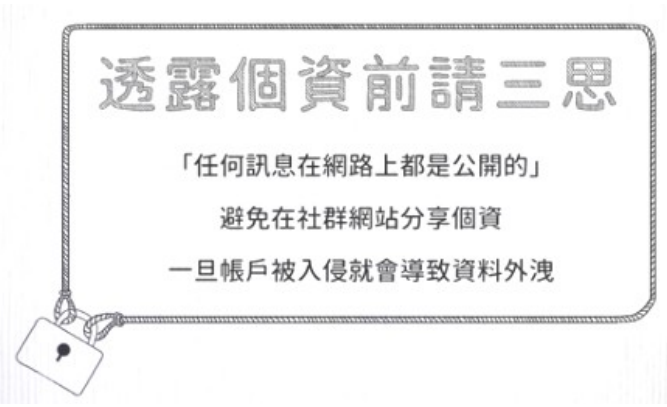
臺東林區管理處

中華民國 106 年_ 3 月號

資安不能靠運氣，個資防護最實際。



資安時事案例

史上最大宗！　6 券商集體遭駭客攻擊勒索

垃圾鴿臉書爆紅 資安專家 ：小心潛在危機

個人資料保護法

第 8 條

輕鬆學資安

Misfortune Cookie

數位學習

105 年資安動畫金像獎

資安Circle

史上最大宗！　6 券商集體遭駭客攻擊勒索

記者 相振爲 / 攝影 傅建誠 台北 報導　107.2.7

台灣券商業者遭到史上最大規模的駭客攻擊！行政院證實，有 6 家券商日前遭到境外駭客攻擊，下單網頁被癱瘓，而且對方勒所 10 比特幣，折合台幣約 30 萬元，否則會有更大規模攻擊，等同跟證券業開戰。行政院資安處已經介入，並且提高到國安層級防範。

電影《黑帽駭客》：「從連接網路的那一刻起你就沒有主導權，我可以攻擊任何人，任何事務、任何地方。」

電影《黑帽駭客》描述網路時代中，透過網路駭客就能輕易對金融等行業造成極大破壞，沒想到新春才剛開工，台灣就有多家券商遭到駭客攻擊。

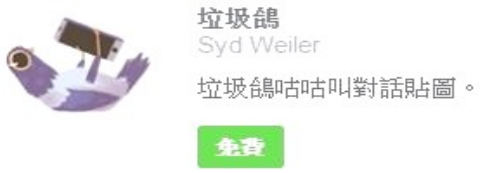
行政院資安處處長簡宏偉：「大概有 6 家券商有收到勒索信，勒索信裡面都有提到說，如果不支付一些費用，可能會做更嚴重的網路攻擊，來源是有一、兩個特定國家。」

據了解，被攻擊的券商包括元富、大展等 6 家，這 2 個境外駭客透過「分散式阻斷服務攻擊」，先癱瘓券商的下單網頁，揚言要求支付 9 到 10 個比特幣，約台幣 30 萬元，否則就會進行更大規模攻擊。而所謂的 DDoS 分散式阻斷服務攻擊，就是駭客透過不同地方的電腦，組成「魁儡殭屍網路」，灌爆目標的系統連線跟處理程式，讓其他的顧客無法進入，最大規模每小時可以攻擊 28 次。

行政院資安處處長簡宏偉：「假設今天有家店開了店，讓客人過來用餐之類，結果就有人在門口擋住，讓想用餐的都沒辦法進來。」

由於這次攻擊，宛如跟整個證券業開戰，依照刑法 360 條，如果攻擊者在國內可處以 3 年以下有期徒刑，拘役或科或併科 10 萬以下罰金。不過因爲攻擊者在國外，行政院資安處已經介入，把資安防護提高到國家層級，邀請刑事局等相關單位共同研商，替未來可能發生的攻擊提早做好防範。

HOME



垃圾鴿臉書爆紅 資安專家：小心潛在危機

2017 年 2 月 19 日

（中央社記者吳家豪台北 19 日電）最近你是否常在 Facebook （臉書）上看到一隻快速晃動的紫色鴿貼圖？資安大廠趨勢科技提醒，網路爆紅現象時常源自於社群網站的加持，但也請注意社群網站的潛在危機。

趨勢科技透露，事實上，紫色鴿正確的名稱是「垃圾鴿」。圖文創作者魏勒（ Syd Weiler ）於 1 月 31 日在 Facebook 貼圖初登場後，短短兩週的時間就成爲時下最夯的話題。且不只在台灣受到極大的迴響，「垃圾鴿」在短時間內就掀起全球風潮。

垃圾鴿貼圖囊括各種情境，總計 24 張，其中包含常見的喜怒哀樂情緒，但最爆紅的還是最後一張上下甩動脖子的垃圾鴿動態貼圖。滑開 Facebook 動態牆，每一個留言區都可以看到一整排快速晃動的紫色垃圾鴿。

作者魏勒表示，這單一貼圖並沒有特定的註解，牠可以是代表快樂、興奮、兩者皆是、或兩者皆非。多數用戶表示不能理解，但是很好笑，也許無厘頭就是「垃圾鴿」爆紅的主因。

以「無厘頭」爆紅的題材近年已不是少數， PPAP 就是最好的例子。然而，趨勢科技提醒，網路爆紅現象時常源自於社群網站的加持，多多使用社群網站是了解時事的其中一環，但也請注意社群網站的潛在危機。

趨勢科技建議使用「 Dr. Safety 安全達人」等行動安全軟體，利用「社交網路隱私檢測」功能，針對社群使用率最高的 Facebook 提供隱私設定檢測與建議，避免重要個資、親密相簿在不知不覺中外流。

第 8 條

直接蒐集個人資料應告知事項及免告知之情形

公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：

一、公務機關或非公務機關名稱。

二、蒐集之目的。

三、個人資料之類別。

四、個人資料利用之期間、地區、對象及方式。

五、當事人依第三條規定得行使之權利及方式。

六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

有下列情形之一者，得免爲前項之告知：

一、依法律規定得免告知。

二、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。

三、告知將妨害公務機關執行法定職務。

四、告知將妨害公共利益。

五、當事人明知應告知之內容。

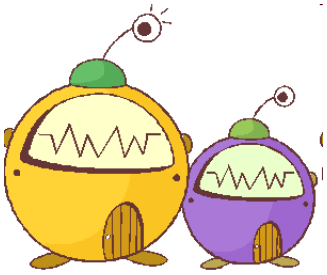
六、個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

HOME

Misfortune Cookie 不幸小餅干

資料出處： iThome

影響軟體的 HTTP cookie 管理機制有一項錯誤，使攻擊者可以發送經由改造的 HTTP cookies 攻擊該漏洞，並毀損記憶體、變更應用的狀態，進而遠端取得管理員權限，導致裝置使用者的不幸，並在侵入閘道之後，即可使 LAN 環境下的裝置面臨中間人攻擊（ man-in-the-middle ）的風險，安裝惡意程式或是永久改變其設定，此路由器安全漏洞命名爲 Misfortune Cookie 。



HOME