

# 智慧時代新生活 ~你為什麼會被騙



講師 呂守箴

## 大綱

- 近期資安案例探討：
  - 個資外洩與詐騙手法
  - 利用 AI 進行深偽技術 (Deepfake) 詐騙
- 隱私與個資的新風險：
  - 網路蒐集哪些隱私與個資？
  - 蒐集的隱私與個資外洩，被詐騙集團利用
  - 如何調整隱私與個資，防止被廣告騷擾



參考資料 & 教學影片  
(掃描後按超連結)

- 講師： 呂守箴
- E-Mail： shooujen@gmail.com



- 講師資料： [goo.gl/Uzv2BW](https://goo.gl/Uzv2BW) (注意英文大小寫)

- 智慧時代新生活 FB 粉絲專頁： [facebook.com/SmartEraNewLife](https://facebook.com/SmartEraNewLife)
- 智慧時代新生活 IG 專業帳號： [instagram.com/SmartEraNewLife](https://instagram.com/SmartEraNewLife)
- 智慧時代新生活 YouTube 頻道： [youtube.com/OpenBlueSmartLife](https://youtube.com/OpenBlueSmartLife)
- 資安玩家村 LINE 社群： [ppt.cc/fDWsrX](https://ppt.cc/fDWsrX)
- 資安玩家村 Discord 社群： [discord.gg/Wfktn6qWdY](https://discord.gg/Wfktn6qWdY)



- 講師個人 FB： [facebook.com/openblue](https://facebook.com/openblue)
- 講師個人 IG： [instagram.com/openblue.ig](https://instagram.com/openblue.ig)
- 講師個人 YouTube： [youtube.com/OpenBlue](https://youtube.com/OpenBlue)



 facebook



 YouTube



 Instagram



LINE 社群



Discord 社群

# 近期資安案例探討： 個資外洩與詐騙手法

📅 發布日期：112-12-29 🔄 更新日期：112-12-29 📍 發布單位：刑事警察局公共關係室



## 刪系統又竊客戶個資 工程師及共犯遭警查獲

一、偵辦單位：臺灣臺中地方檢察署(冬股)、刑事警察局偵查第九大隊(第二隊)、科技犯罪防制中心科技偵查隊、臺中市政府警察局豐原分局。

二、查獲時間：112年7月13日、112年12月14日。

三、查獲地點：臺中市、南投縣等地。

四、查獲嫌犯：主嫌游○○(72年次、男)、陳○○(76年次、男)、林○○(81年次、男)等3人

五、查獲贓證物：查扣手機3支、電腦2臺及遭移轉會員訂單資料庫約19萬筆等資料庫電磁紀錄。

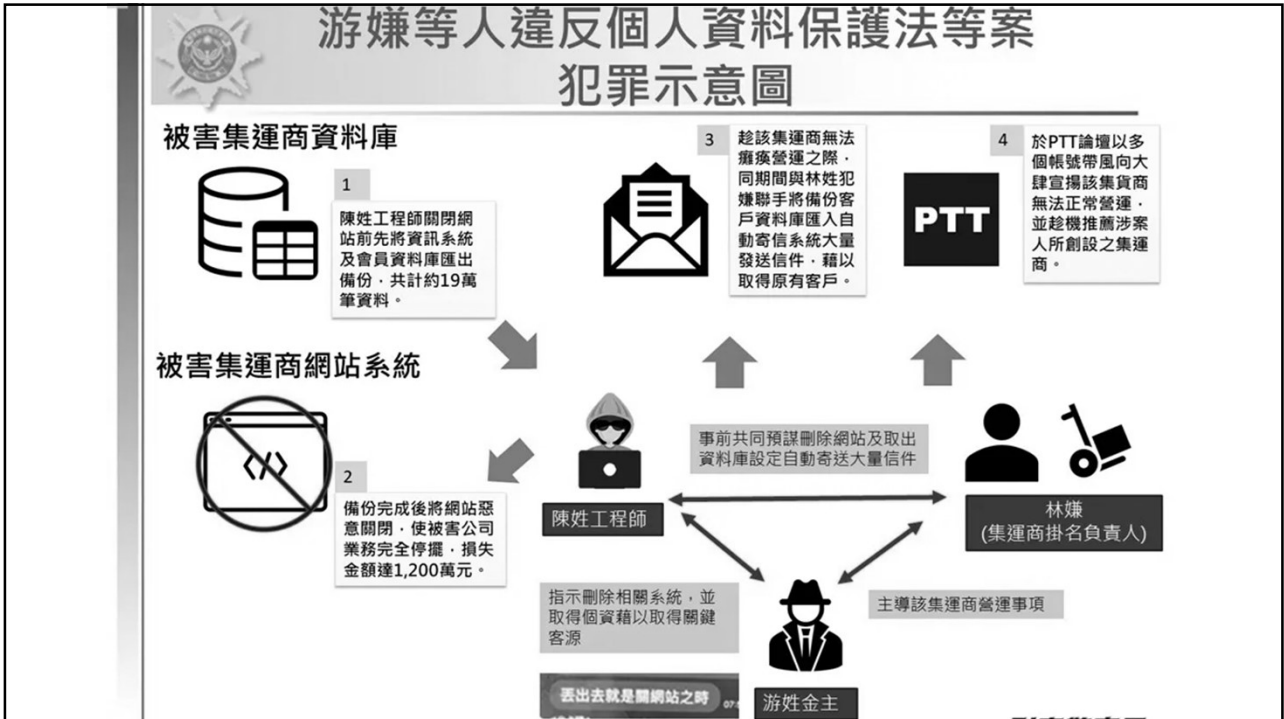
六、案情摘要：

刑事警察局於111年11月中發現PTT論壇及相關資安新聞網站熱烈討論某美國集運物流網站突然無預警關閉，經向廠商確認，證實網站及系統已關閉無法運作，復發現該網站多名註冊會員反映於網站遭關閉期間，亦收到另一家新成立之競爭廠商廣告電子郵件，研判有個資遭對外洩與不當使用情事，刑事警察局遂錄案偵辦。

經調查，網站系統遭惡意關閉後，公司業務完全停擺，損失金額逾新臺幣1,200萬元，案經報請臺中地方檢察署冬股檢察官指揮，於112年7月13日、12月14日由刑事警察局偵查第九大隊第二隊、科技犯罪防制中心科技偵查隊、臺中市政府警察局豐原分局共同執行搜索、拘提勤務，查獲游姓主嫌、陳姓工程師及林姓共犯，查扣作案手機、電腦及會員訂單資料庫近19萬筆個人資料等電磁紀錄，全案將依違反個人資料保護法、背信、妨害電腦使用等罪嫌移請臺灣臺中地方檢察署偵辦。

