

公務 機密

密碼 123 盜用好簡單



資安時事案例

- ◎ 臉書個資遭盜用 專家：
心理測驗、占卜遊戲別亂點
- ◎ 想避免臉書隱私被侵害 KPM
G
建議做好「雙清」工作

個人資料保護法

輕鬆學資安

- ◎ Hotspot 熱點

數位學習

- ◎ 資安大叮嚀

臉書個資遭盜用

專家：心理測驗、占卜遊戲別亂點



聯合新聞網 107.30.20

劍橋分析（Cambridge Analytica）未經用戶允許便擷取臉書逾 5,000 萬名用戶的個資，使臉書遭受對個資處理不當的批評。對此，消基會副董事長、台科大資訊工程系副教授鄧惟中指出，應儘量少用臉書，因為一旦你的個資被盜用，不僅你上網的次數和從事的活動都曝光外，人際關係也都有可能受到波及，影響層面相當大且無遠弗屆。

鄧惟中特別提醒，尤其現在臉書上正流行的一些心理測驗、有趣的占卜遊戲，千萬都不要亂點，例如：2018 最能代表你的字、你最像什麼明星、你前輩子是什麼名人，其實那些文字都是亂掰，拍馬屁，讓你看起來心裡會很舒服的內容。要不要玩，可以自己決定，但只要玩了，就代表多一個人看到了你的個資。

鄧惟中指出，前年 11 月臉書雖已在使用頁面的右上角做了一些安全設定的導引，但並不是每一個使用者都會去認真去看並執行設定，再加上臉書每隔一段時間就會推出新的設定，若你未做更新，就會多了一個個資外洩的風險，若有一段時間沒有使用臉書了，也一定要記得先將帳號凍結，千萬不要放著不管。

鄧惟中表示，臉書的使用者條款落落長，許多人為了怕麻煩，多半都選同意，但若使用者不同意，臉書甚至還有但書「我們可以拒絕服務你」，因此使得使用者往往也只能同意，但試問有哪一條法律可以管得著你自己都同意的事？因此法律根本管不到。

為避免臉書個資遭盜用，鄧惟中指出，「隱私設定與工具」、「關閉定位服務」都是使用者可以加強留意的部分。



想避免臉書隱私被侵害

KPMG 建議做好「雙清」工作



鉅亨網記者許雅綿 台北 2018 年 3 月 22 日

臉書陷入個資外洩風暴，KPMG 數位安全服務負責人謝昀澤今（22）日指出，對臉書或社群工具的用戶，要保護自身個人隱私，至少要做到經常清理社群工具中 APP 連結，清理所使用瀏覽器的 cookie 瀏覽紀錄這兩件「雙清」的工作，才能避免成為下一個隱私被侵犯的受駭者。

謝昀澤指出，嚴格來說，此一事件並非傳統的駭客入侵竊取個資的傳統資安事故，而是社群網路服務因營業模式或協作廠商的管理疏失或不當利用，所導致的侵害用戶隱私事件。

他說，此類事件檢討的關鍵重點，並不在企業的防毒、防駭，而在這些新科技媒體產業，能否修正隱私保護的重大瑕疵與缺陷流程，並升級成能兼顧隱私保護的產品或服務。這項轉型是否能成功，也攸關臉書這樣的互聯網大帝國，能否持續壯大的關鍵因素。

謝昀澤表示，台灣科技產業，特別是大量對歐美進行出口的 IOT、或網通相關軟硬體廠商，對於相關風險應特別注意。近來各種商品與服務，如 IOT 玩具、智能穿戴型裝置等，未落實用戶隱私保護而遭裁罰的案件越來越多，產品遭停售者也時有所聞，KPMG 預測，在今年五月歐盟正式實施新版 GDPR（歐盟個資法後），全球相關訴訟案例或裁罰也將會激增。

過去廠商的做法常是以模糊的隱私權條款告知客戶，或增加一些資安控制手段，如資料加密等來保護用戶個資。KPMG 認為，參考世界最新隱私保護相關法規與規範，企業應該對新興科技的應用場域，無論是產品或服務，均須能落實隱私工程。

