主題 達人專欄

# 你的網站密碼會如何外洩？如何兼顧方便和安全？

解凍豬腳 | 2020-10-22 08:00:03 | 巴幣 2290 | 人氣 4799

以前我們曾經在《巴哈帳密可能外流？快來了解你的帳號風險！》介紹過，當你在網站上註冊了帳號，你設定的密碼就會被以下的其中一種方式儲存在他們的伺服器裡：

1. 透過雜湊函數轉換成 hash 值後儲存在伺服器裡

2. 原封不動地直接把明文儲存在伺服器裡（比較爛的網站可能會這麼做）

如果你有把當初那篇文章看完就會知道：如果你註冊的其中一個網站對於資訊安全控管得不好、被入侵了，你使用的那組密碼就會被駭客拿去當成嘗試密碼的素材，那你在其他也使用了同一組密碼的網站帳號也就形同跟著外洩。

## 。你的密碼會如何外洩？

想像一個情境：假設你今天在各大網站的帳號都使用這組看起來已經足夠複雜的強密碼「psFt*$4kM4Du&F^6」。我們都知道，像這種在毫無規則的情況下以大寫英文、小寫英文、數字、特殊符號混合組成的密碼非常安全，因為根本不會被猜出來（光是大小寫英文加數字的 16 位密碼就有至少 4.7 × 10^28 種可能），一部經典電腦（一般的電腦）也難以在短時間用暴力破解的方式測試出你的密碼。

——結果好死不死，這網站出包了，竟然讓偷偷入侵的駭客們得到了你的那組完整密碼。或許是網站管理員不慎把你未經過處理的完整密碼儲存在伺服器或資料庫裡（案 1），或許是服務提供者壓根就沒有幫你做好密碼傳輸過程的防護措施（案 2），或許是駭客透過軟體本身的漏洞

前往大廳 TOP

控制整台伺服器、偷偷埋下後門在不知不覺的情況下監聽你的資訊（案3）。

案 1：2018 年 Twitter 明文儲存密碼事件
案 2：2015 年 PChome IM 使用 HTTP 協定傳輸敏感資訊事件
案 3：2013 年美國國家安全局稜鏡計劃揭發事件（有人來按電鈴囉）

接下來駭客們共享著這份資料庫，所有駭客都已經知道會有人使用 psFt*$4kM4Du&F^6 這組字串當作網站服務的密碼，同時透過計算得到了這組密碼的 MD5（註）是 E67D E4C5 0764 6CFB AF1F 4791 FE76 C86F，把 psFt*$4kM4Du&F^6 <=> E67D...C86F 這樣的對應關係記錄下來。

註：這裡只是用 MD5 算法作例，實際上不是所有的網站都會用 MD5 當作 hash 值的唯一計算方式。

接著，當他們之後又入侵、取得了別的網站的資料庫內容，即使這個網站事前已經透過 MD5 的算法把你的密碼經過轉換才儲存進去，駭客只要注意到有任何一組密碼的 MD5 值是 E67D...C86F，他就可以透過先前的經驗得知，這組帳號的密碼正是 psFt*$4kM4Du&F^6。

最要命的情況是，如果你的帳號、密碼組合在不同網站之間都一模一樣，一旦其中一個網站發生了密碼外洩事件，那就等於其他網站的帳號一起連環爆（即使這些其他的網站伺服器根本沒被入侵）。