刑事警察局呼籲，公司行號應提升資訊安全防護及個人資料保護之意識，落實內部資訊系統權限分流與控管機制，人員異動時個人所保管之資料及所用帳號應確實交接，避免遭不法人士以突破系統漏洞、埋設後門帳號等手法竊取營業秘密或侵害電磁紀錄；另外，保障個人資料安全為當前重點工作項目之一，若有違法蒐集、處理或利用個人資料之情事，警方將嚴加查辦，籲有心人士切勿心存僥倖。

## 游嫌等人違反個人資料保護法等案 犯罪示意圖

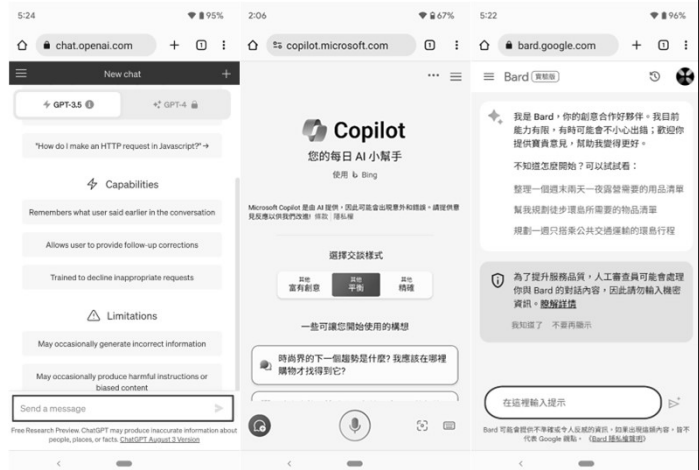


## 近期資安案例探討： 利用 AI 進行深偽技術 (Deepfake) 詐騙

# 什麼是生成式 AI ？

- 生成式 AI 是一種可以創造對話、故事、影像、視訊和音樂等內容和想法的人工智慧。

- OpenAI ChatGPT
- **Microsoft Copilot (將 OpenAI 技術整合到微軟產品)**
- Google Bard
- OpenAI DALL·E
- Midjourney
- Stable Diffusion



## 微軟 Copilot APP 正式版



[正式版] 免費 且 無廣告  
可輸入中文



支援語音生成文字、圖片



### Microsoft Copilot

Microsoft Corporation

專為 iPad 設計

在「生產力工具」類中排名第 27

★★★★★ 2.6 · 34 則評分

免費 · 提供 App 內購買



### Copilot

## 什麼是 深偽技術 (Deepfake) ?

- 深偽技術 (Deepfake) 又稱深度偽造，是深度學習 (deep learning) 和偽造 (fake) 的混和名詞，指將已有的圖像或影片合成疊加至目標圖像或影片上進行偽造的技術。
- 一種肉眼難辨的修圖或者影片合成的技術。
- 目前常見於換臉偽造的手法，主要是透過交換兩張圖像的人臉達到偽造身分的目的。
- 現階段換臉偽造和表情偽造，已經可以結合語音偽造技術，達到完全偽裝的手法。

📅 發布日期：112-07-16 🔄 更新日期：112-07-17 📄 發布單位：刑事警察局公共關係室



### 刑事警察局提醒注意深度偽造詐欺風險

近年來，深度偽造 (Deepfake) 技術的快速發展給社會帶來巨大的衝擊。這項技術可以製造出逼真的虛假影像和音訊，將人們的臉孔和聲音合成到完全捏造的場景中，不肖分子可能使用這種技術製造出假訊息、甚至用於詐欺犯罪或侵犯個人隱私，深度偽造可能冒充公眾人物、政府官員或其他知名人士，以製造虛假信息、進行詐騙或破壞他人形象，這種行為將對社會秩序和公民信任造成巨大威脅。

鑑於近期各國有關投資加密貨幣之詐欺案情升高，最新的詐欺案例是關於埃隆·馬斯克 (Elon Musk) 的深度偽造，這段假影片由假交易平台BitVex發出，假冒馬斯克推銷一個「新投資」，鼓勵人們應該把錢投入到這個加密貨幣中，號稱可以獲得30%的股息。特斯拉首席執行長立刻在推特上發出警告說，聲明該影音是深偽假冒的，不但聲音不清楚且很機械化。

美國聯邦調查局FBI也已經於今年6月發布警告，指出深度偽造的影音開始被利用於挖礦、區塊鏈、虛擬資產等投資詐騙案件，今年4月份開始，利用深度偽造進行「性勒索詐騙」的受害者也有增加趨勢。

因此，刑事警察局再度提出呼籲如下：

一、提高警覺：多留意媒體報導，吸收最新的詐欺手法或深度偽造資訊與案例，適度了解深度偽造技術的工作原理和應用場景以學習分辨真實和虛假的影像或音訊。

二、冷靜分析求證：在接收到可疑訊息時，要保持冷靜和懷疑態度，尋找可靠信息來源，留意相關的報導以及評論以確認信息的可信度，識破偽造信息。

三、降低身份被盜用風險：除了保護個人隱私外，使用雙重身份驗證、強密碼和其他數位安全措施保護自己網路資訊。

警方呼籲民眾務必提高警覺、多方求證，並提醒身邊親友，瞭解此類犯罪手法；若遭遭疑似涉及Deepfake技術的犯罪情事，請立即撥打110或165反詐騙諮詢專線查證。



**利用深偽技術成產出的合成影像、圖片及語音，讓這些騙術變得更加真實**

## 駭侵者開始訓練 AI 聊天機器人進行釣魚、惡意軟體攻擊

◎發布日期：2023-08-04

資安廠商 SlashNext 發現有駭侵者推出專門用於進行釣魚與惡意軟體投放攻擊的 AI 聊天機器人，分別採用最新的 ChatGPT 與 Google Bard AI 技術來訓練。

SlashNext 旗下的資安研究人員，在 7/25 發現一個自稱為 CanadianKingpin12 的駭侵者，於多個駭侵相關論壇上刊登廣告，推廣其用於進行網路詐騙、駭侵攻擊與垃圾訊息發送專用的 AI 聊天機器人 FraudGPT。

在進一步追蹤後，SlashNext 的資安研究人員證實 CanadianKingpin12 很早就開始利用在暗網上出售的各種駭侵資料集，以 ChatGPT 和 Google Bard 等大型語言模型 (Large Language Model, LLM) 來訓練自己的 AI 聊天機器人 DarkBART；研究人員也發現 CanadianKingpin12 也利用韓國研究人員研發的另一個大型語言模型，來訓練另一個 AI 聊天機器 DarkBERT。

