資安月報四月號

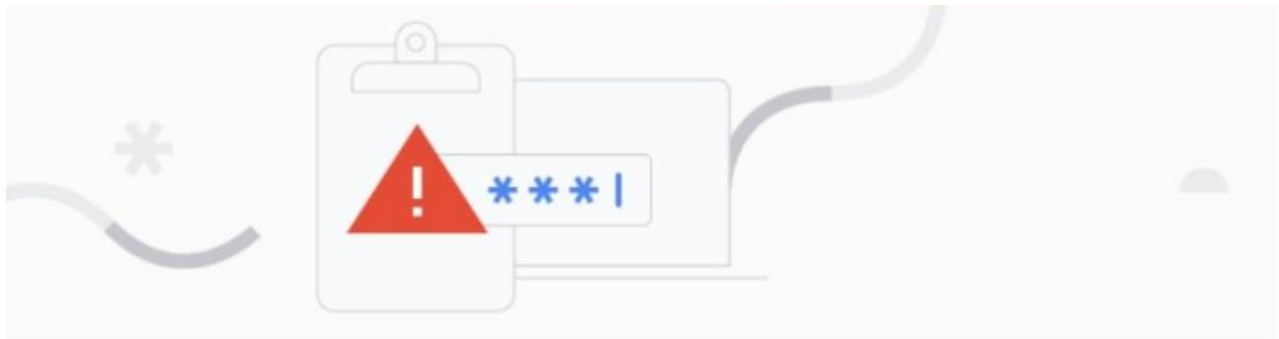
Google Chrome的密碼保護功能

康聯生醫
Healthconn

1. 前言
2. Chrome的密碼保護如何運作
3. 繼續使用被警告的密碼有何風險
4. 收到警告後五步驟自我保護
5. 如何建立高強度密碼

康聯生醫 Healthconn

前言



你曾經在Chrome 輸入密碼後看過左圖的警告訊息嗎?

前言 (續)

- 其實這是Chrome於 2019 年 2 月開始推出的密碼保護功能。
- 該功能最初僅在 Chrome 78 中提供給 Android 和 Windows 使用者，後來於 2019 年 5 月擴展到 macOS、Linux 和 iOS 使用者。
- 如果 Chrome 偵測到您使用的密碼曾在資料外洩事件中曝光，Chrome 會顯示警告訊息，代表密碼有外洩風險，建議您變更密碼。

Chrome的密碼保護如何運作？

Chrome 透過以下方式偵測外洩密碼：

- Chrome 會將您儲存在 Chrome 中的密碼與已知的資料外洩密碼資料庫進行比對。
- Chrome 會在您登入網站時檢查該網站是否已發生資料外洩。

繼續使用被警告的密碼有何風險？

繼續使用被警告的密碼存在著相當大的風險。當密碼被警告為可能在資料外洩事件中曝光時，意味著該密碼可能已被駭客或不當取得。如果您繼續使用這個密碼，可能會面臨以下風險：

- 未經授權存取： 駭客可能已經獲取了您的密碼，這意味著他們有可能進行未經授權進而掌控您的帳戶，從事不當活動，例如更改密碼、修改個人設定、發送詐騙訊息，甚至進行欺騙性行為。比如：使用您的帳戶發送垃圾郵件、傳播電腦/手機病毒等惡意軟體或進行其他惡意活動。
- 帳戶被連鎖盜用： 如果您在多個網站上使用相同的密碼，駭客可能試圖使用已獲取的密碼來存取其他帳戶,這會增加您在其他網站上的帳戶被盜用的風險。
- 個人敏感資訊外洩： 如果您的帳戶包含敏感信息，他們可以登入您的帳戶並竊取您的個人資訊，例如信用卡號碼、地址等，這些信息可能被不當使用，導致財務損失或身份盜竊。

康聯生醫 Healthconn

收到警告後五步驟自我保護

以下是一些建議的處理方式：

1. 立即更改密碼： 如果您收到這樣的警告，建議您為所有使用相同密碼的帳戶變更密碼。確保新密碼強健且不易被猜測，建議包含大、小寫字母、數字和特殊符號。
   - 使用強密碼。
   - 使用短句而不是單字。
   - 使用密碼生成器來生成強密碼。
   - 不要在多個帳戶中重複使用相同的密碼。
2. 使用密碼管理器： 考慮使用密碼管理器，以生成並存儲複雜、獨特的密碼。密碼管理器有助於提高安全性，並確保您不會因過於簡單或重複使用密碼而受到風險。並定期更新您的密碼管理員中的密碼。
3. 啟用雙重驗證： 如有可能，啟用帳戶的雙重驗證/兩步驟驗證 (2FA)，以提高安全性。這通常需要您在輸入密碼後再進行一個額外的身份驗證步驟。
4. 定期檢查帳戶活動： 定期檢查您各個線上帳戶的活動紀錄，確保沒有異常或未授權的活動。
5. 保持軟體更新： 確保您的瀏覽器和相關的安全軟體都是最新版本，以確保擁有最新的安全性修補程式。

如何建立高強度密碼

2023年8月號資安月報曾建議過如何建立高強度密碼呢！這裡再和大家複習一下：

- 混合使用特殊字符、數字和大寫字母。包括一系列大寫和小寫字母以及數字和符號（例如$£！），這使得密碼更安全且更難以破解。

- 密碼應盡量長，至少包含8-12 個字符。密碼越長越好。較長的密碼需要更多的時間來計算組合，而尋求快速破解的駭客可能會放棄。

康聯生醫 Healthconn

參考資料

- https://blog.trendmicro.com.tw/?p=80701
- 2023年8月號資安月報：弱密碼排行榜