كاسبرسكي لاب تضع كلمات المرور تحت المجهر

السبت 13 يناير 2018 09:01 م

يدخل المستخدمون إلى حساباتهم على الإنترنت في كل الأوقات لتحويل الأموال بين الحسابات المصرفية، أو التسوق أو التحقق من الطقس أو حجز سيارة أجرة. ولكن ماذا لو لم يتمكّن المستخدم فجأة من الدخول إلى حساب يحتاج إليه؟ ماذا لو ظهرت له تلك الرسالة المزعجة "خطأ في كلمة المرور"؟ ألن يكون قادراً على العودة إلى المنزل في الوقت المناسب؟ مع إدراك أن الواقع في بعض الأحيان قد يتمثل في مواقف أكثر خطورة من ذلك. لقد وضعت أبحاث كاسبرسكي لاب معضلة كلمات المرور تحت المجهر لتكشف عن جوانبها للمستخدمين من أجل تمكينهم من حماية حساباتهم على الإنترنت بالطريقة المثلى.

وجدت كاسبرسكي لاب، في ظل الاعتماد المتزايد على حسابات الإنترنت في الحياة اليومية، أن المستخدمين يواجهون بشكل متزايد معضلة تتمثل بكيفية اختيارهم لكلمات المرور؛ فالبعض يلجأ إلى اختيار كلمات مرور قوية ومختلفة لكل حساب كي لا تكون الحسابات عُرضة للاختراق أو السرقة، ولكن هؤلاء يبقون عُرضة لخطر نسيان كلمات المرور، في حين يختار البعض الآخر كلمات مرور يَسهُل تذكرها وتتيسّر معها شؤون حياتهم، ولكنهم يكونون بذلك كمن يلعب بالنار ويعّرض نفسه لخطر مجرمي الإنترنت.

الخيار الأول لحلّ المعضلة: كلمات مرور قوية يصعب تذكّرها
وفقاً للدراسة البحثية التي أجرتها الشركة المختصة بأمن الإنترنت، يُدرك العديد من المستخدمين الحاجة إلى وضع كلمات مرور قوية على حساباتهم. وعندما سئل مستخدمون استطلعت آراؤهم في دراسة كاسبرسكي لاب في دولة الإمارات عن حسابات الإنترنت الثلاثة التي تتطلب أقوى كلمات المرور، اختار 47 في المئة منهم الحسابات المصرفية عبر الإنترنت، و35 في المئة اختاروا تطبيقات الدفع التي تشمل المحافظ الإلكترونية، و26 في المئة حسابات التسوق الإلكتروني.

لكن صعوبة تذكر كل كلمات المرور المُحكمة يعني ترجيح نسيان المستخدمين لها والعجز عن الوصول إلى حساباتهم. وقد أفاد ثلث المشاركين في الاستطلاع تقريباً 35 في المئة بعدم القدرة على استعادة كلمات المرور المنسية بسرعة، قائلين إن ذلك قد يؤدي إلى الشعور بالإحباط أو التوتر لا سيما مع عدم التمكن من مواصلة النشاط المعتاد جرّاء ذلك.

وعندما يتعلق الأمر بتخزين كلمة المرور، اعترف نصف المشاركين في الدراسة من دولة الإمارات بأنهم يخزّنون كلمات المرور بطريقة غير آمنة، في حين أقرّ 19 في المئة بأنهم يقومون بكتابتها في مفكراتهم فلا يضطرون إلى تذكرها، الأمر الذي يضع أمن حساباتهم على المحكّ.

الخيار الثاني لحلّ المعضلة: كلمات مرور ضعيفة يسهل اكتشافها واختراقها

يلجأ بعض المستخدمين إلى عادات غير آمنة في وضع كلمات المرور، كحلّ بديل لهذه المعضلة، وتجنباً للإحباط الناجم عن نسيان كلمات المرور القوية والطويلة؛ فعلى سبيل المثال، يضع 14 في المئة من المستخدمين في دولة الإمارات كلمة مرور واحدة فقط لجميع حساباتهم، وفق الدراسة، ما يسهّل حياتهم على الإنترنت، ويريحهم من عناء تذكّر كيفية الدخول إلى أي حساب. لكن ذلك قد لا يستمر إلا لحين حصول أحد مجرمي الإنترنت على كلمة المرور تلك وقيامه بالاستيلاء على جميع الحسابات وترك المستخدمين يعانون تبعات الكارثة ويعاينون أضرارها.

