妥善管理網絡密碼自保安全

許佳龍
科大資訊、商業統計及營運管理學系講座教授

臉書（Facebook）於 3 月下旬再爆出資訊保安事故。據報導，Facebook 從 2012 年開始不當處理用戶密碼，有 2 億至 6 億用戶密碼，以明文（plain text）的形式儲存，沒有經過加密，亦即沒有以密文（cipher text）的安全形式儲存。這些以明文儲存的密碼，該公司內部上千名員工都可以輕易搜尋得到。雖然 Facebook 事後表示，受影響的密碼並未流出該公司；也還沒有發現任何濫用事件，不過，該公司將會通知受到影響的 Facebook、Facebook Lite 和 Instagram 用戶。

誠然，網絡活動已成為今日人們日常生活的重要組成部分，包括在社交媒體與友儕通訊、電郵、在網絡上進行金融活動、購物，甚至在物聯網中的家居電子裝置設施開關控制，都離不開使用密碼，如何對密碼進行管理，絕對不能掉以輕心，以保障自身在網絡世界裡的資訊安全。

不加密處理令人費解

多月前，程式碼版本控制服務網站 Github 和社交網絡平台 Twitter 都發生過類似事情，亦即儲存了未經特別處理的密碼，但卻沒有像 Facebook 今次受影響用戶規模那麼龐大；另一方面，能夠不當存取這些密碼的人數也不多。然而，由這些事故可見，管理好自己的網絡密碼，是今天網絡生活一個重要組成部分。

營運網站不當處理用戶密碼，其實也很令人費解，因為自從電腦問世，以至中央電腦系統使用後，已很清晰地確定，不會直接以明文形式來儲存帳戶的密碼，而是透過加密來儲存，亦即以密文（cipher text）形式儲存。例如先使用散列函數（hash function），把密碼轉換成一串看似隨機的數字，散列函數的特點是，光看輸出值很難猜出輸入的明文內容。當用戶登入時，輸入密碼後會經過散列函數轉換，系統會對比轉換結果，以確認密碼是否正確。這樣一來，系統無需直接比較用戶密碼的明文，又能確認輸入密碼正確，減少密碼外洩機會，即使系統遭受入侵，入侵者也不能看到帳戶密碼的明文原貌。

竊取密碼從中可圖利

看深一層，若然網絡營運者沒有謹慎地處理帳戶的密碼，用戶的確沒有辦法杜絕

「洩密」事故發生，即使如 Facebook 和 Twitter 這樣規模龐大的公司也未能堵塞這種粗略處理帳戶密碼的紕漏，反映用戶自身需要參與網絡安全進行「自保」。事實上，筆者過去在本欄談及網絡保安問題時，都強調在網絡安全上，用戶也有進行「自保」的個人需要以至責任。

用戶「自保」，首先要理解網絡入侵者攫取這些密碼資料後用來幹什麼？事實上，企業的網絡系統遭黑客入侵，帳戶的密碼資料遭一併竊取，事故時有所聞。嚴格來說，網絡攻擊者攫取了這些密碼資料，往往也未能從中直接得到金錢利益。以 Facebook 今次事故為例，假設這些密碼資料遭外部黑客竊取了，黑客亦未見得能夠馬上從中得到金錢上的利益。

不過，竊者可以從資料中，發掘和掌握若干用戶使用密碼的心態和行為習慣，例如，同一個用戶會使用同一組密碼在不同的網站上使用，甚至用來在網上進行金融活動和購物交易。於是，黑客便可以登入這個用戶其他牽涉金錢、或其他實質性得益的網站，從而把竊取密碼的利益實現。甚至可以非法冒充用戶當事人進行借貸甚或種種活動，從中謀利。

網絡安全需自我保護

因此，網絡使用者必須謹記，不宜用同一組密碼在多個網絡系統中使用。筆者明白，這樣做的確令當事人感到繁瑣，因為畢竟大多數人今天都擁有多個需要密碼登入的不同功能網絡帳戶，若每個帳戶都用不同密碼，人們有限的記憶力委實十分吃力，而遺忘密碼也難免發生，並因此帶來極大的不便。怎麼辦？

筆者建議，雖然在每個應用的網絡系統使用不同的密碼，我們會感到為難，但卻可以按不同網絡系統在安全性需要和敏感性上，進行高低程度的排列，在安全性需要或對安全敏感性高的應用網絡系統上，如個人銀行帳戶、支付系統等，宜用一組內容組合較複雜的密碼；那些安全性需要較低的應用網絡系統，則用另一組內容較為普通的密碼，亦即避免採用同一組密碼應用到個人所有的應用網絡系統中。此舉除了可以減少忘記密碼的機會外，還可得到較安全的保障。