因此，網站密碼外洩的風險通常都是連鎖發生的。特別是你也無法確定你使用的網站究竟有多安全，那你就應該要使用具有同時以下四個特徵的密碼：

1. 足夠複雜
2. 足夠長
3. 不太可能會被別人使用
4. 你也不曾在別的網站使用過

前往大廳
TOP

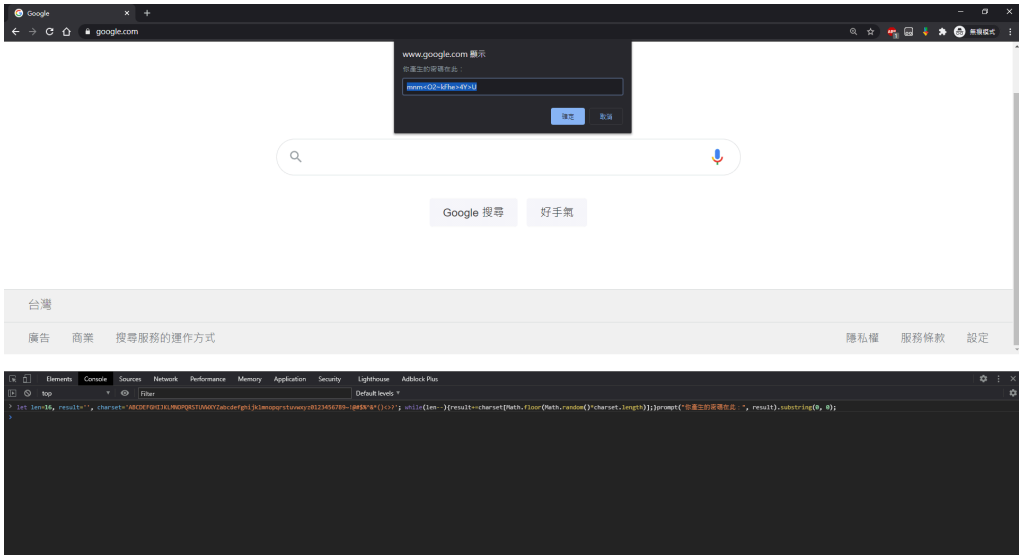
## 。如何決定密碼？

掌握了上面幾項原則，我們會得到「安全」的目的——即使其中一個網站密碼外洩，其他的網站至少不會跟著遭殃。

所以我們可以寫一段 JavaScript 的腳本，專門用來產生密碼（len 是密碼長度，charset 是產生字串採用的字元表）：

```
let len=6, result='', charset='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789~!@#$%^&*()<>?'; while(len--){result+=charset[Math.floor(Math.random()*charset.length)];}prompt("你產生的密碼在此：", result).substring(0, 0);
```

只要打開瀏覽器按一下 F12，找到「控制台」或是「Console」的地方，接著把這段腳本丟進去再按 Enter 就可以了：




如果想要做到一樣的效果，只要 Google 一下就可以找到很多現成的線上工具。然而，有些產生隨機字串的線上工具並不是直接用 JavaScript 全程在你的電腦上產生出字串來，所以仍然會有「被對方記下你產生了什麼字串」的可能，畢竟你不知道這個工具是否能信任——這正是刻意使用自己的瀏覽器（而不是依賴別人）來產生字串的原因。

問題來了，如果我們每一組密碼完全都是隨機產生的字串，這樣的

密碼必然難以記憶，所以我們還有一項要求就是「方便記憶（或取得）」，具體做法就是把這樣的內容和其他好記的東西組合起來。

假設我們產生了一組字串「Ty^a5Z」，我們可以首先把字串抄寫下來放在安全的地方，然後想辦法把它背起來。一般來說在「不使用『記住密碼』」而且「時常使用」的情況下，這樣的字串對一般人來說應該不難記憶。

為了在方便記憶的前提上繼續加長密碼以提高安全性，我們可以加上一些簡單的元素，比如說網址裡網站名稱的後面四位英文字母（ref：個人公式密碼 by 巴哈姆特站長 sega），然後再加上自己的出生年份，像這樣：

巴哈姆特：amerTy^a5Z1997
Facebook：bookTy^a5Z1997
Google：ogleTy^a5Z1997
Twitter：tterTy^a5Z1997
LINE：lineTy^a5Z1997
Spotify：tifyTy^a5Z1997
露天：utenTy6a5Z1997 ← 注意：露天、PChome、momo 購物網是少數不接受特殊符號當作密碼的網站，我們可以直接用喜歡的數字或是按鍵位置對應的數字來當作替代方案。

僅此，我們就已經達到了複雜、長度、獨特、記憶的四大需求，至少純粹的資料庫外洩和自動化的攻擊絕對不會經由擴散而波及到你的其他帳號。

## 。對於資訊安全有高度要求怎麼辦？（進階使用者適用）

剛才提到的密碼設計原則足以抵抗八成以上的連鎖風險。然而，你沒辦法排除「駭客就是衝著你來」的可能（就算這種可能性很小）。

比如說，也許你在 Twitter 上面使用了這樣的組合：
帳號：johnny860726

前往大廳
TOP

密碼：tterTy^a5Z1997

然後在 Google 服務上面使用了這樣的組合：
帳號：johnny860726@gmail.com
密碼：ogleTy^a5Z1997

如果我是駭客，我透過前面幾段提到的方式，剛好拿到了你在 Twitter 上面的帳號密碼。接著，我發現你在 Twitter 上面的密碼是 tter 開頭，判斷你就是使用網站名稱後四位來當作密碼前綴，同時我就可以按照「大部分的 Google 使用者都是直接使用 Gmail 地址」的常理推斷出你可能使用 johnny860726@gmail.com 和 ogleTy^a5Z1997 當作 Google 服務的帳號密碼。

