

المركز الوطني للأمن السيبراني البريطاني يوصي بمفاتيح المرور بدلاً من كلمات المرور حيثما توفرت



لم يعد المركز الوطني للأمن السيبراني البريطاني يوصي بكلمات المرور حيثما تتوفر مفاتيح المرور، وينصح الشركات بجعلها الخيار الافتراضي للعملاء. ويرى تقريره الجديد أنها بأمان لا يقل عن كلمة مرور قوية مع التحقق بخطوتين.

- يوصي المركز، التابع لمقر الاتصالات الحكومية البريطاني (GCHQ)، بأن تكون مفاتيح المرور الخيار الأول للأفراد حيثما تدعمها الخدمة.
- يخلص تقرير تقني جديد إلى أن مفاتيح المرور بأمان لا يقل عن كلمة المرور القوية مع التحقق بخطوتين، وغالباً أعلى منها.
- ينصح المركز الشركات بتقديم مفاتيح المرور بوصفها خيار المصادقة الافتراضي للمستهلكين.
- إذا لم تدعم الخدمة مفاتيح المرور، يُنصح باستخدام مدير كلمات مرور مع إبقاء التحقق بخطوتين مفعّلاً.

• امتنع المركز العام الماضي عن التأييد بسبب تحديات في التطبيق، وقد تجاوزتها الصناعة بتقديمها.

أعلن المركز الوطني للأمن السيبراني البريطاني (NCSC)، التابع لمقر الاتصالات الحكومية (GCHQ)، أن مفاتيح المرور ينبغي أن تكون الآن الخيار الأول للأفراد في تسجيل الدخول إلى الخدمات الرقمية. ولم يعد يوصي بكلمات المرور حيثما يتوفر مفتاح مرور، لضعف قدرتها على الصمود أمام التهديدات الحديثة.

ما توصل إليه المركز

يخلص تقرير تقني نُشر خلال مؤتمر CYBERUK إلى أن مفاتيح المرور بأمان لا يقل عن أقوى كلمة مرور مقترنة بالتحقق بخطوتين، وهي في الغالب أكثر أماناً. ويشير المركز إلى أن معظم الأضرار السيبرانية التي تصيب الأفراد تبدأ بسرقة بيانات الدخول أو اختراقها، وأن مفاتيح المرور شديدة المقاومة للتصيد ولا يمكن اعتراضها أو إعادة استخدامها أو تخمينها.

وكان المركز قد امتنع العام الماضي عن تأييدها بسبب تحديات في التطبيق، أما اليوم فقد سمح تقدم الصناعة بالتوصية بها للجمهور، وللشركات بوصفها خيار المصادقة الافتراضي للمستهلكين.

نقاط عملية

ويذكر المركز مزايا في سهولة الاستخدام، منها إتمام الدخول أسرع بما يصل إلى ثماني مرات مقارنة باسم المستخدم وكلمة المرور ورمز التحقق، وتخفيف إرهاق كلمات المرور. ويشير لمقدمي الخدمات إلى وفورات عند الاستغناء عن التحقق عبر الرسائل النصية القصيرة التي تتحمل تكلفة إضافية. وإذا لم تدعم الخدمة مفاتيح المرور، ينصح باستخدام مدير كلمات مرور وإبقاء التحقق بخطوتين.

الإرشاد موجّه لمصادقة المستهلكين. ويمكن للمؤسسات في المملكة اعتباره مرجعاً مفيداً عند مراجعة خيارات تسجيل الدخول لعملائها، مع تقييم ملاءمته لمتطلباتها التنظيمية.

ما يجب فعله الآن

1. مراجعة التطبيقات الموجهة للعملاء والموظفين لمعرفة ما يدعم مفاتيح المرور (FIDO2/WebAuthn).
2. دراسة تقديم مفاتيح المرور خياراً افتراضياً أو مفضلاً لتسجيل دخول العملاء إلى جانب الضوابط الحالية.
3. التحقق من توافق اعتماد مفاتيح المرور مع متطلبات المصادقة لدى الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي قبل تعديل السياسات.
4. تقييم تكلفة ومخاطر التحقق عبر الرسائل النصية القصيرة بوصفه مرشحاً للاستبدال.
5. تشجيع استخدام مديري كلمات المرور وإبقاء المصادقة متعددة العوامل مفعّلة للخدمات التي لا تدعم مفاتيح المرور.