廉政園地

消費者保護
--遏止黃牛變賣演唱會門票 台業者可拒絕黃牛退票
公務機密維護宣導
--資料外洩危機吹向社群網站、觀光產業以及雲端儲存
機關安全維護宣導
--竊中要害 小心為上
廉政案例宣導
--查緝靠線民 躲緝靠交情

2019年3月號

消費者保護--黃牛變賣演唱會門票
台業者可拒絕黃牛退票

近年熱門演唱會的門票券常發生「黃牛」大量搶票 及高價轉售賺取價差的情況，衍伸不少消費糾紛，行政院 消費者保護處（消保處）促請文化部修法，增訂多元化的 藝文表演票券退、換處理機制，包括：業者可以拒絕黃牛 大量退票。 時下熱門演唱會如：江蕙封麥演唱會、「五月天」 跨年演唱會、張學友世界巡迴演唱會等門票開賣秒殺，沒 買到票的民眾只能轉由二手票券交易平台高價購票。表演 主辦單位也因為「黃牛」濫用現行退票機制導致營業損失 。 消保處促請主管機關文化部研擬「藝文表演票券定 型化契約應記載事項」修正草案，明定業者對於非供自用 ，購買票券而轉售圖利者，得拒絕辦理退(換)票等機制； 另外，增訂業者應依藝文表演的性質，可選擇4種退換票機制之一。

消保處表示，「黃牛」搶門票目的是為了高價轉售牟利， 但業者仍難避免「黃牛」大量退票。為協助業者防堵「黃 牛」大量搶(退)票，明定業者對於非供自用，購買票券而 轉售圖利者，可拒絕辦理退(換)票。 消保處表示，遏止「黃牛」濫用退票機制，同時明定業者應依藝文表演之性質，可以選擇4種退票方案。4種方案主 要差別在民眾退票時，會按照演出開演前的日期，業者收 取手續費的幅度。消保處表示，其中，業者可選擇若「演出當日至演出日前 第2日內辦理退(換)票者，業者得不予退、換票」等方案

公務機密維護宣導--資料外洩危機吹向社群網站、觀光產業以及雲端儲存

最近幾年的資料外洩事件頻傳，在2018年裡，不僅這類攻擊的次數極為頻繁，幾乎每個星期都會出現，而且，許多事件遭竊的資料數量都非常龐大。2018年列於規模前20大者就有4件，而且前3大攻擊所洩露的資料數量，都在1億筆以上，比起過往都要來得多。而這種現象，代表駭客想要將攻擊的效益最大化，在2019年應該會更加明顯。

不光是歐美出現災情，就連亞洲的國泰航空也在調查超過半年之後，對外公告有940萬旅客資料遭到未授權存取，於引起香港引進了不小的風波，許多客戶向媒體表示，曾向該航空用來購買機票的信用卡，遭到重覆盜刷。因此，不只是前述會出現規模更為嚴重的事件，攻擊目標也不再局限於資訊化程度較高的地區與產業類型。

事實上，2018年規模最大的2起攻擊，受害的分別是飯店業者與運動用品公司（Under Armour），其次才是社群網站Quora和MyHeritage，所以，2019年駭客下手的產業類別，應該也會延續這樣的趨勢。

不只駭客動手偷取資料的情況相當嚴重，同時，值得留意的是，由於企業對雲端服務的接受度，較以往增加，連帶因存取權限設置不當，導致儲存在雲端機敏資料，在無意中遭到公開，使得任意人士只要能找到路徑，就能取得上述檔案，這類事件在2018年出現也相當頻繁，而且，其中不乏大型的IT公司。

而較為值得慶幸的是，截至目前為止，被資安專家揭露的問題，大部分曝光的資料尚未遭到濫用，但這也代表駭客在未來的一年，可能會朝向找尋沒有妥善設置權限的機敏內容，做為日後犯案的工具。例如，得手後的使用者個人資料，駭客可以用在銀行帳戶或是電信門號的詐騙上。其中後者已經出現了冒充手機用戶（SIM-Swapping）的手法，透過向電信業者的客服要求補發新的SIM卡，或是修改使用者的個人資料，然後控制被害人的門號，再進一步發動攻擊，像是洗劫受害者的加密貨幣帳戶等。

以往駭客的攻擊目標，可能會優先朝政府單位與醫療機構下手，不過，近年來臉書的個資外洩事件，可說是不斷發生，像是2018年3月，劍橋（Cambridge Analytica）分析公司不當取得臉書5,000萬名用戶的資料，並暗中濫用來投放廣告等，隨後，這起事件陸續延燒，臉書執行長祖克柏更是親上火線，到美國國會進行說明。

另一起重大攻擊事件，則是在9月份，臉書網站出現網站功能的漏洞，這是結合了供使用者確認個人首頁的檢視角度（View）功能、祝賀朋友生日的影片上傳工具，以及維持用戶登入狀態的Token派送機制等。總計約有9,000萬名使用者受到影響。

