林業及自然保育署
臺東分署

公務機密
資訊安全維護

國家安全的守門員

反情報！ So Easy

反情報懶人包～1分鐘了解

六大守則

- 可疑人士要追查
- 機密公文要收好
- 機敏資訊不透露
- 非管事項不探詢
- 涉陸背景要留意
- 招待旅遊要當心

最高500萬元檢舉敵諜獎金

海洋委員會海巡署
Coast Guard Administration, Ocean Affairs Council

檢舉可疑 02-82300397
通報專線 02-22399241

目錄

資安時事案例

韓國酷澎大規模個資外流　引發釣魚詐騙等二次受害

（中央社檔案照片）

2025/12/11 11:26（12/11 11:47 更新）

（中央社首爾11日綜合外電報導）韓國酷澎近期爆發大規模個資外流事件，警方今天進入第3天搜查扣押，盼追查涉嫌外洩個資的中國籍前員工行蹤；這次事件也引發多起二次受害，近10天釣魚詐騙報案已達229件。

韓國警方自9日開始針對酷澎（Coupang）3370萬名顧客個資外流事件展開強制調查。根據韓聯社今天報導，今天進入連續第3天的搜查扣押，上午9時40分起重新展開扣押行動。

首爾警察廳網路搜查科表示，由於酷澎所持有的數位資料量極為龐大，因此預計蒐集相關資料將耗費相當長的時間。

警方指出，將會根據取得的資料追查涉嫌外洩個資的中國籍前員工行蹤，同時也會調查酷澎內部管理系統是否存在技術性漏洞。

此外，在酷澎發生大規模個資外流事件之後，國會科學技術資訊放送通信委員會所屬的共同民主黨議員李政憲表示，自上個月30日至這個月9日的10天內，共發生229件與酷澎個資外洩有關的釣魚詐騙案件。

主要報案類型包括冒充酷澎聯絡受害者，謊稱提供補償金進行詐騙，或是假冒物流配送通知進行詐騙。另外還有常見詐騙手法包括謊稱入選酷澎評價體驗團、活動得獎等。

李政憲表示，「因酷澎事故引發的釣魚犯罪等二次受害令人非常憂心」。他強調，在酷澎的資訊不透明公開、選擇躲避責任的情況下，酷澎與金範錫（創辦人暨執行長）應深刻反省，並盡快提出受害者補償方案。（編譯：楊啟芳）1141211

資安時事案例

國安局示警：5款大陸AI模型藏資安風險 勿下載DeepSeek

2025-11-17 01:16 聯合報／ 記者程嘉文、馬瑞璿、陳宥菘／台北報導

兩岸資安角力，國安局昨發布新聞稿表示，測試五款中國大陸開發的「生成式人工智慧（ＡＩ）語言模型」，包括DeepSeek、豆包、文心一言、通義千問、騰訊元寶，發現普遍存在資安風險與內容偏頗等問題。國安局建議國人提高警覺，避免下載具資安疑慮的中製應用程式，保護個人隱私及企業資訊。

公務機關已全面禁用

數發部、陸委會昨指出，基於資安考量，行政院已明文規定公務機關不得使用大陸廠牌資通訊產品（含軟體、硬體或服務），公務機關目前已全面禁用DeepSeek等ＡＩ服務，包含雲端服務、App及地端下載等方式。數發部建議，民眾應慎選App來源，定期檢查權限設定，避免自身隱私資料洩漏造成不必要風險，也防止個資遭不當利用。

國安局蒐研各國資安報告及情資，並協調統合調查局、刑事警察局等單位進行抽測。國安局指出，在應用程式部分採用數發部的基本資安檢測基準，針對「過度蒐集個資」、「逾越使用權限」、「數據回傳與分享」、「擷取系統資訊」及「掌握生物特徵」執行分析，發現五款程式均存在要求位置資訊、蒐集截圖、強迫同意不合理隱私條款，以及蒐集設備參數等問題。「通義千問」在十五項指標中有十一項違規、「豆包」與「騰訊元寶」十項違規、「文心一言」九項、「DeepSeek」八項。