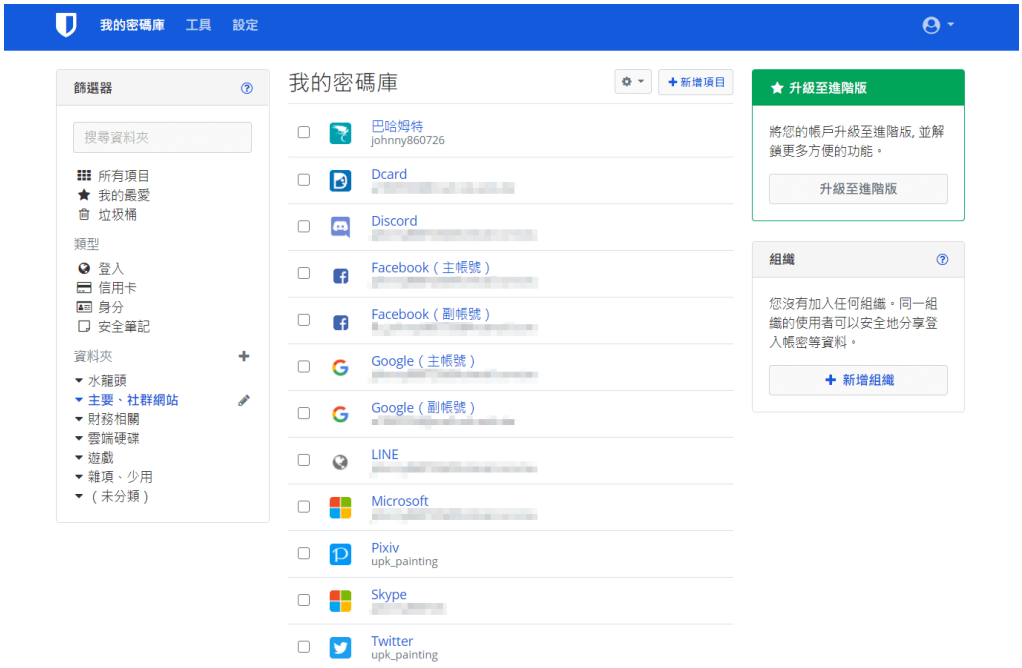
於是你在 Google 雲端硬碟放的那些自拍屌照通通都被駭客看光光了。這種事情一旦發生了，而且還是遇上最惡質的那種駭客的話，他甚至可以透過人肉搜索的手段找到你的好友圈，然後藉此要脅你支付贖金。

Oh, my god. 這聽起來真的挺恐怖的。

在最近網路使用需求暴增的年代，各家廠商也逐漸發展出了「密碼管理服務」。閱讀本篇內容至此，大家應該都有了「不能輕易把共通的密碼交給任何一個網站的伺服器」的觀念，所以你應該不會想要使用密碼管理服務。

但密碼管理服務也不是那麼可怕。為了取信於使用者，這些廠商通常會採取「加密後才上傳保管」的策略。有的廠商還會開源（公布軟體的原始碼），讓進階使用者得以檢驗程式碼內容，甚至自行架設獨立的伺服器來運作密碼管理服務。所以如果你又懶又怕危險，可以選擇一個「已經維持運作一段時間，而且已經有大量客群」的密碼管理服務。

以我個人而言，我使用的是 Bitwarden 這個服務（註：非業配！我沒收錢，而且這是免費的服務）。這個服務基本上就是你選定一個複雜的密碼註冊一個帳號，然後就可以把你各個網站的帳號密碼通通存進去：



