政風室

法令宣導電子報

103/07

機密維護宣導
安全維護宣導
消費者保護宣導
反詐騙宣導
法務部廉政署多元檢舉管道

公務機密維護宣導

客戶資料安全管理

◎魯明德

知名拍賣網站 eBay 驚爆資料庫遭到非法入侵，且可能成為美國史上最大的資料外洩事件，據說是由駭客入侵，先竊取多名 eBay 員工的登入憑證以進入 eBay 的企業網路，再盜取 eBay 資料庫中儲存的客戶名稱、密碼、電子郵件帳號、住址、電話號碼及生日等。

科技新貴小潘看到這則新聞，馬上聯想到他的公司正在規劃從事 B2C 的電子商務，應該要事先預防駭客入侵造成資料外洩的事件發生，於是趁著端午節的師生下午茶約會，跟司馬特老師討論如何維護客戶資料安全的問題。

司馬特老師聽完小潘的問題，喝口咖啡，先從 eBay 的案例談起。eBay 的資料庫被盜模式，是由駭客先入侵系統，竊取員工的登入憑證後，再以合法的途徑進入資訊系統，進而盜取資料庫中的客戶資料。

分析該公司的系統規劃，顯然沒有採取 3-tier 的方式建置，駭客才能一下子就進入系統，盜取員工登入憑證，因此，未來在建置系統的規劃，除了要有防火牆、防毒軟體等軟體防護外，應該在硬體上考量採取 3-tier 的模式，讓外部使用者不能直接進到資料庫層。

其次，使用者登入系統的帳號、密碼，應該規劃以加密後的亂碼方式儲存在資料庫中；顯然，eBay 在這方面可能也沒有落實，否則駭客不會這麼容易在取得員工的登入憑證後，立即就能進入系統。

小潘聽完司馬特老師的分析後，馬上舉一反三地想到：電子商務中最重要的是金流，客戶的信用卡帳號應該如何保管才不會被盜？司馬特老師喝口咖啡，接著表示：電子商務的業者，最佳狀況是不要儲存客戶的信用卡資料。小潘聽完後一頭霧水，不儲存客戶的信用資料，怎麼確定信用狀況？將來怎麼收錢？

司馬特老師喝口咖啡，仍然笑著回應這個問題。現在雲端技術這麼發達，為什麼要把所有資料都放在自己家裏呢？信用卡資料應該從消費者端就要加密傳送，電子商務業者的系統也不需要解密，而是直接送給銀行確

認，以減少洩密風險；系統只要記下銀行確認後的授權碼即可，將來請款時再透過授權碼到雲端去核對信用卡號，就可以減少信用卡帳號在業者端洩密的風險。客戶資料的洩漏，還涉及《個人資料保護法》的問題，電子商務的業者要非常小心處理，除了在系統設計之初，就要把相關內、外部的防護作為列入規劃外，還要在作業面運用管理規章加以規範，以防杜人為疏失造成洩密的危安事件發生。

資訊安全不是只把網路及系統做好就可以，環境也是一個重要的危安因子，不可疏忽。機房管理也是影響資訊安全的重要因素，機房應有門禁管制作為，禁止非管理人員任意出入；若他人有必要進入機房，應有登記制度，記錄進出時間，並禁止攜帶資訊媒體（如行動碟、照相手機…等）進入，同時對於攜出物品也要詳加檢查，以杜絕洩密管道。合法的使用者往往是不易控管的洩密管道，因為他可以合法地接觸各種資料，因此，透過系統的管制也不易防範，系統的管理者就要藉由異常處理來加以防範。小潘聽到這裏，又有了疑問，什麼是異常處理呢？

司馬特老師喝了咖啡，繼續說道，在管理上，因為資源有限，所以管理者不可能鉅細靡遺，什麼事都管得到；這個時候，就要運用資訊系統的優勢，來做例外管理，利用電腦的特性，把異常狀況抓出來。

我們的系統每天都會記錄 log 檔，這個 log 檔就是可以用來做異常管理的工具，通常危安事件不會沒有任何徵兆，我們可以透過程式分析 log 檔找出異常。以本次 eBay 的客戶資料洩漏為例，據報導外洩資料有 1.4 億筆，這是很大量的資料，當入侵者或內部合法使用者在做這件事的時候，log 檔應會顯示大量的下載紀錄，系統管理者就應該要注意這種異常行為，強行介入系統加以排除。

