أفضل 3 طرق لاختيار كلمة مرور قوية دون أن تنساها

الأربعاء 11 فبراير 2026 06:00 م

معظمنا يستخدم كلمات المرور يوميًا، لكن تذكرها جميعًا يكاد يكون أمرًا مستحيلاً، فإذا استخدمت كلمة مرور سهلة مثل تاريخ ميلادك، يمكن اختراقها، وحتى لو بذلت جهدًا كبيرًا لحفظ كلمة مرور عشوائية، فلن يُجدي ذلك نفعًا إذا استخدمتها على أكثر من موقع، لأن اختراق واحدة منها قد يُعرّض جميع خدماتك الأخرى للخطر.

والحل الوحيد هو الاعتماد على مدير كلمات المرور، وبفضل هذه الأداة، أصبح استخدام كلمة مرور قوية مختلفة لكل موقع إلكتروني أمرًا في غاية السهولة.

تعمل برامج إدارة كلمات المرور المتكاملة والفعّالة على جميع أجهزتك، سواء كانت أجهزة كمبيوتر مكتبية أو محمولة أو هواتف ذكية أو أجهزة لوحية. فهي تُنشئ كلمات مرور يصعب تخمينها، مثل Z~/NQ"e5=|OO=qf9، وتحفظها نيابةً عنك، وتستخدمها تلقائيًا لتسجيل الدخول إلى مواقعك الآمنة.

لكن ثمة مشكلة واحدة، فمعظم برامج إدارة كلمات المرور تعتمد على كلمة مرور رئيسة لحماية جميع كلمات المرور الفردية. ويجب أن تكون كلمة المرور الرئيسة غير قابلة للاختراق، لأن أي شخص يمتلكها يستطيع الوصول إلى جميع مواقعك الآمنة. ولكن يجب أن تكون أيضًا سهلة التذكر، على عكس الكلمات غير المفهومة منمولدات كلمات المرور العشوائية.

لنفترض أنك اتخذت جميع الإجراءات الأمنية الصحيحة. وقمت بتثبيت برنامج مكافحة فيروسات أو حزمة برامج أمنية، واستعنت بمدير كلمات مرور لإدارة كلمات مرورك الكثيرة، لكنك ما زلت تواجه صعوبة في تذكر كلمة مرور رئيسة واحدة شديدة الأمان لحماية مدير كلمات المرور هذا. إليك بعض النصائح لاختيار كلمة مرور يسهل تذكرها ويصعب تخمينها.

1. ابتكر كلمات مرور شعرية

لكل شخص قصيدة أو أغنية مفضلة لا تُنسى. قد تكون بيتًا من الشعر، أو مقطعًا محببًا من أغنية، أيًا كان المقطع أو البيت، يمكنك تحويله إلى كلمة مرور. إليك الطريقة:

طريقة الأحرف الأولى: اختر بيت شعر مفضلاً وخذ الحرف الأول من كل كلمة.

مثال: "ألا ليت الشباب يعود يومًا" ← تصبح Alsyw.

التطوير: أضف رموزًا وأرقامًا في البداية أو النهاية لتصل إلى 12 حرفًا على الأقل.

طريقة الدمج الرقمي: اختر سطرين من قصيدة واستخدمهما كجملة واحدة مع استبدال المسافات برموز.

مثال: "الخيل والليل والبيداء تعرفني" ← AlkH@yl&WalyL#2025.

طريقة الاستبدال الرمزي: اختر كلمة مفتاحية من قصيدة وعقدها باستبدال الحروف برموز تشبهها.

مثال: كلمة "المتنبي" ← lmTnB1@ Facebook +5

نصائح للأمان:

الطول أهم من التعقيد: استهدف 12-16 رمزًا على الأقل.

التنويع: استخدم مزيجًا من الأحرف الكبيرة والصغيرة، الأرقام، والرموز.

