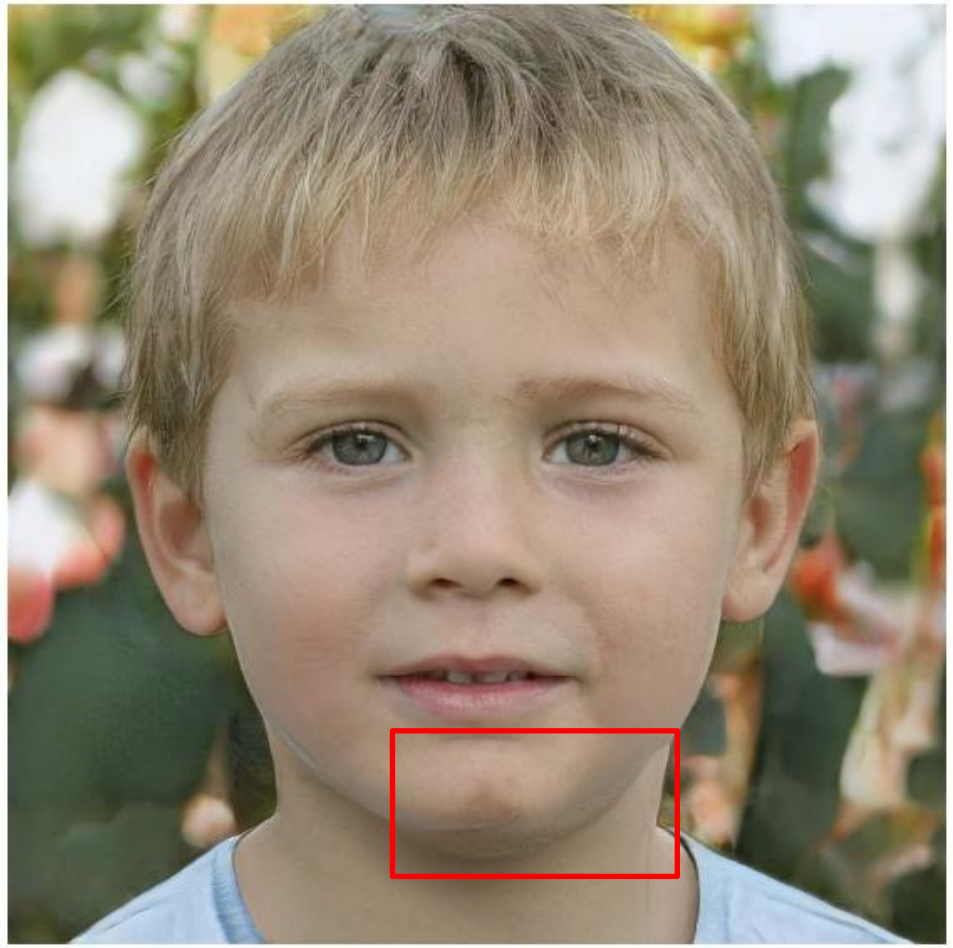
https://www.whichfaceisreal.com/

# Deepfake技術模仿圖像範例 2



https://www.whichfaceisreal.com/

# Deepfake技術模仿圖像範例 3



https://www.whichfaceisreal.com/

# 如何避免遭到駭客攻擊

# 駭客常使用的五種手法

1. 釣魚郵件
2. 公用wifi
3. 惡意App
4. 軟體漏洞
5. 惡意網站

# 釣魚郵件防範手法

- 收到郵件時，應注意事項
  - 寄件人
  - 收件人
  - 超連結
  - 附件
  - 日期
  - 主旨
  - 內文

# 公用wifi防範手法

- 盡量使用自己手機的熱點
- 注意所連接的SSID
  - 是否與店家提供的名稱一致
- 避免傳輸機敏資訊
  - 基本上都是店家的電話

# 惡意App防範手法

- 注意評論
- 注意開發商資訊
- 注意要求權限
- 注意更新日期
- 避免在來源不明的網站下載

# 軟體漏洞防範手法

- 定期更新軟體
- 避免使用停止更新服務的軟體

# 惡意網站防範手法

- 避免瀏覽與自身業務無關之網站
- 注意該網站是否加密
- 注意網址是否與官方網址一致
  - 直接輸入機關或企業名稱，比對網址是否一致

# 謝謝聆聽!

漢昕科技 蘇森堯