根據 CanadianKingpin12 的說詞，DarkBERT 在各種通用暗網資料來訓練的 AI 駭侵工具中，可說是功能最強大的一款，可以用來進行以下攻擊：

- 發動成熟的釣魚攻擊活動，用以取得目標對象的密碼與信用卡資訊；
- 執行先進的社交工程攻擊，以取得機敏資訊或目標系統的登入權限；
- 利用電腦系統、軟體或網路的資安漏洞加以攻擊；
- 製作並散布惡意軟體；
- 利用 0-day 漏洞來獲得不法所得，或破壞目標系統。

SlashNext 指出，這兩個 AI 惡意聊天機器人的開發時程都不到一個月就完成推出，由此可見 AI 的濫用，即將成為資安防護與網路犯罪令人頭痛的嚴重問題。

建議資安研究與防治單位應加強研究如何偵測並防範由 AI 執行的各種惡意攻擊手法，擁有 LLM 等先進 AI 技術的大型科技公司，亦應加強防範其工具遭到濫用於資安攻擊之上。

## 詐騙集團會如何利用「深偽」？

### 「猜猜我是誰」

詐騙集團假冒成親戚朋友，撥打電話給受害人，並稱因故急需用錢，請求儘速匯款應急……  
或是將換臉技術用於視訊，偽裝成公司高層，向下屬發出轉帳的指示……

### 「不雅照恐嚇信」

有多位知名大學教授，其肖像遭詐騙集團移花接木，拿來合成不雅照片，再以此寄送恐嚇信向這些教授勒索，威脅說若不繳交封口費便將照片散布出去……



利用深偽技術產出的合成影像、圖片及語音，讓這些騙術變得更加真實

反詐騙小金剛

臺北市府警察局刑事警察大隊

## 該怎麼加以預防？



### 針對來電匯款要求，保持警覺，主動確認

透過深偽製作的合成語音，可能讓受話者難辨真偽，誤認為是真正的親戚或朋友打來，碰到類似情形，應主動暫停通話，並透過其他管道聯繫對方以確認真實性，多一層警覺，謊言將不攻自破！

### 《刑法》第339-4條加重詐欺罪，也為因應這種手法新增了第4款的行為態樣



以電腦合成或其他科技方法製作關於他人不實影像、聲音或電磁紀錄之方法而犯詐欺罪者，處1年以上、7年以下徒刑，得併科100萬元以下罰金。

反詐騙小金剛



臺北市政府警察局刑事警察大隊

## 你知道 DEEPAKE嗎？

「利用科技不法製造的假訊息和影片，有一天都可能傷害到你我，我們都有責任阻止錯假影像傷害無辜的人。」



## DeepFake 的危害：

圖像、影片、聲音都可以偽造

- 移花接木色情影片
- 偽造名人傳播假訊息
- 破解人臉辨識盜領存款

成為一種非常不容易辨識的社交工程手法以及詐騙工具。

Facebook 蔡英文    @iing    Instagram tsai\_ingwen



# 隱私與個資的新風險： 網路蒐集哪些隱私與個資？

## 隱私與個資

- 何謂「隱私」？
  - 隱私指個人有部份不想讓眾人知道，也有權利去保護不想讓眾人知道的部分。
- 「隱私」vs「個資」
  - 隱私的範圍包含能夠辨識身分的個資，以及不能辨識身分(去識別化)的資訊。(例如：個人嗜好、飲食習慣)
  - 範例：名字+地址是個資、但喜歡住在依山傍水的別墅+偏好日式風格+吃日本料理就是隱私。
- 何謂「隱私權」？
  - 隱私權就是為了保障個人生活私密領域免於受到他人侵擾，以及保障個人資料之自主控制。
  - 保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權，以及資料記載錯誤之更正權。

- 目前沒有針對隱私/隱私權的專法

- 憲法：

第 12 條 人民有秘密通訊之自由。

第 22 條 凡人民之其他自由及權利，不妨害社會秩序公共利益者，均受憲法之保障。

第 23 條 以上各條列舉之自由權利，除為防止妨礙他人自由、避免緊急危難、維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。

- 隱私權乃為不可或缺之基本權利，應受憲法保障。

## 第二十八章 妨害秘密罪

第 315 條 無故開拆或隱匿他人之封緘信函、文書或圖畫者，處拘役或九千元以下罰金。無故以開拆以外之方法，窺視其內容者，亦同。

第 315-1 條 有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：

一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。

二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。

第 315-2 條 1 意圖營利供給場所、工具或設備，便利他人為前條之行為者，處五年以下有期徒刑、拘役或科或併科五十萬元以下罰金。

2 意圖散布、播送、販賣而有前條第二款之行為者，亦同。

3 製造、散布、播送或販賣前二項或前條第二款竊錄之內容者，依第一項之規定處斷。

4 前三項之未遂犯罰之。

- 規範的是個資，不是隱私。

- 隱私(興趣、嗜好、上網紀錄、購物紀錄、定位軌跡、裝置識別碼、IP位址等)

- 無法請求停止蒐集、處理、利用與刪除隱私。

第 2 條

本法用詞，定義如下：

- 一、個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
- 二、個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
- 三、蒐集：指以任何方式取得個人資料。
- 四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
- 五、利用：指將蒐集之個人資料為處理以外之使用。
- 六、國際傳輸：指將個人資料作跨國（境）之處理或利用。
- 七、公務機關：指依法行使公權力之中央或地方機關或行政法人。
- 八、非公務機關：指前款以外之自然人、法人或其他團體。
- 九、當事人：指個人資料之本人。

