**不只你我，連臉書執行長也在不同網路服務使用相同帳號密碼**

只要其中一個使用相同帳號、密碼的網站資料遭到外洩，駭客就可以嘗試使用這些外洩的帳號密碼，繼而到其他的網站試用，看看使用者是否在其他網站，也使用相同的帳號、密碼，如果是的話，駭客就可以用這組萬年帳號、密碼，輕易登入其他網站，不論是修改資料甚至是取得更多私人資訊等，都是具有極高的資安風險行為。

像是，駭客團體 OurMind 宣稱已經駭入臉書執行長馬克. 祖克柏（Mark Zuckerberg）的推特（Twitter）、Pinterest 和 Instagram 帳號，綜合各方報導，主要是因為馬克. 祖克柏這些社群服務使用的帳號密碼，和在 2012 年發生超過 650 萬、大規模資料外洩的社交網站 LinkedIn 的帳號密碼一致，駭客只需要測試使用早先外洩的帳號密碼，就可以掌控使用者各種網站的帳號。

無獨有爾，除了臉書外，還傳出 Google 執行長 Sundar Pichai 的及 Amazon 技術長 Werner Vogels 兩人的 Quora 或 Twitter 帳號，也都遭到駭客團體 OurMind 的入侵。據了解，同樣也是因為當年 LinkedIn 的使用者資料外洩，讓駭客團體有機可趁。甚至於，今天也傳出Twitter執行長Jack Dorsey的推特帳號也同樣被OurMind，對於堂堂推特執行長的推特帳號也被駭客入侵，顯得十分尷尬。

或許，有很多人會覺得意外，這些科技業界知名人士，應該是最熟悉這些新興社交科技工具的使用，也最理解潛藏的資安風險，怎麼樣也無法想像，馬克. 祖克柏的推特帳號的密碼，其實簡單到不能再簡單的「dadada」，而這也是無法在任何網站服務的密碼設定規則中，脆弱到不能再脆弱的弱密碼規則。

當然，這也可能有一個原因就是，臉書執行長因為平常使用的社群服務就是臉書，其他包括推特或者是 LinkedIn 等，可能已經是多年未曾使用，甚至是忘了這些社群服務的存在，也因此，就沒有針對相關帳號的密碼作密碼強化。這也可以從馬克. 祖克柏的 Google+並沒有同時遭駭，可以得此推論。

**臺灣也曾經發生過類似的資訊拼圖資安事件**

不論是因為鮮少使用而輕忽密碼的設定，或者是根本忘記這些網路服務的存在，類似這種使用不同網站服務所因為資料外洩取得的帳號密碼等資訊，有心者，基本上都可以用來在其他不同網站試試看。

多數人都覺得，臺灣民眾的個資老早就已經外洩光光，怎麼樣保護也都沒有意義，而這種駭客使用外洩的帳號密碼，用來在其他網站嘗試

登入使用者帳號的手法，臺灣稱之為資訊拼圖手法，而臺灣在將近十年前，也曾經發生過類似手法的資安事件。

2007 年 12 月，當時全臺灣鎖定女性客戶為主的康迅數位整合（Payeasy），當時有來自中國及香港的 IP，異常大量登入該網站並且試圖破解正確的帳號與密碼，光是在 12 小時內就登入了 3 萬 9 千多次，其中，登入成功的帳號也超過 5,400 個帳號。

這些駭客其實是藉由從其他地方蒐集而來 4 萬筆的帳號和密碼等資料，試圖使用相同的帳號密碼，登入 Payeasy 網站，而這些駭客所蒐集的帳號中，大約有 4 成是 Payeasy 的會員帳號（大約 1 萬 6 千個帳號），但針對這些是該網站會員的資料，可以成功登入網站的數量大約 5,400 筆，占整體比例約為三分之一，這也意味著，當時駭客從其他地方蒐集而來的使用者資料，可重複利用的比例相當高。

而根據當年的資訊顯示，這些駭客用來登入 Payeasy 的帳號密碼，其中有三分之一可以順利登入成功的，都是一次登入就生效。這也就是說，就算 Payeasy 想要利用封鎖特定 IP 位址甚至是某些網段的手法，其實是無效的方式。

當時有許多人在不同的網站，為了怕自己忘記，都習慣使用相同的帳號和密碼，也容易發生這種「一處外洩，處處外洩」的高風險情況。而舊事重提讓人感到膽顫心驚的狀況卻是，將近十年前發生的歷史，在十年後又發生類似的狀況，這表示資安事件本身有一種循環的特性，而連人的本性，其實也都沒有長進，一直在重蹈覆轍。

**採用更安全的密碼設定，是保護帳號安全的第一步**

從這些科技名人發生的案例中可以看出，許多人對於密碼的設定，都還是容易輕忽，不論是使用很容易被破解的弱密碼，或者是一些可以透過使用者個人資訊，取得重新設定密碼的管道，都讓網站的密碼的設定，陷入一種不確定的不安之中。

也因此，近年來，有許多網站在提供相關的網路服務時，為了資安的因素，已經會開始在帳號尤其是密碼的設定上，以系統性的方式作限制，例如，網站業者會在經過某一段時間後，開始強迫使用者更換新的密碼；也會設定密碼強度規則，必須要有英文大小寫和數字，甚至包含符號在內的 6 個字元以上的密碼；也有一些網站提供安全性更高的雙因素認證服務，使用者可以利用手機發送確認簡訊，或者是電子郵件發送重設密碼的連結方式，重新設定更安全的密碼。

不過，從各種更安全的強密碼建議方式看來，除了至少 6 個位元以上的長度設定外，使用者其實可以自行設定一個屬於自己才知道的密碼設定邏輯，同樣採用雙因素認證的精神，透過一組固定的密碼設定原則，搭配另外一組變動的密碼設定原則，就可以創造一個可以適用於不同網站服務的密碼設定，但又不容易忘記的密碼原則。

舉例而言，固定的密碼設定原則，可能是一組只有你自己才知道的密碼設定，不論是將一句中文改用英文輸入作為不規則的密碼原則，或者是某些鍵盤上的排列原則，甚至是某些只有自己長年使用的密碼設定資料等等，都可以作為第一組固定的密碼設定原則。

現在多數網站密碼設定幾乎不會設定上限時，另外一組變動的密碼設定原則，可以採用像是，如果在 iThome 網站申請會員帳號時，設定密碼時，就可以固定在密碼的第幾個字元開始，加入自行設定的字元規則，例如，取 3 個網站的字母作為該網站的密碼設定：iTh。

也就是說，使用者可以設定一組固定常用的密碼類型作為密碼設定的基礎，再搭配另外一個可以變動但有邏輯和原則的密碼設定方式，就有機會創造一個既安全又不容易遺忘的安全密碼。