تحقق من أمن حساباتك 24 مليار اسم مستخدم وكلمة مرور تسربت إلى الويب المظلم

الخميس 23 يونيو 2022 09:46 م

نشرت شركة "ديجيتال شوز" (Digital Shadows) الرائدة في مجال استخبارات التهديدات والحماية من المخاطر الرقمية دراسة جديدة تحدد حجم اختراق كلمات المرور عالميا

وكشف الخبراء أن هناك أكثر من 24 مليار اسم مستخدم ومجموعات كلمات مرور متداولة في أسواق مجرمي الإنترنت، وكثير منها على الويب المظلم، ويمثل هذا الرقم زيادة بنسبة 65% على الرقم المذكور في التقرير السابق في عام 2020.

وتشير الدراسة إلى أن عددا صادما من مستعملي الإنترنت يستخدمون كلمات مرور سهلة جدا على الرغم من التحذيرات المتكررة، والعديد منها متداول على شبكة الإنترنت المظلمة حيث يختبئ مجرمو الإنترنت

ووجدت "ديجيتال شوز" أن كلمة "باسورد" (password) جنبا إلى جنب مع كلمة "كيو ويرتي" (qwerty) الكلاسيكية تصنفان من بين أفضل 50 كلمة مرور شائعة سهلة التخمين بشكل لا يصدق على الويب

كما توصلت الدراسة إلى أن واحدا من كل 200 مستخدم تقريبا يستعمل كلمة السر "123456".

ويقول خبراء شركة "ديجيتال شوز" إن 49 كلمة مرور من أصل 50 كلمة مرور شائعة الاستخدام يمكن "اختراقها" في أقل من ثانية واحدة بأدوات سهلة الاستخدام ومتوفرة وشائعة في المنتديات الإجرامية

ويمكن لإضافة رمز خاص مثل # أو * أن يزيد نحو 90 دقيقة إلى الوقت الذي يستغرقه المحتال في حل كلمة المرور

وبمجرد أن يخرق المتسلل قاعدة بيانات كلمات المرور ويأخذ البيانات يمكنه المضي قدما في فعل شيء يسمى حشو بيانات الاعتماد، حيث يجرب أسماء المستخدمين وكلمات المرور نفسها على كثير من المواقع الأخرى ليعرف إذا كنت تستخدم تفاصيل تسجيل الدخول ذاتها

وقال كبير محللي استخبارات التهديدات الإلكترونية في شركة "ديجيتال شوز" كريس مورغان "سننتقل إلى مستقبل من دون كلمات مرور، ولكن في الوقت الحالي أصبحت قضية اختراق بيانات الاعتماد خارج نطاق السيطرة؛ فلدى المجرمين قائمة لا حصر لها من بيانات الاعتماد المخترقة التي يمكنهم تجربتها، ولكن إضافة كلمات مرور ضعيفة إلى هذه المشكلة يعني أنه يمكن تخمين العديد من الحسابات باستخدام أدوات آلية في ثوان فقط".

ويحث الخبراء المستخدمين على التفكير في استخدام "مدير كلمات المرور" (password manager)، وهو تطبيق برمجي يساعد على توليد كلمات السر المعقدة واسترجاعها، ويحتمل تخزين كلمات السر هذه في قاعدة بيانات مشفرة، أو حساب مخصص على الطلب من قبل المستخدم نفسه

ويمكن أيضا استخدام المصادقة المتعددة العوامل (MFA) إذا كانت متوفرة، وذلك يسمح للأشخاص بتأكيد هويتهم باستخدام أرقام التعريف الشخصية أو التعرف على الوجه أو بصمات الأصابع بدلا من كلمة المرور

ومن الأفضل أيضا تخصيص كلمات مرور فريدة لكل موقع تستخدمه، وليس كلمة مرور واحدة للجميع