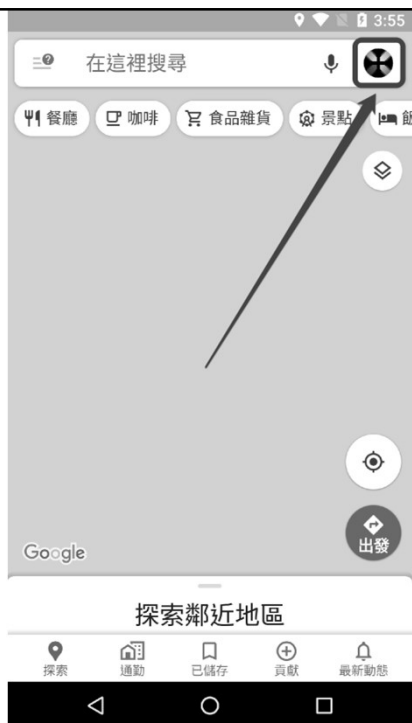
第 3 條

當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

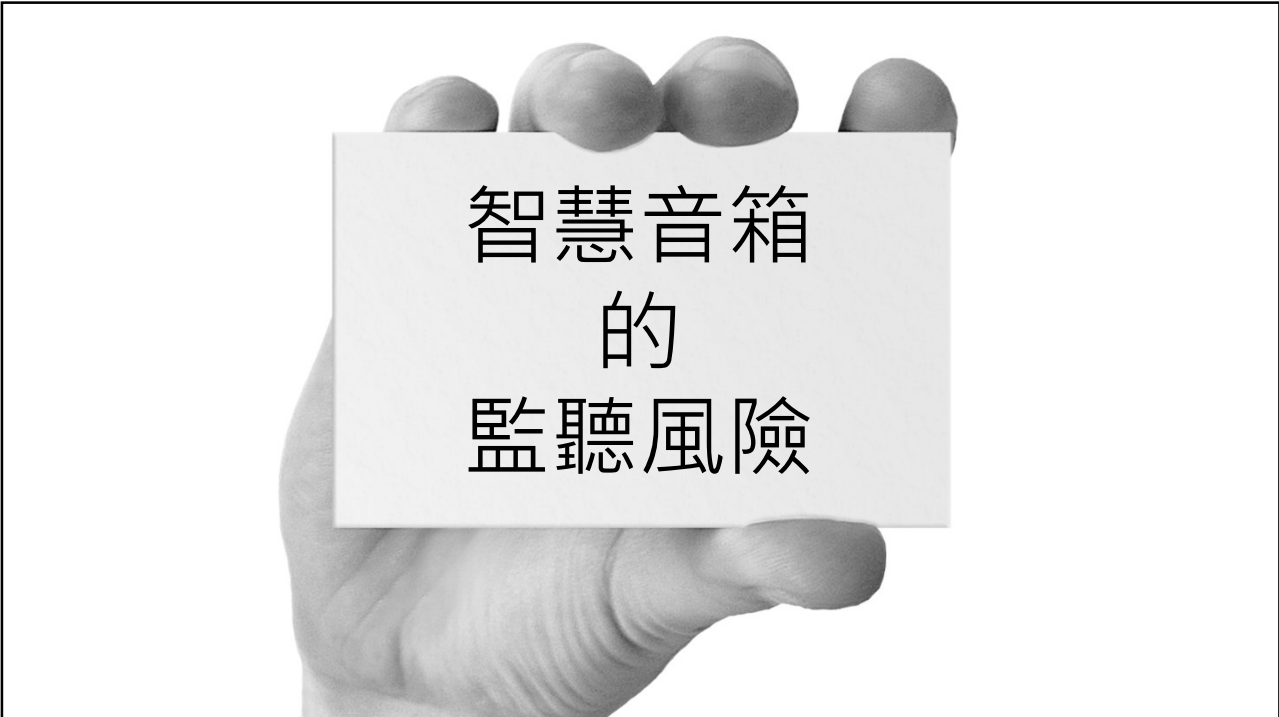
- 一、查詢或請求閱覽。
- 二、請求製給複製本。
- 三、請求補充或更正。
- 四、請求停止蒐集、處理或利用。
- 五、請求刪除。

## 隱私與個資的新風險： 網路蒐集哪些隱私與個資？ (以 Google 為例)

# 定位紀錄 的隱私







# 智慧音箱 的 監聽風險

## 查看及管理搜尋活動

啟用「[網路和應用程式活動](#)」之後，您在其他 Google 服務上的搜尋和活動都會儲存至 Google 帳戶。如此一來，系統就能提供您更符合需求的搜尋結果和建議。

您可以自行決定要儲存的內容，也可以隨時刪除搜尋記錄和活動，或是停用「[網路和應用程式活動](#)」服務。

注意：如果您的 Google 帳戶是由公司或學校提供，可能需要請管理員為貴機構開啟「[網路和應用程式活動](#)」服務。

[電腦](#)   [Android 裝置](#)   [iPhone 和 iPad](#)

## 開啟或關閉網路和應用程式活動

1. 在電腦上前往[活動控制項](#) [頁面](#)。系統可能會要求您登入 Google 帳戶。
2. 開啟或關閉「[網路和應用程式活動](#)」。
3. 將切換按鈕設為開啟後，您可以視需要勾選 [納入 Chrome 瀏覽紀錄以及您在採用 Google 服務的網站和應用程式中的活動] 旁的核取方塊。

注意：在某些瀏覽器和裝置中，可能還有其他設定會影響這類活動的儲存方式。

## 查看或刪除搜尋活動

您可以前往我的活動 [網頁](#) 查看及刪除自己的搜尋記錄和瀏覽活動。進一步瞭解如何查看及管理帳戶活動，或是如何刪除搜尋記錄和活動。

https://myactivity.google.com



## 管理 Google 語音和音訊記錄

您可以允許 Google 儲存語音和其他音訊記錄，讓 Google 各項服務為您提供個人化體驗，以及改善語音技術，使人人受惠。

**重要注意事項：**根據其他設定，語音和音訊記錄可能會儲存在其他位置。

### 語音和音訊記錄中儲存的内容

當您透過下列方法啟動語音服務時，Google 會將您的語音和音訊內容錄下，並在前面加上幾秒空白：

- 說出啟動指令，例如「Hey Google」。
- 輕觸「麥克風」圖示。

### 系統可能會儲存語音和音訊記錄的其他位置

「語音和音訊記錄」設定不會影響用來儲存語音和音訊資訊的其他 Google 服務 (例如 Google Voice 或 YouTube)。

視其他裝置設定而定，這些語音和音訊記錄仍可能會儲存在您的裝置上。系統也可能會將語音模型改善內容傳送給 Google，但不會上傳您的語音和音訊記錄。舉例來說，如果「協助改善 Gboard」設定為開啟狀態，Gboard 可改善文字建議來造福所有使用者，但不會將您的語音記錄傳送到伺服器。瞭解 Gboard 如何更臻完善。



## 隱私與個資的新風險： 蒐集的隱私與個資外洩 被詐騙集團利用



https://policies.google.com/privacy



隱私權政策

當您開始使用 Google 服務，即表示您信賴我們對您個人資訊的處理方式。我們深知這份責任重大，因此會盡力保護您的資訊，並為您提供相關的管理功能。

本《隱私權政策》旨在協助您瞭解 Google 收集的資訊類型以及收集這些資訊的原因，也說明了您可以如何更新、管理、匯出與刪除資訊。

隱私權政策

- 簡介
- Google 收集的資訊
- Google 收集資料的原因
- 您的隱私權控制項
- 分享您的資訊
- 捍衛資安
- 匯出及刪除您的資訊
- 保留您的資訊