小潘聽到這裏才發現，原來資訊安全不是只有防止系統的非法入侵，在管理面上也要交互運用，才能確保系統的安全。師生的下午茶就在華燈初上之際進入尾聲，小潘帶著滿滿的收穫又回到工作崗位！

（源自清流月刊）

安全維護宣導

防災須知－颱風洪水

（資料來源：內政部消防署網站）

消費者保護宣導

小心「APP」操作安全，確保荷包免被「A」！

隨著智慧型行動裝置應用的普及化，依據資策會研究報告約有 2/3 的智慧型手機持有者有下載應用程式(簡稱 App)的經驗，其中有「程式內購買(軟體內消費)」(簡稱 IAP)消費經驗的民眾裡，約 1/4 消費者每月消費金額平均超過 500 元。在業者以「免費」宣稱但其實內含許多看不見的花費誘惑、扣款流程的「方便、貼心」設計，不免也曝露出消費者可能陷入之非必要消費、非預期帳單等消費風險。

行政院消保處表示，目前市場上架 APP 可分為付費下載及免費下載兩部分，雖然多數消費者以下載免費 APP 為主，但在業者標榜「免費」的 APP 之下，其內部所隱藏的真正花費，常巧妙運用分階段顯示「現在購買」或「立即升級」等設計手法，誘惑、鼓勵消費者進行可能非必要或過度之消費；甚至對於費用支付作業採取預設自動扣款、未逐次要求密碼等低度控管方式，讓消費者在不經意間陷入高度風險的消費環境。

隨著 4G 行動科技時代來臨，APP 產業提供之服務內容必定更加豐富多變，行政院消保處也要再次提醒消費者：

一、下載 APP 前應先瞭解其服務內容是否包含付費項目，及購買價格等資訊，先行查閱 APP 平台業者之購物及付款等規定，並採取相對安全之管理措施。

二、建議可能將行動裝置提供給未成年兒童或少年使用之家長，審酌考量下載內含 IAP 項目之 APP 的必要性；購物時所輸入之信用卡資料及帳戶密碼更應避免自動儲存於該裝置設備上，以防造成兒女之不當使用。（本文轉載自行政院消費者保護會）

反詐騙宣導

「新門號幫我打打看會不會通？」小心打完自己變假賣家！

幫朋友打一通電話，結果自己變成網拍假賣家！？最近陸續有民眾接到朋友傳來的 LINE 訊息或簡訊，內容說自己剛辦了一支 0809 開頭的新門號，請您用手機幫他打打看會不會通，但其實這支號碼是某拍賣網站的申請帳號認證電話，只要一撥通就等於確認申請帳號，接著您的門號就可能被用來當成假賣家行騙！

國內某知名拍賣網站採用以門號申請帳號的認證措施，民眾申請帳號後必須填寫自己的門號，並且用這支門號撥打該拍賣網站的認證電話 0809031088 來確認留下的是真實門號，以杜絕假賣家橫行，方便交易糾紛發生後循線追查。沒想到詐騙集團也會隨機應變出新招，歹徒先用被害人的手機門號申請網拍帳號，再傳訊息給被害人：「0809031088 用手機打給我一下，新辦的，幫個忙打試試看能通嗎？」被害人一時不查照辦，就等於確認了自己手機申請了一個網拍帳號卻渾然不覺，等對方用這個帳號在網路上行騙，警方循線找上門，或是被買家追殺，才發現代誌大條，自己也成了詐騙集團的一份子！

刑事警察局呼籲，民眾接到朋友傳來的訊息，無論要您撥打電話或點選連結都務必要謹慎，可直接打給那位朋友求證；在拍賣網站上購物亦要仔細觀察賣家的評價，不要一看到心動的產品就立刻下標，因為假賣家通常行騙不到一週就會被其他網友檢舉而停權。此外，刑事局也持續要求各拍賣網站再加強防護機制，避免成為詐騙集團犯案的媒介。如有任何疑問歡迎撥打 165 反詐騙諮詢專線查詢。

（資料來源：內政部警政署網站 http://www.165.gov.tw/fraud.aspx?id=220）

勇敢吹哨

24小時廉政專線：0800-286-586

（0800-你爆料-我爆料）

其他多元檢舉管道：

傳真：02-2562-1156

郵政信箱：台北郵政 14-153 號信箱

電子郵件：gechief-p@mail.moj.gov.tw

親身舉報：臺北市中山區松江路 318 號 5 樓

廉能是政府的核心價值，貪腐足以摧毀政府的形象，公務員應堅持廉潔，拒絕貪腐。

潭子區公所政風室關心您