

مواقع توضح لك مدى قوة كلمات شرك وهل تم تسريبها؟



الخميس 11 أبريل 2019 11:04 م

أثبتت التسريبات الأخيرة لشركات كبرى مثل فيسبوك أنه مهما كانت كلمة شرك طويلة وقوية فإنها باختصار لا تزال غير آمنة، أي شيء يدخل الإنترنت فهو غير آمن

وذلك لأن أمان كلمة المرور لا يأتي فقط وفقاً لتقدير المستخدم الذي أنشأها، ولكن أيضاً من الخادم الذي يتم تخزينها عليه

لا يوجد شيء يمكننا القيام به لتغيير حقيقة أن قواعد البيانات عرضة للانتهاكات، وأن بياناتنا ليست مقدسة، لذلك يجب علينا مراقبة كلمات المرور الخاصة بنا على الإنترنت باستمرار

ويمكن القيام بذلك عن طريق مواقع تقوم بتحديث بياناتها كلما حدث اختراق لمساعدتك في مراقبة ما إذا كانت كلمات مرورك قد تسربت عبر الإنترنت

1- هاف أي بين بواند (Haveibeenpwned)

كلمة "pwn" هي مصطلح يستخدمه الناس غالباً في ثقافة الإنترنت -عادةً من قبل اللاعبين- لوصف هزيمة شخص ما بطريقة ما

لاستخدام الموقع، اكتب ببساطة عنوان بريدك الإلكتروني واضغط على زر "pwned"، وسيتم إخبارك إن كانت كلمات المرور الخاصة بك آمنة، أو ستري عدد المواقع التي تم اختراقها وكلمات المرور التي تم العثور عليها والتي تخصك

يحتوي الموقع أيضاً على قسم يسمى "كلمات مرور Pwned"، حيث يمكنك البحث باستخدام كلمة المرور بدلا من البريد الإلكتروني سيعلمك هذا إذا كانت كلمة المرور هذه موجودة بالفعل في قوائم الكلمات عبر الإنترنت

2- كريديت كارما (Credit Karma)

يتمتع "كريديت كارما" بسمعة جيدة لمراقبة كلمات الأمان الخاصة بك، يتجاوز كريديت كارما كل مواقع مراقبة كلمات المرور الأخرى، حتى يظهر لك نسخة خاضعة للمراقبة من كلمة المرور التي تم تسريبها في كل موقع مدرج

كل ما عليك القيام به هو تسجيل الدخول، والانتقال إلى صفحة مراقبة الهوية الخاصة بالموقع، وانقر فوق عرض التفاصيل أسفل جدول مراقبة خرق البيانات فهذا الموقع واحد من أكثر الطرق الجيدة لتتبع كلمات المرور الخاصة بك على الإنترنت

3- دي هاشد (DeHashed)

بعد "دي هاشد" خيارا نهائيا قوياً قد يساعدك في العثور على كلمات المرور المسربة التي لم تتمكن من إيجادها في الموقعين السابقين، وعلى الرغم من أنه لا يتميز كثيراً عن سابقيه، فإنه قد يوفر بعض المعلومات عن كلمات السر الخاصة بك

مع تحققك من هذه المواقع الثلاثة بشكل دوري، ستكون قادراً على معرفة وضع كلمات المرور الخاصة بك بمجرد ظهورها، وقد تفاجأ بما تجده