3:40 隱私權政策

我們收集的資訊包括唯一識別碼、瀏覽器類型和設定、裝置類型和設定、作業系統、行動網路資訊 (包括電信業者名稱和電話號碼)，以及應用程式版本編號。此外，我們也會針對您的應用程式、瀏覽器和裝置與 Google 服務的互動收集相關資訊，包括 IP 位址、當機報告、系統活動，以及您提出要求的日期、時間和參照網址。

如果您裝置上的 Google 服務與我們的伺服器連線 (例如當您從 Play 商店安裝應用程式，或是當該服務自動檢查更新時)，我們便會蒐集這類資訊。要是您使用的是安裝了 Google 應用程式的 Android 裝置，您的裝置會定期與 Google 伺服器連線，將有關裝置本身以及您與 Google 服務連線情形的資訊提供給 Google。這類資訊包括您的裝置類型和電信業者名稱、當機報告、您已安裝的應用程式，以及 Android 使用情形的其他資訊 (視您的裝置設定)。

3:40 隱私權政策

我們會收集您使用 Google 服務時進行的活動相關資訊，以便向您推薦您可能會喜歡的 YouTube 影片或提供類似功能。我們收集的活動資訊可能包括：

- 您搜尋的字詞
- 您觀看的影片
- 內容和廣告的瀏覽次數與互動次數
- 語音和音訊資訊
- 交易活動
- 您交流或分享內容的對象
- 在採用 Google 服務的第三方網站和應用程式中的活動
- 您同步到 Google 帳戶的 Chrome 記錄

3:44 隱私權政策

### Google 帳戶中刪除

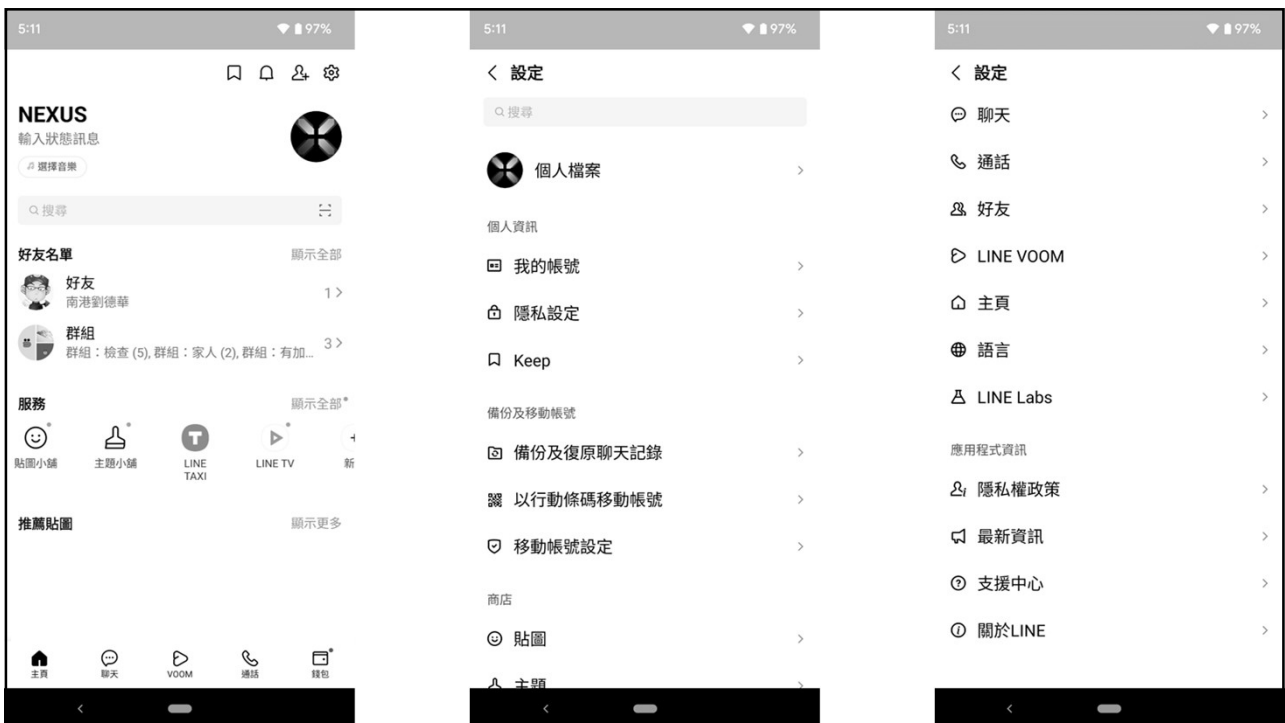
您可以匯出 Google 帳戶中的內容副本，做為備份資料或用於 Google 以外的第三方服務。

匯出資料

如要刪除您的資訊，您可以：

- 將您的內容從特定 Google 服務中刪除
- 使用我的活動搜尋您帳戶中的特定項目，然後予以刪除
- 刪除特定 Google 產品，包括與這些產品相關的資訊
- 刪除整個 Google 帳戶