就單一事件而言，臉書洩露的資料數量並非最多，但是2018一整年下來，外洩事件接連不斷發生，根據在Gemalto推出的2018上半年報告裡，社群網路洩露的個資數量就超過一半，達到25億筆，而光是臉書占了22億筆之多。這樣的情況，也導致整體遭駭資料筆數，較去年同期大幅增加為2.3倍。

至於其他類型的社群網站，在2018年也出現大規模的資料外洩事件，像是美國知識問答社群網站Quora，12月表示1億用戶個資遭駭，成為前述2018年洩露資料第3多的事件。其次是以色列的家譜網站MyHeritage，也在6月時外洩超過9,200萬名使用者個資。

在社群網站之外，與觀光產業有關的公司，像是飯店業者、航空公司、訂房與訂機票的網站等，2018年受到攻擊的情形也層出不窮，而且不乏洩露筆數相當龐大的事件，包含了近期才揭露的萬豪（Marriott）酒店集團資料外洩事件，約有5億筆資料受到未經許可的存取。

這起事件中，受害單位是萬豪酒店集團旗下的喜達屋（Starwood）飯店，他們美國地區的預約客戶資料庫於9月時，資料遭到未經授權存取，範圍遍及2014年至今的訂房客戶資料。這樣的資料外洩規模可說是第2大，僅次於雅虎遭駭30億筆資料的事件。

除了上述2種攻擊事件頻傳，另一種型態的資安風險，那就是企業將資料放上雲端之後，因為沒有將權限設置正確，導致公司的機敏內容，任何人都能取得。雖然這種事件多半在資安公司通知之後，資料的所有者就關閉相關存取權限，並未造成災情，不過，這樣的現象，也突顯企業潛藏了許多機密，可能因此曝光而不知情。而且，就連專門開發虛擬備份平臺的IT業界龍頭Veeam，也照樣中招。

資安研究員在2018年9月，無意間透過物聯網搜尋引擎Shodan，發現Veeam公開的MongoDB資料庫，而且，不需密碼就能存取。這套搜尋引擎在8月底時，把上述的資料庫納入索引，並於9日9日才關閉。這個資料庫總共存放4.45億筆的客戶資料，對於想要發送大量垃圾郵件的人，或是利用網路釣魚發動攻擊的駭客而言，簡直就是寶庫。

機關安全維護宣導—竊中要害　小心為上

壹、機關遭竊情形

先前發生於某縣市政府的竊盜案，竊賊在數月內先後光顧高雄、臺南、臺中、新竹、桃園及彰化等6個縣市政府，作案手法如出一轍，趁上班時間洽公民眾進出頻繁之際混入大樓內，先躲在樓梯間等隱蔽角落，待員工下班後，伺機至各樓層，發現若沒有員工在內加班，就逕行闖入，隨機打開或撬開抽屜 搜刮財物。蒙受損失的縣市政府員工大多求償無門，只能自認倒楣。

貳、預防方式

各機關仍應於必要範圍內，制訂「人員進出管制辦法」，對於機敏資料存放區、財產存放庫房、中央控制室、電腦機房、網路交換中心等，不分上下班時間， 皆應全面監控。除了由保全人員確實巡邏外，還要定期檢視監視錄影系統運作狀況，並維修保養及檢討拍攝角度及位置，強化設施安全功能，建立滴水不漏的維護措施。維護機關安全絕非少數人責任，必頇全體同仁齊心努力。

參、小叮嚀

維護機關安全乃全體員工共同責任，除應時時提高警覺，留意身邊可疑人、事、物並確實通報處理外，並應定期檢查各項安全維護設備，共同發揮整體力量，以期達到「防患於未然，弭禍於無形」的目標。

廉政案例宣導—查緝靠線民，躲緝靠交情

放水弟在警察局擔任警察，負責查緝非法外勞；因為工作關係而與人力仲介公司的多金妹熟識，時常請多金妹提供非法外勞藏匿地點的情報，進而查獲非法外勞、賺取績效。

某日，放水弟又要求多金妹提供非法外勞的情報，多金妹於是就將曾傻僱用非法外勞及工地宿舍等資訊，提供給放水弟；數日後，放水弟順利在宿舍查獲非法外勞並帶回警局。曾傻質疑多金妹洩漏消息給警察，多金妹連忙否認並告訴曾傻：「僱用非法外勞會被裁罰至少新臺幣（下同）15萬元罰鍰喔，如果不想被罰，我有認識的管道可以幫忙，但要先支付4萬元作為疏通費用。」曾傻無奈之下，只好給多金妹4 萬元作為協助的酬勞。

多金妹打電話給放水弟，請他用「查獲非法工作外勞」來處理就好，不要再追查有無非法僱用情事，放水弟顧念與多金妹的交情，就在筆錄上記載「無非法雇主」，僅將非法外勞移送有關單位，讓曾傻免於遭裁罰。

放水弟身為警察，當查獲到非法外勞時，應該深入追查有無雇主非法聘僱情形，並將非法雇主函請當地勞工主管機關處理。放水弟明知相關法令規定，卻未將曾傻函送裁罰，讓曾傻獲得免於受裁罰的不法利益。最後，放水弟被法院依貪污治罪條例第6條第1項第4款之圖利罪，判處有期徒刑5年4個月，褫奪公權3年。