ووجدت دراسة كاسبرسكي لاب أن نسبة كبيرة بلغت 53 في المئة من المستخدمين الذين شملهم الاستطلاع في دولة الإمارات واجهوا تهديداً باختراق أحد حساباتهم على الإنترنت، أو عانوا اختراق حساب في الأشهر الاثني عشر الماضية. وأوضحت الدراسة أن أكثر الحسابات استهدافاً كانت البريد الإلكتروني بنسبة 51 في المئة، تلتها حسابات وسائل التواصل الاجتماعي بواقع 42 في المئة، فحسابات التسوق بنسبة 19 في المئة، وأخيراً الحسابات المصرفية بنسبة 12 في المئة.

الخيار الثالث لحلّ المعضلة

وترى كاسبرسكي لاب، أن على المستخدمين ألاّ يقصُروا الحلول على خيارين اثنين لحلّ معضلة كلمات المرور، فلا داعي للمساومة في هذا الأمر، بحسب أندري موكولا، رئيس قسم الأعمال التجارية للمستهلكين لدى كاسبرسكي لاب، الذي أكّد أنه سيكون بمقدور المستخدمين، إذا لجأوا إلى كلمات مرور قوية بطريقة يمكن تذكرها دائماً، الوصول إلى كل ما يحتاجون إليه متى ما أرادوا، والحفاظ في الوقت نفسه على أمن المعلومات الموجودة في حساباتهم، وأضاف: "هذا أمر مهم للمستهلكين الذين يريدون عيش حياتهم اليومية المعتادة بأمان، كإيجاد معلومات الاتصال بشخص ما، واستذكار مكان اجتماع معين، والفوز في لعبتهم المفضلة، والاطلاع على رسائل البريد الإلكتروني، وشراء شيء ما يحتاجون إليه، وأن يفعلوا ذلك في الوقت الذي يريدونه ومن دون تعريض معلوماتهم الشخصية لخطر القرصنة".

ولكن الصعوبة في تذكر كلمات المرور الآمنة تعني، وفق موكولا، أن المستخدمين "يواجهون معضلة كلمات المرور كل يوم، وغالباً ما ينتهي بهم المطاف بالتالي إلى نسيان كلمات المرور القوية أو وضع كلمات مرور بسيطة يسهل تذكرها، ولكن أيضاً يسهل كشفها واختراق الحسابات التي وُضعت لحمايتها". إلا أن الخبير الأمني أوضح أنه هناك خياراً ثالثاً يمكن أن يحقق للمستخدمين راحة البال، ويتمثل باستخدام حل برمجي يعمل بمثابة "مديرٍ لكلمات المرور" يسمح لهم بوضع كلمات مرور قوية من دون الحاجة لكتابتها في مفكرات أو تذكر سلاسلها المعقدة المؤلفة من حروف وأرقام ورموز خاصة

ويقوم Kaspersky Password Manager بتخزين جميع كلمات المرور الخاصة بالمستخدم في ما يشبه القبو الآمن، لمساعدته على استعادة السيطرة على هوياته المتناثرة في أرجاء الإنترنت ويحتاج المستخدم فقط إلى تذكّر كلمة مرور رئيسية واحدة من أجل الوصول إلى جميع حساباته، ليزيل عن كاهله احتمال الشعور بالتوتر جرّاء منعه من الوصول إلى حساب ما لأي سبب من الأسباب ويمكن للمستخدمين الوصول إلى كلمات المرور الخاصة بهم عن طريق أي جهاز، من خلال حساب My Kaspersky المجاني من كاسبرسكي لاب، بغضّ النظر عن الوقت أو المكان، ما يساعدهم في الحفاظ على الحسابات والمعلومات القيمة آمنة ومتاحة لأنفسهم فقط وتساعد ميزة التأليف التلقائي لكلمات المرور في هذا الحلّ على إنشاء كلمات مرور قوية تريح المستخدمين ولكن تتسبب بصداع مرهِق للقراصنة والمجرمين