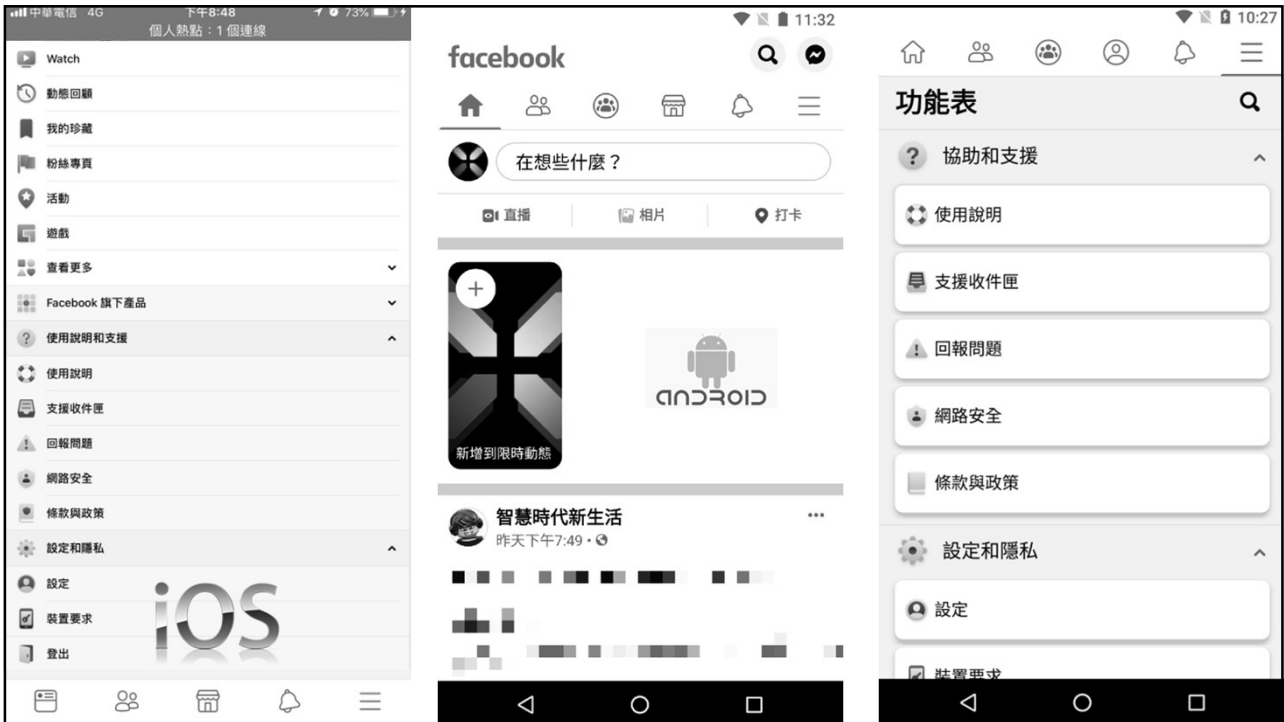
# LY 公司 (LINE) 隱私權政策





## LINE會從第三方蒐集個人資料嗎？

- 會從第三方收受個人資料。
- 在這些資訊中，有些個人資料來自提供特定服務的合作夥伴，有些來自使用官方帳號、將您的個人資料與該等服務連結，並將其分享給該第三方。
- LINE如何使用我的資訊？
- 用於核實您的身份；
  - 監控、發現並制止未經授權使用服務、不正當獲取服務或濫用服務等行為；
  - 為確認您的身分並於您的帳號遭未經授權使用時通知您；
- 為實現個人化或提供廣告：
  - 為提供與我們服務相關、或與我們的關係企業相關等資訊、或LINE以外企業的廣告商的廣告資訊。
  - 為改善及/或優化服務及任何額外服務相關的資訊；及
  - 用於評估我們刊登在網際網路或其他媒體上廣告的效果。
- 來源：(LINE隱私權政策)
- [http://terms.line.me/line\\_rules/?lang=zh-hant](http://terms.line.me/line_rules/?lang=zh-hant)





## 二、資料之蒐集：

我們蒐集您的個人資料，係為確認您在我們網站/APP、門市或客服專線之使用者身分，及為您提供各項服務之用，其範圍如下：



中華電信 遠傳心... 台灣大...

(一). 我們在您使用我們網站/APP、加入會員、申辦各項電信服務、線上購物、瀏覽網頁、參加宣傳活動或贈獎遊戲、訂閱電子報、訂購我們產品/服務時，依實際情況，將會請您提供您的個人相關資料，包括但不限於姓名、身分證字號、行動電話門號、電子郵件地址、出生日期、性別、地址...等。

(二). 我們會保留您所提供的上述資料，也會保留您上網瀏覽或查詢時，在系統上產生的相關紀錄，包括IP位址、使用時間、瀏覽器、Cookie中的資料、瀏覽及點選紀錄、通信紀錄、位置與帳單資訊、使用紀錄等資料。



中華電信



遠傳



台灣大哥大



全聯



全支付



蝦皮購物

抖音



LINE Pay

小紅書



街口支付

Netflix



- 問題就出自於大家最常用的 Google、Youtube、Facebook、Instagram、LINE 服務，才會導致多數人誤以為是 iPhone 遭竊聽，當然 Android 也同樣會有此問題，主因還是出自於 Google 和 Facebook 等在背後紀錄你的對話和分析你的行為。

- iPhone 避免被 Facebook、Google 竊聽方法：

1. 關閉 FB、IG、Youtube、LINE 麥克風與定位。
2. 限制 Siri 與搜尋功能。
3. 刪除伺服器上的 Siri 聽寫紀錄。
4. 關閉 APP 追蹤。
5. 刪除伺服器 Siri 聽寫紀錄。
6. 加強 LINE 隱私與關閉個人化廣告。
7. 關閉 Facebook 追蹤站外瀏覽。
8. 關閉或刪除 Google 活動紀錄。



- 引用來源：

- <https://mrmad.com.tw/iphone-eavesdropping-conversation>

## 隱私與個資的新風險： 如何調整隱私與個資 防止被廣告騷擾

## 寫在前面

- 截至目前為止。
- Google、LINE、FB、IG 的廣告是**無法完全取消**，但可以調整廣告顯示內容。
- 部分廣告功能可以關閉，但效果不彰。
- 目前使用者僅只能透過**檢舉廣告**這個機制，讓同一則廣告不再顯示。
- (備註：但相同廠商所投放的不同廣告，還是會出現。)

<https://myadcenter.google.com/>





## 控制系統向您顯示的廣告

您可以控制系統為您顯示更實用的廣告，或顯示為您量身打造的廣告。您會在以下位置看到 Google 廣告：

- Google 服務，例如 [Google 搜尋](#)或 [YouTube](#)。
- 與 Google 合作刊登廣告的網站和應用程式。

### 廣告設定的運作方式

每個 Google 帳戶的廣告設定不盡相同。如果您有多個帳戶，每個帳戶都會有專屬的廣告設定。系統會在您登入 Google 帳戶時儲存您的廣告設定。

當您登入 Google 帳戶後，系統會根據您 Google 帳戶中的活動和資訊向您顯示個人化廣告。您可以前往我的活動 [查看及編輯您的活動](#)。

如果您並未登入 Google 帳戶，系統會將您的廣告設定儲存到您的裝置或瀏覽器。當您清除瀏覽器的 Cookie、取得新裝置或重設廣告 ID 時，系統就不會儲存您的廣告設定。

## 有爭議的第三方 Youtube APP

由於使用第三方 Youtube APP 是**侵權行為**，Google 已控告這些開發團隊並提出停止散佈與開發的法律文件，並呼籲使用者不要使用，以免 Google 帳號因**違規被停權**封鎖使用。

- iOS :
  - YouListen
- Android :
  - YouTube Vanced (已停止更新與下載)
  - SkyTube
  - Tube Browser Pro
  - YouListen



Vanced has been discontinued. In the coming days, the download links on the website will be taken down. We know this is not something you wanted to hear but it's something we need to do. Thank you all for supporting us over the years.