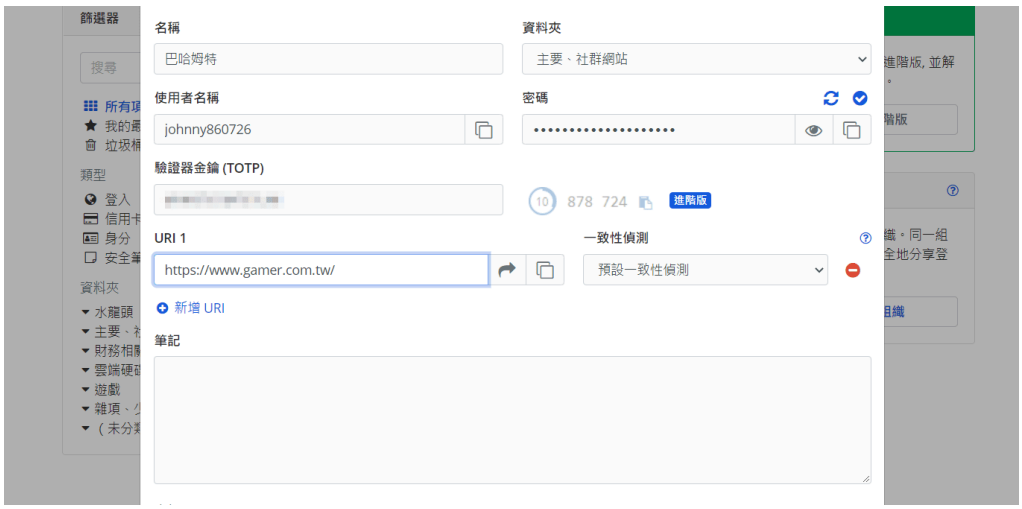

它也有現成的工具可以代替剛才前面寫的簡單 JavaScript 腳本，替你產生隨機的高強度密碼字串：


如果不想每次登入帳號都得使用網頁版複製密碼，你還可以在瀏覽器上安裝 Bitwarden 的擴充外掛，直接在小面板上操作：

前往大廳
TOP


這個小面板平時分為鎖定狀態或非鎖定狀態，如果你超過一段時間沒有動作，它就會自動上鎖，這時候你就得輸入一次 Bitwarden 的主密碼來解鎖，解鎖後就可以存取裡面的密碼了。要是連輸入主密碼都懶的話，你還可以幫這個小面板設定 PIN 碼。設了 PIN 碼，每次打開瀏覽器輸入主密碼登入以後，只要它進入鎖定狀態，輸入 PIN 碼就會解鎖（就像手機一樣）。

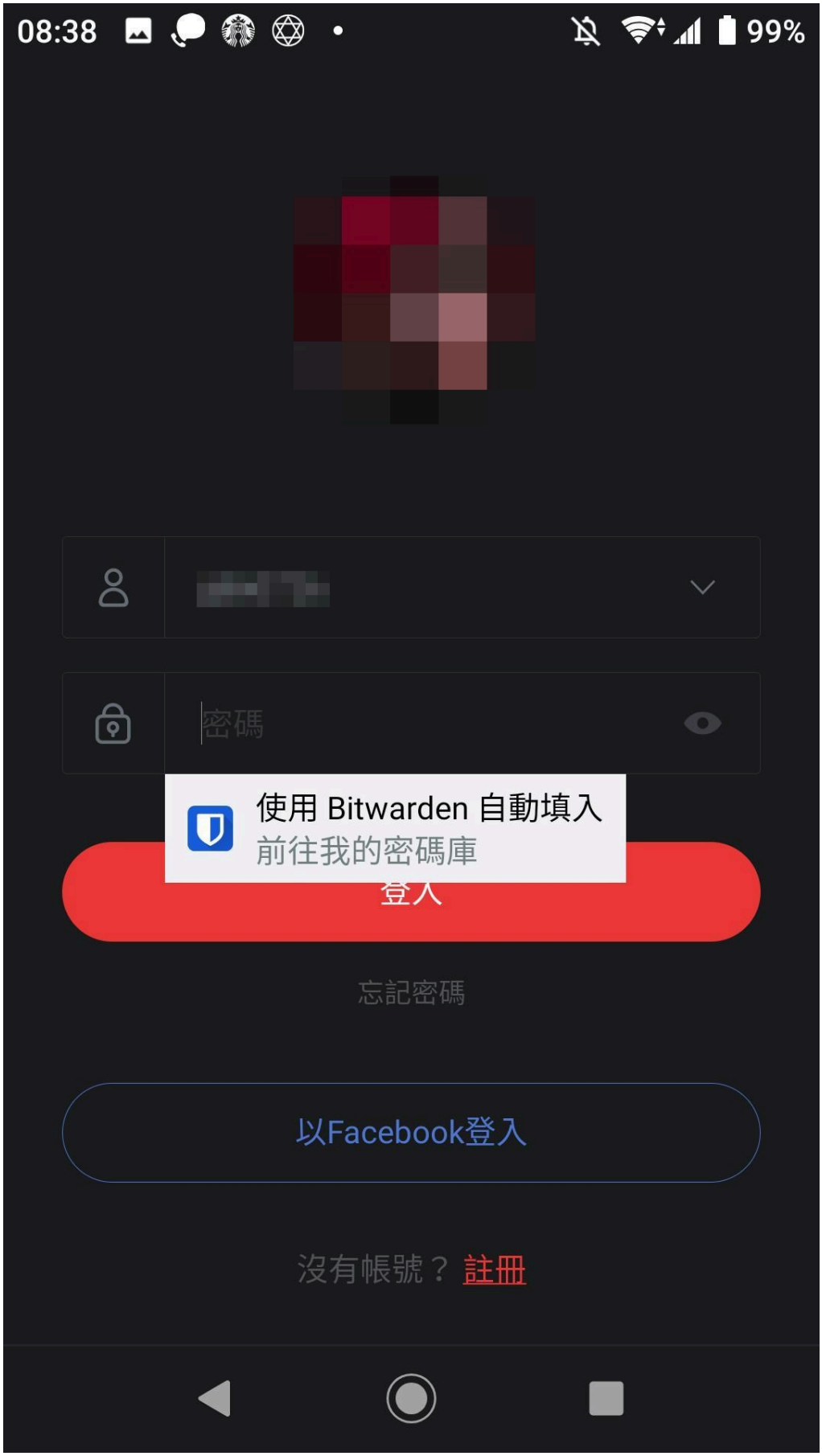
這擴充外掛還有一個很炫炮的功能，就是你可以直接從右鍵選單輸入帳號密碼。這個功能要在你有填入該網站的 URI（網址）才會有效，所以你在建立網站帳號密碼資料的時候可以把該網站的主站網址一起丟進去：