勤業眾信風險管理諮詢股份有限公司副總經理林彥良則認為，企業宜採取定期檢視隱私保護機制、落實委外安全管理、全面落實預設隱私保護三大因應措施，以落實數位時代的隱私與資安保護。

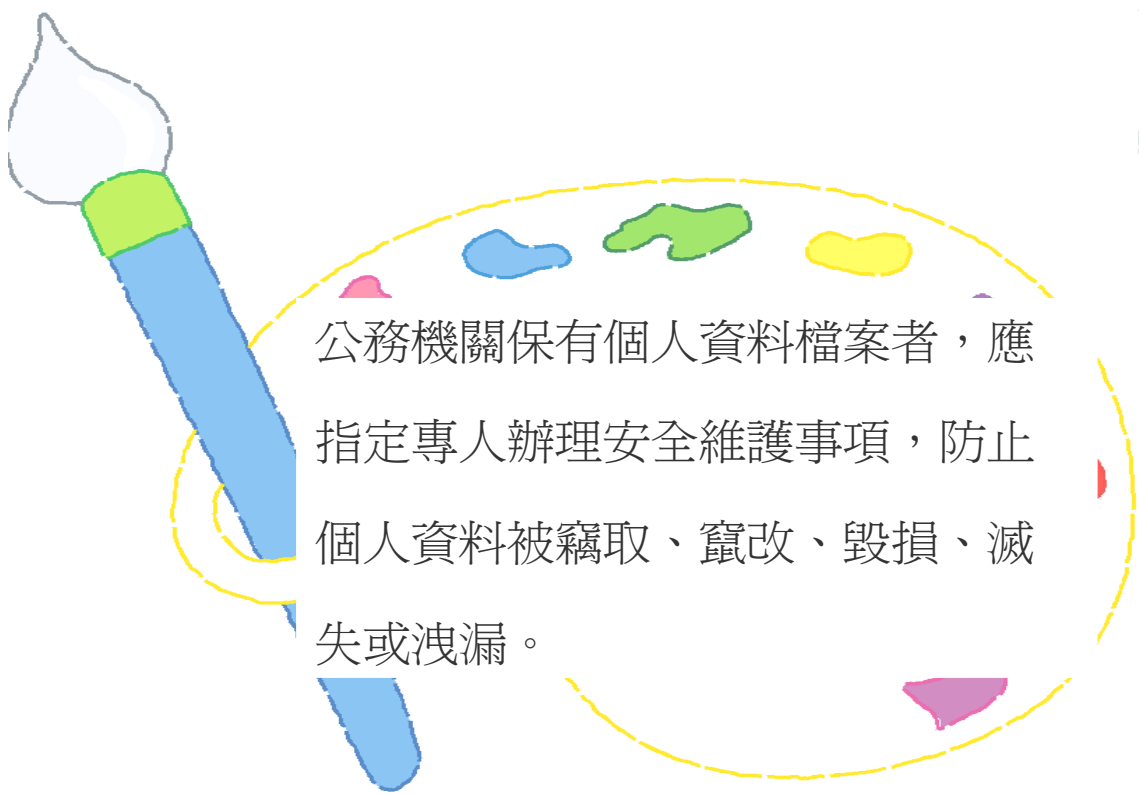
首先，企業應定期檢視隱私保護機制，包括：公開透明的告知與明確的同意，便捷的當事人權利行使、預設保護的隱私設定及落實當事人隱私設定，且應定期實施資料外洩應變演練等作業。

再者，企業應落實委外安全管理，包括：盡職調查、合約安全要求、資料安全管理、定期安全評估與現場實地稽核等。

最後，企業應全面落實預設隱私保護，將預設隱私嵌入業務營運流程，並定期或於業務流程、資訊系統發生重大變更時實施隱私衝擊評估，確保隱私保護機制持續有效。



第 18 條（公務機關個人資料檔案之安全維護）

A stylized illustration of a paintbrush with a blue handle and a green band, and a palette with a yellow dashed border containing several blobs of paint in blue, green, yellow, pink, and purple. The text is centered within the palette area.

公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

Hotspot 熱點



資料出處：[i-Security](#)

指在公共場所提供無線網路服務的地點
，使用者可以使用自己的筆記型電腦，
透過 **Hotspot** 的無線基地台上網。