翻譯原文

上午12:55 · 2022年3月14日 · TweetDeck

	YouTube Premium	YouTube Music Premium
Android iOS	月繳 NT\$ 199 (個人) NT\$ 260 (個人)	NT\$ 169 (個人) NT\$ 220 (個人)
<b>蘋果 App Store 額外抽成</b>		
零廣告的音樂體驗	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
背景播放	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
下載內容	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>YouTube</b>		
沒有廣告	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
背景播放	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
下載內容	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

訂閱 YouTube Premi...

## YouTube Premium

零廣告的 YouTube 和 YouTube Music

**免費試用**

免費試用 1 個月，之後每月只要 \$179.00  
週期性付款，隨時皆可取消

你也可以選擇家庭方案或學生方案，輕鬆省更多

本方案有特定的限制和規定，請按這裡瞭解詳情。

**零廣告與背景播放**  
享受零廣告干擾的觀影體驗，就算使用其他應用程式或鎖定螢幕時也能繼續收看。

**下載內容**

首頁 發燒影片 訂閱內容 收件匣 媒體庫

**LINE 廣告  
(廣告設定)**

## 為什麼 LINE 有一大堆廣告？ 如何知道我的喜好？

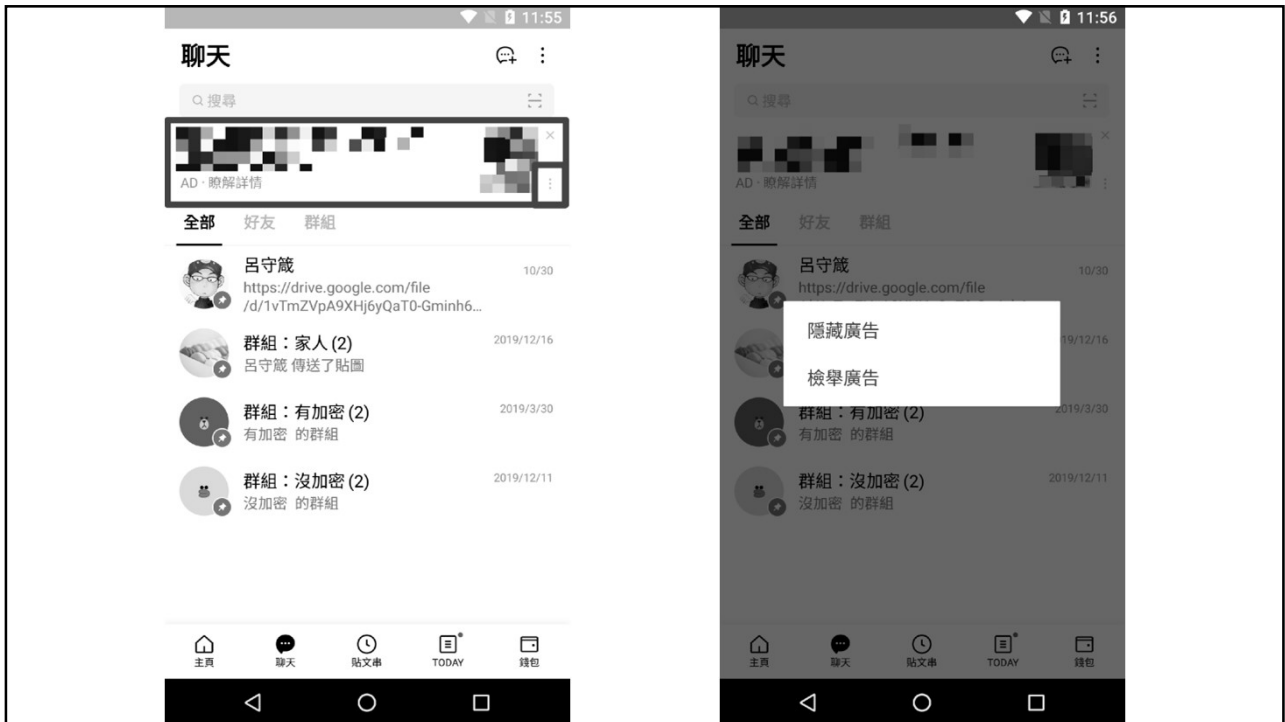
- LINE 使用 Cookies 或其他類似技術追蹤使用者喜好。
- 我們將基於以下目的使用Cookies：
  - 協助我們在您使用服務和（或）所有額外服務時維護您的使用；
  - 提高我們系統的安全性；
  - 儲存您偏好的相關資訊及向您提供自訂服務；以及
  - 幫助我們瞭解用戶使用服務的情況並提高服務品質。
- 我們還在網站中使用下列協力廠商的Cookies：
- Google Analytics
- 來源：
- [http://terms.line.me/line\\_rules/?lang=zh-hant](http://terms.line.me/line_rules/?lang=zh-hant)











# FB & IG 廣告設定







境外敵對勢力介入我總統大選 國人宜謹慎識別網路假訊息



發布日期 112-12-20 14:49:36 更新日期 112-12-20 14:58:14 公共事務室

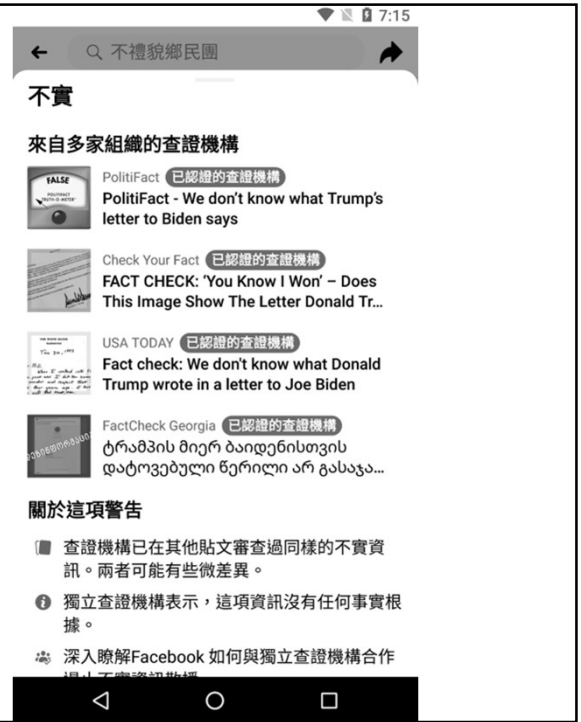
調查局資安工作站監控境外勢力網路水軍集團，112年12月18日發現Youtube「不要打仗要吃飯」帳號、臉書「不打烊便利店」粉絲專頁、「吳o瑩」等帳號頁面發布深偽AI手法製作之影片搭配聳動標題「網傳賴清德有三名情婦，堪稱政界李宗瑞」，又以人頭帳號於Youtube、臉書貼文下方留言，且留言數量均為8則、留言內容均相同，研判係自動化系統操作手法。