鎖定狀態：


未鎖定狀態：


甚至連手機版的 Bitwarden 都可以自動偵測相似的 App 讓你自動填入：




為什麼要強調這個自動填入功能，主要是因為「在手機上面複製密碼」是一件很危險的事情。你安裝在手機裡的 App 不見得每個都是安全的，它們有可能會不經你的允許去偷窺你手機的剪貼簿內容（也就是你

前往大廳
TOP

複製起來的東西），你永遠不知道它們會把你複製的東西偷偷拿去幹什麼，所以你會需要使用自動填入功能。

不過，使用密碼管理服務一定要非常小心！因為它是加密過後才送過去儲存起來（所以要是忘記了主密碼，官方沒辦法幫你找回來），而且世界上也沒有人可以保證這些服務百分之百不會遇上任何意外，所以在你信任這個服務的同時，也應該自行用安全的方式保證自己仍然可以找回所有密碼，例如：

1. 把密碼管理服務的所有密碼匯出，然後把匯出的檔案用壓縮檔加密，自己保存數份，同時把未加密的匯出檔刪除，不要讓別人有機會翻閱

2. 把密碼管理服務的主密碼抄寫下來，藏在房間裡某個不會被人發現也不會被蟲子啃光的角落

市面上當然還有其他很多款像這樣的密碼管理服務，不過有些沒有自動填入功能、有些光是基本功能就要付費，有興趣的話可以去研究一下。我目前實際套用密碼管理服務以後，大部分網站的密碼（包括糟糕的網站）都是超過 20 位的大小寫英數符號混合隨機字串，這樣一來我也不用擔心網站資料庫外洩的連鎖效應，而且只要記得主密碼就可以存取全部的帳號又同時保有一定的安全性了。

再次強調兩點，如果你要使用密碼管理服務的話：

1. 請找你可以信任的廠商，每個廠商都不信任的話你就得自己架設伺服器

2. 用來登入密碼管理服務的主密碼一定要記得比你的身分證字號還要牢

篇幅好像有點長了，本來想要順帶講講二階段驗證的原理，今天就到這裡作結吧。在這個依賴網路生活的時代，記得千萬不要忽視資訊安全的重要性。

上一篇 下一篇 前往大廳

#網路 #資訊 #資訊安全 #網路安全 #密碼 #帳號 #密碼管理