دراسة تحذر من أخطر كلمات المرور التي يتم اختراقها بأقل من ثانية حول العالم



تعد كلمات المرور خط الدفاع الأول الذي يمنع "المجرمين الإلكترونيين" من الوصول إلى البيانات والمعلومات الحساسة الخاصة بمستخدمي شبكة الانترنت.

ومع تزايد عدد الحسابات الرقمية المرتبطة بمختلف جوانب حياتنا، أصبح من الضروري على المستخدمين إنشاء كلمة مرور قوية، قادرة على حماية حساباتهم من الاختراقات، فكلما كانت كلمة المرور قوية، كلما كانت المعلومات الشخصية المرتبطة بالعمل أو المصرف أو الحياة الخاصة في مأمن، في حين أن اللجوء لاستخدام كلمات المرور الضعيفة يشبه إلى حد بعيد خطوة ترك باب المنزل مفتوحاً أمام السارقين.

ولكن التحول التقني الكبير الذي شهده العالم والذي أدى إلى امتلاك الأفراد، للعديد من الحسابات المرتبطة بشبكة الإنترنت، جعل من المرهق على هؤلاء اللجوء إلى كلمات المرور الفريدة، والقوية لتأمين حساباتهم المتعددة، فقاموا بدلاً من ذلك باستخدام كلمات مرور بسيطة لطالما تم التحذير منها، ما قد يتسبب لهم وللشركات والمصارف التي يتعاملون معها بعواقب وخيمة.

وهذه العادة السيئة حذّرت منها مؤخراً أداة NordPass لإدارة كلمات المرور، حيث أظهرت دراسة جديدة أجرتها الأداة بالتعاون مع خبراء مستقلين، أنه رغم الثقافة التكنولوجية الكبيرة التي بات يتمتع بها عدد كبير من الاشخاص حول العالم، إلا أن هناك الكثير من هؤلاء أصرّوا على استخدام بعض كلمات مرور، سهلة التوقع بسبب "الكسل"، وعدم رغبتهم بتذكر كلمات مرور صعبة.

17 كلمة مرور ابتعدوا عنها

ودعت الدراسة من يريد تأمين رسائل البريد الإلكتروني والخدمات المصرفية، وحسابات وسائل التواصل الاجتماعي وحتى حسابات منصات بث الأفلام، إلى الابتعاد كلياً عن هذه الكلمات وبذل جهد بتعيين كلمات مرور عصية على التخمين.

ويقول مهندس الاتصالات عيسى سعد الدين، في حديث لموقع "اقتصاد سكاي نيوز عربية"، إنه ليس هناك شك في أن مجرمي الإنترنت أصبحوا أكثر مهارة في اختراق مختلف أنواع الحسابات على الشبكة، ولكن المشكلة تكمن في أنه بدلاً من أن يحسّن المستخدمون من عادات إنشاء كلمات المرور، فقد ذهبوا باتجاه آخر وهو الاعتماد على كلمات لطالما تم التحذير منها، مشيراً إلى أن هذا الأمر يساعد المخترقين في عدم استخدام الأساليب المعقدة لتنفيذ هجماتهم، فيلجؤون إلى أسلوب "التخمين" لكلمات المرور الشائعة والسهلة، فتستغرق بذلك عملية اختراق الحسابات أقل من ثانية.

و شدد سعد الدين على أن الإنترنت تحوّل في الآونة الأخيرة، من وسيلة للترفيه والتواصل إلى وسيلة أساسية لتنفيذ مهام العمل وإجراء المعاملات المالية، ونقل المعلومات عالية الأهمية، ولذلك فإنه عندما يحصل المجرمون الإلكترونيون على بيانات ومعلومات خاصة بمؤسسات مالية، عن طريق بيانات العملاء أو الموظفين، فإن ذلك قد يعرضها لخسائر كبيرة، فضلاً عن إلحاق الضرر بسمعتها.

و أضاف أن إهمال المستخدمين لضرورة اختيار كلمة مرور قوية وصعبة، دفع بالعديد من المؤسسات والمصارف، إلى منع عملائها من تأمين حساباتهم المرتبطة بالخدمات التي تقدمها بكلمات سهلة وشائعة كالتي ذكرتها دراسة NordPass.

و يشرح سعد الدين أن كلمة المرور هي بمثابة البصمة الرقمية المميزة لكل شخص، والتي يفترض أن تكون عصية على الاختراق، ولذلك فإن تبرير خطوة اللجوء إلى كلمات المرور السهلة، بأن هناك صعوبة لتذكر الكلمات الصعبة والمتعددة، هو أمر لا يمكن القبول به، فالمحتالون يحلمون بالوصول إلى أي نقطة ضعف

أو ثغرة في حسابات المستخدمين، وهذا الحلم إذا تحقق سيكون كابوساً بالنسبة للمستخدمين، الذين عليهم اتخاذ خطوات تجنبهم الوقوع ضحية السرقة والابتزاز، وتحديداً من خلال الابتعاد عن الكلمات الـ 17 التي ذكرتها دراسة NordPass وغيرها من الكلمات السهلة.

العالم يتجّه للتخلص من كلمات المرور

من جهته يقول المحلل التقني عامر الطبش، في حديث لموقع "اقتصاد سكاي نيوز عربية"، إن العالم يمر اليوم بمرحلة الانتهاء من استعمال كلمات المرور، لصالح الاعتماد على نظام يتيح للمستخدمين، التعريف عن هويتهم من خلال بصمة الوجه أو الاصبع، الأمر الذي سيساهم في حلّ إحدى مشكلات الأمن الإلكتروني الأكثر انتشاراً على الإنترنت، والمرتبطة بقدرة مجرمي الانترنت على اكتشاف كلمات المرور، كاشفاً أن العديد من التطبيقات المصرفية وتطبيقات تحويل الأموال وتطبيقات المحافظ المالية، باتت تعتمد على "الحماية البيوميترية" التي توفرها بصمة الوجه أو بصمة الأصابع.

ولفت الطبش إلى أنه خلال هذه المرحلة الانتقالية التي يعيشها العالم التقني، يجب على المستخدمين الذين يحمون حساباتهم بكلمات المرور، مكافحة التهديد المتزايد الذي يواجهونه، والتأكد من أن لديهم كلمة مرور جيدة، والامتناع عن العادات السيئة المتمثلة باستخدام كلمات المرور الشائعة في العالم، وأسماء السيارات وأسمائهم وأسماء حيواناتهم الأليفة، إضافة إلى استخدام طبقات الحماية الإضافية التي توفرها بعض المواقع والمعروفة بـ authentication factor-Two.

و وصف الطبش "كلمة السر" بمثابة الدرع الذي يحمي المستخدمين في عالم الإنترنت، مشدداً على ضرورة اختيار أقواها عبر الالتزام بالقواعد التالية:

- أن تكون كلمات المرور طويلة، ومؤلفة من 12 حرفاً.

- أن تتضمن أحرفاً كبيرة وأحرفاً صغيرة وأرقاماً ونقاطاً ورموزاً.

- ألا تحتوي على أي معلومات شخصية.

- أن تكون كلمة غير مألوفة.

- أن لا يتم استخدام كلمة مرور واحدة لعدة حسابات على شبكة الإنترنت.