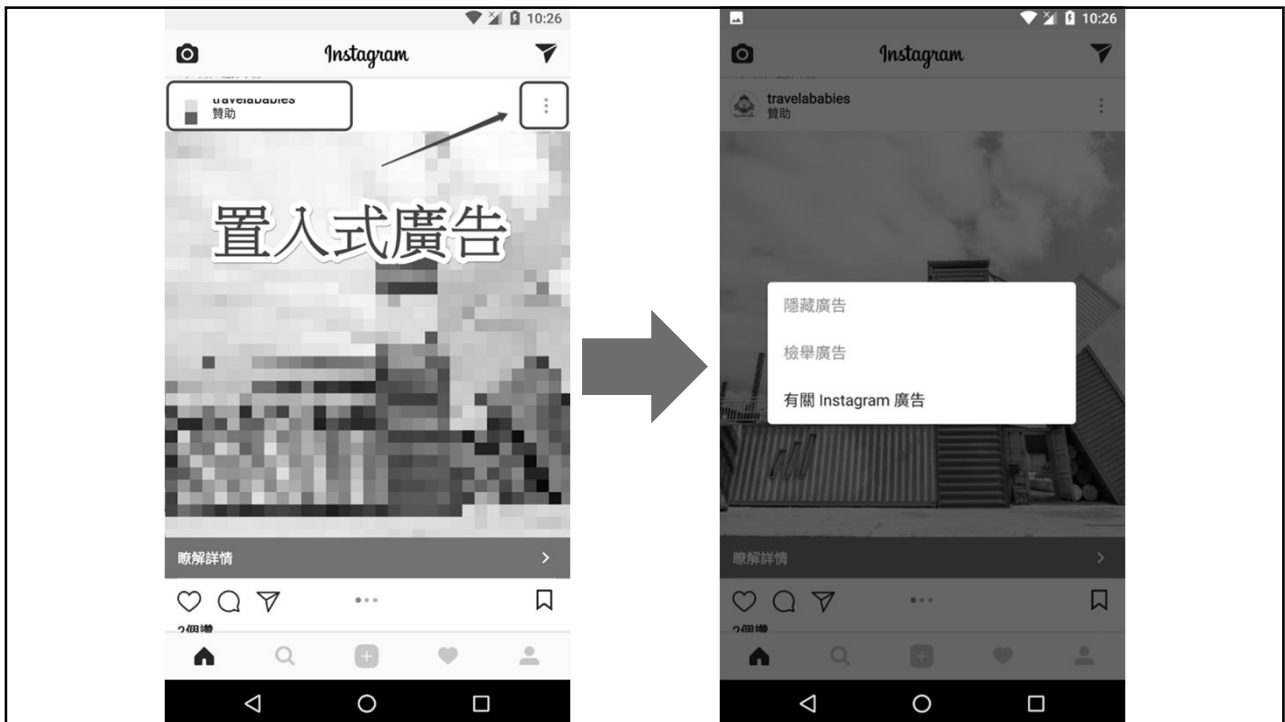


調查局資安工作站監控境外勢力網路水軍集團，112年12月18日發現Youtube「不要打仗要吃飯」帳號、臉書「不打烊便利店」粉絲專頁、「吳o瑩」等帳號頁面發布深偽AI手法製作之影片搭配聳動標題「網傳賴清德有三名情婦，堪稱政界李宗瑞」，又以人頭帳號於Youtube、臉書貼文下方留言，且留言數量均為8則、留言內容均相同，研判係自動化系統操作手法。調查局資安工作站監控境外勢力網路水軍集團，112年12月18日發現Youtube「不要打仗要吃飯」帳號、臉書「不打烊便利店」粉絲專頁、「吳o瑩」等帳號頁面發布深偽AI手法製作之影片搭配聳動標題「網傳賴清德有三名情婦，堪稱政界李宗瑞」，又以人頭帳號於Youtube、臉書貼文下方留言，且留言數量均為8則、留言內容均相同，研判係自動化系統操作手法。

該手法與調查局往年偵辦之「茯苓有點兒甜等臉書粉絲專頁認知作戰案」、「Diss纏綿等臉書粉絲專頁認知作戰案」相同，均是透過如柬埔寨、緬甸等境外人士管理之臉書「柴犬大大」及「不打烊便利店」等粉絲專頁，先後針對我國九合一及二合一選舉相關議題及輿論進行多層次散布與操作，如112年11月間針對總統候選人賴清德操弄「200億元醫療戰備」、「把臺灣變成下一個戰場」相關爭議訊息，散布架構及手法如下：

- 一、創建無法識別真實身分及國籍之臉書或推特「吳o瑩」、「顧o瑩」、「廖o瑋」共計40個以上人頭帳號，發布爭議或不實訊息貼文。
- 二、由境外勢力控制之臉書「柴犬大大」及「不打烊便利店」等20個以上粉絲專頁進行散布。
- 三、透過大量人頭帳號進行點讚、留言、分享，以營造聲量並散布至80個以上我國臉書社群涵蓋生活、娛樂、地方、宗教等不同類型之社群。
- 四、國人誤信再轉傳、分享至個人頁面或其他社群，造成擴散。





## 結論

- 近期資安案例探討：
  - 個資外洩與詐騙手法
  - 利用 AI 進行深偽技術 (Deepfake) 詐騙
  
- 隱私與個資的新風險：
  - 網路蒐集哪些隱私與個資？
  - 蒐集的隱私與個資外洩，被詐騙集團利用
  - 如何調整隱私與個資，防止被廣告騷擾

## 參考資料 教學影片



智慧時代新生活 YouTube 頻道：  
[youtube.com/OpenBlueSmartLife](https://www.youtube.com/OpenBlueSmartLife)

智慧時代新生活 FB 粉絲頁：  
[facebook.com/SmartEraNewLife](https://www.facebook.com/SmartEraNewLife)