「兩岸議題偏向中共」

在生成內容部分，依我國「ＡＩ產品與系統評測中心」公告十項評鑑類別，結果顯示五款軟體所生成內容，出現嚴重偏頗與不實資訊，包括在兩岸、南海、國際爭端等議題或針對台灣歷史、文化、政治時，均採取中共官方立場，如「台灣目前由中國中央政府管轄」、「台灣地區不存在所謂國家領導人」、「強調中國社會主義特色」、「台灣不是一個國家」、「台灣是中國領土不可分割的一部分」、「中國台灣」等。特定關鍵字彙則遭排除，如「民主」、「自由」、「人權」、「六四天安門事件」等。

評鑑也指出，這些語言模型可輕易生成抹黑他人、散播謠言的高煽動性內容。在特定情況下，可生成網路攻擊指令及利用程式碼漏洞，增加網路安全管理風險。

國安局表示，目前美、德、義、荷等國已對特定中國大陸製生成式ＡＩ語言模型發出警告，甚至禁用、下架。主要在於其可識別使用者身分，透過蒐集對話等功能，將使用者個資回傳至伺服器，甚至依中共「國家情報法」、「網路安全法」等規定，提供其政府運用。

個人資料保護法

公投連署帶動自然人憑證申辦潮
內政部：防詐勿外借

（中央社檔案照片）

2025/12/14 21:08（中央社記者高華謙台北14日電）公投電子連署熱潮帶動自然人憑證申請數暴增。內政部提醒，自然人憑證限本人使用，應謹記「憑證不外借，密碼不透露」，若出借給他人，帳戶可能成人頭帳戶，也要承擔個資外洩、財產損失，甚至法律責任。

自然人憑證以非對稱加密原理來保護資料機密性，經由憑證即可進行數位簽章及身分識別，且加密資料即使被攔截也無法輕易解開。因此，辦理自然人憑證就能透過線上處理報稅、申辦良民證、銀行開戶、有條件線上申請辦護照等多項政府服務，不必事事臨櫃辦理。

相較實體自然人憑證IC卡須以讀卡機操作，內政部也推動「行動自然人憑證」，使民眾無須再攜帶實體卡或讀卡機，只要下載APP即可隨時隨地完成身分識別及數位簽章。

內政部統計，截至12月10日，實體自然人憑證有效數達347萬餘張，行動自然人憑證有效數為71萬餘張。全台已有超過1400個應用系統介接，採用自然人憑證相關服務。

針對辦理方式，內政部指出，只要年滿18歲、未受監護宣告且設籍中華民國的國民，就可以攜帶身分證、Email信箱，至任一戶政事務所申辦櫃檯辦理。臨櫃申辦實體自然人憑證，費用為新台幣250元；臨櫃申辦行動自然人憑證費用為30元，但若臨櫃合併申辦實體及行動自然人憑證，費用為250元。

內政部說，民眾如已取得實體自然人憑證，但日後有行動自然人憑證需求時，無須回到戶所，可自行下載行動自然人憑證APP，透過手機NFC功能讀取實體自然人憑證，完成申請。

針對為何要設定使用期限，內政部表示，按內政部憑證實務作業基準（CPS）規定，私密金鑰使用期限10年到期必須更換金鑰，考量資訊安全並降低憑證遭盜用或破解風險，以及民眾更換行動裝置等因素，實體自然人憑證有效期為5年，到期可延展1次3年，共計8年效期。

至於行動自然人憑證，有效期限為1年，不過在裝置、憑證正常且有完成展期情況下，最長可使用8年；但如果忘記在時效內展期，行動自然人憑證須重新申辦。

內政部提醒，自然人憑證是個人專屬數位簽章工具，只限本人使用。若隨意出借，等同把身分授權給別人，不僅帳戶可能變成人頭帳戶，也要承擔個資外洩、財產損失，甚至法律責任。