很顯然，在今日大數據時代，資訊既是力量，也是財富，因而無論是網絡攻擊者、企業、或其他使用者，都對這些訊息甚感興趣。因為通過這些巨量的數據，可以從中掌握用戶與用戶之間的關聯性，分析這種種的關聯性，往往可以洞悉社會個體或群體行為的資料，據此用來進行營銷、推廣、說服甚至改變消費行為的策略性行動依據。

個體數據「群體化」

值得注意的是，過往，個人資訊的確只牽涉和影響到個人，但在目前的網絡世界，個人數據的儲存如此海量，個人的資訊已不再以「個體式」為單位，而是基於箇中種種關聯性而形成一個「集體式」單位，透過數據的分析，即可以得到一些超越個體的「集體性行為」訊息，這些訊息具極大價值，於是難免引來黑客攻擊數據庫、甚或出現公司以合法卻又過度地收集個人資料或訊息的行為。對市民用戶來說，進行網絡安全自保，除了對密碼進行妥善管理外，還需要考慮把一些沒有必要在網絡上保留的個人資料作出刪除。

在風險管理上，有「風險終止」（risk termination）和「風險減少」（risk reduction）之說。把風險終止，徹底消除，在網絡安全的情景而言，是不介入這個網絡系統或不下載這個應用程式，這樣便無風險問題可言。但是，在今日資訊網絡年代，我們很難不跟網絡打交道，故而盡量「風險減少」，減少自己承受的風險機會，盡量地減少個人資料在網絡上保存。這是用戶能夠實際地保護自己的方法。這些方法無疑很被動，卻又的確有點「無可奈何」。

法律條文保障的局限性

對於如何保護個人的資料和信息，歐盟於 2016 年 4 月 27 日通過了《一般資料保護規範》（General Data Protection Regulation・GDPR）法案，並於 2018 年 5 月 25 日起強制執行。

按法案規定，個人數據處理者必須清楚地披露任何數據收集，並聲明數據處理的合法基礎和目的，保留數據的時間，以及是否與任何第三方或歐盟以外的國家共享數據。用戶亦有權在特定情況下要求刪除其數據。公共主管部門和定期或系統地處理個人數據的企業，需要僱用數據保護官員（DPO）負責管理 GDPR 的合規性。若然數據洩露對用戶私隱產生不利影響，企業必須在 72 小時內向外公開通報，讓受影響的用戶能夠盡快作出應對，減少損失。

換言之，歐盟以新通過的 GDPR 法案，取代 1995 年推出的歐盟個人資料《數據保護指令》（Data Protection Directive），對數據處理者作出更嚴格的網絡個人資料保護要求。不過，即使法案作出更嚴格的保安要求，依然出現英航大量客戶的信用卡資料外洩事件。

在美國，負責網絡安全機構要求數據收集企業切實執行同用戶之間的協定，在服務合約開始釐訂時，清楚向用戶說明收集個人資料的用途，目的和儲存，若最後發現數據收集公司沒有履行合約上的承諾，該公司便要承擔事故過失的責任。

提高個人參與網絡保安意識

可以說，即使在法律層面，對個人的網絡系統資料作出保護，但在今日網絡世界和數據儲存規模如此龐大之下，網絡營運商如何應用和處理用戶的個人資料，用戶實在無從得知，甚至營運商自身恐怕亦非瞭如指掌，完全掌握。以 Facebook 今次事故例，密碼處理失當，可能真的是員工不小心的意外所造成，但是，在今日海量數據儲存的情況下，一個小錯失往往牽一髮動全身，引起「災難性」後果。因此，即使營運商全心真意想保護用戶的網絡資訊安全，但也有「百密一疏」出現安全事故的機會。所以，用戶在網絡安全上進行「自保」，是減少事故對自身作出損害的理性和有效方法。

總括來說，網絡保安是需要網絡系統營運商和用戶一起攜手進行保護。用戶有需要和有參與的責任為網絡安全出一分力。照目前資訊科技發展一日千里、金融科技不斷落實應用到實務環節，而物聯網的應用也日趨普遍的情況下，用戶應加強自我保護和有參與網絡保安責任的意識；了解自身在網絡上的潛在風險暴露狀態，從而作出有效的應對，只有如此，才能有效減少自身承受風險損失的機會。

〔本文由科大商學院傳訊部筆錄，許佳龍教授口述及整理定稿，文章在信報 4 月 8 日發表〕