تجنب المشهور جدًا: لا تستخدم أبياتًا شائعة للغاية (مثل "ما كل ما يتمنى المرء يدركه") دون تعديلات جوهرية، لأن الهاكرز يستخدمون قواميس تضم أشهر الاقتباسات.

2. كلمة مرور مثالية

ينصح خبراء كلمات المرور دائمًا بتضمين جميع أنواع الأحرف الأربعة: الأحرف الكبيرة، والأحرف الصغيرة، والأرقام، وعلامات الترقيم. والسبب هو أنه بتوسيع نطاق الأحرف،

يزداد الوقت اللازم لاختراق كلمة المرور بشكل كبير. ولكن طول كلمة المرور بحد ذاته يزيد من صعوبة اختراقها، ومن طرق الحصول على كلمة مرور طويلة يسهل تذكرها استخدام عبارة مرور.

سخرت سلسلة الرسوم الهزلية الإلكترونية الذكية والساخرة XKCD من أنظمة كلمات المرور الغريبة، التي توصي بالبدء بكلمة شائعة، واستبدال بعض الأحرف بأرقام متشابهة، ثم إضافة بضعة أحرف إضافية. لأنه قد يجعلك هذا تتساءل: هل كانت Tr0ub4dor&3، أم Tr0ub4dor&3؟ أم ربما Tr0m30ne&3؟ عبارة مرور مثل: دبوس، بطارية، حصان، صحيح يصعب فك شفرتها بشكل ملحوظ بسبب طولها، ولكنها أيضًا أسهل بكثير في التذكر.

لا تسمح جميع برامج إدارة كلمات المرور باستخدام المسافات في كلمة المرور الرئيسة. ما عليك سوى اختيار رمز مثل الشرطة، أو علامة المساواة للفصل بين الكلمات. نصيحة احترافية: تجنب استخدام فاصل يتطلب الضغط على مفتاح Shift. اختر كلمات لا تبدو مترابطة بشكل طبيعي، ثم ابتكر قصة أو صورة تذكيرية لربطها.

إذا كنت تواجه صعوبة في ابتكار كلمات غير ذات صلة لكلمة المرور الخاصة بك، فهناك العديد من مولدات عبارات المرور عبر الإنترنت، ويمكنك توليد عبارات مرور متعددة وحذف كلمة من كل منها.

3. كلمة المرور الطويلة

يقول خبير الحواسيب المخضرم ستيف جيبسون إن سر كلمات المرور الطويلة والقوية يكمن في إضافة أجزاء زائدة. إذا لم يتمكن المهاجم من اختراق كلمة مرورك باستخدام هجوم القاموس، أو أي وسيلة بسيطة أخرى، فإن الملاذ الوحيد هو إجراء مسح شامل لجميع كلمات المرور المحتملة. كل حرف إضافي يجعل هذا الهجوم أكثر صعوبة بشكل كبير.

ينضمن موقع جيبسون الإلكتروني برنامجًا يقوم بتحليل أي كلمة مرور تُدخلها بناءً على أنواع الأحرف المستخدمة وطولها. ويُقدّر البرنامج المدة التي سيستغرقها الهجوم المحتمل لكسر كلمة المرور. إنه ليس مقياسًا لقوة كلمة المرور، بل هو مقياس لوقت الكسر، ومن المفيد ملاحظة كيف يزداد وقت الكسر مع زيادة طول كلمة المرور.

والحل الأفضل في النهاية لتأمين كلمة المرور هو تعزيز حمايتها بنوع آخر من المصادقة. المصادقة متعددة العوامل، وتتضمن عادةً اثنين على الأقل من هذه الأنواع الثلاثة: شيء تعرفه (مثل كلمة المرور)، وشيء تملكه (مثل تطبيق الهاتف الذكي)، وشيء أنت عليه (مثل بصمة الإصبع).

وتتيح لك معظم برامج إدارة كلمات المرور استخدام تطبيق المصادقة لزيادة الأمان.