內政部說，詐騙集團會謊稱代辦業務、協助驗證等，誘騙民眾交出晶片卡或PIN碼。但無論任何理由，都應記得「憑證不外借，密碼不透露」，也應妥善保管綁定行動自然人憑證的行動裝置，否則後續恐導致個資外洩或遭冒用，而蒙受不必要的法律責任及財產損失。（編輯：楊凱翔、林克倫）1141214

每月一常識

新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

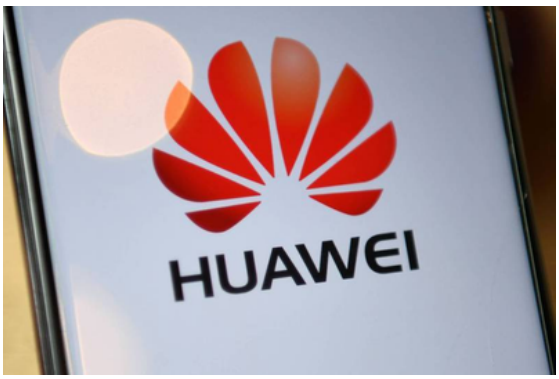
Q21 什麼情況下可不必事先告知當事人？

A 有下列情況之一，可以不必告知當事人：

1.依法律規定得免告知。
2.個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
3.告知將妨害公務機關執行法定職務。
4.告知將妨害第三人之重大利益。
5.當事人明知應告知之內容。

文/iThome

偷光你隱私2》不願手機螢幕被綁架 中國人裝成台灣人



（法新社）

自由時報〔記者高嘉和／台北報導〕近年來，中國不少科技網紅如「極客灣」、「小白測評」等，都曾針對中國品牌手機的垃圾廣告轟炸進行實測，結果都是「一台中國手機就是一台廣告播放器」、「您買了手機但螢幕不是您的」；網路討論區甚至教民眾怎麼避雷，最簡單方式就是將語言設定從簡體中文改為繁體中文，就會被判別是「海外用戶」，因收不到廣告費、就不會頻繁廣告轟炸，因為「中國人只欺負中國人」、「不想被收割就裝台灣人」。

手抖動一下 廣告直接跳轉

這些科技網紅實測發現，中國品牌手機為了彌補硬體利潤越來越薄，就將腦筋動到手機廣告，最令用戶崩潰的是「搖一搖」跳轉，就是打開一個App出現「開屏廣告」（Splash Ad）後，手機即啟動傳感器，只手抖動一下或走路晃一下，就會判定「點擊」廣告，直接強制跳轉到淘寶、京東或拼多多等購物軟體。

廣告轟炸不僅存在於第三方App，還埋在手機作業系統，例如查天氣時背景是借貸或保險廣告等；看個行事曆，螢幕到處塞滿促銷活動提醒；若安裝新App，系統會彈出檢查畫面，夾帶推薦一推其他App廣告。

還有關不掉的「偽裝按鈕」，例如虛假「X」號，結果不是關閉、而是跳轉下載，而真正關閉按鈕小到幾乎點不到，稍微點偏一點就進入廣告頁面。這些科技網紅實測發現，只要打開手機點個APP、打開想看的內容，至少要過五關斬六將、面對超過50個各類型廣告轟炸。

更令人不安的是隱私權限濫用，為了推播精準廣告，許多App會讀取用戶的剪貼簿、截圖、甚至錄音權限。

開車強制彈窗 影響行車安全

就算在影音串流平台花錢買VIP會員，仍需忍受各類「會員專屬設計廣告」、暫停廣告及浮動廣告，用戶體驗感極差；更有新能源車品牌在行駛啟動時強制彈窗廣告，不僅遮擋導航、甚至影響行車安全。

當你將語言改為繁中，算法會判定誤判為「海外華人」，這類人群通常不使用拼多多或特定的借貸軟體，因轉化率低，算法會減少對這類用戶的投放；但對於微信、抖音、微博、小紅書這些第三方App內部的廣告，效果依然有限，逼著用戶要花費很長時間，透過ADB工具（Android Debug Bridge）來強制刪除系統廣告組件，才能奪回自己的手機螢幕。