عملية احتيال تهدد الخصوصية والأمان على منصات التواصل الاجتماعي

انتشرت عملية احتيال جديدة على منصات التواصل الاجتماعي، تعد المستخدمين بالكشف عن كلمات مرور شبكات "WiFi" الخاصة مقابل خطوات بسيطة.

وهذه الخدعة، التي لاقت رواجًا واسعًا على "فيسبوك"، ليست عديمة الفائدة فقط، بل تشكل تهديدًا خطيرًا لأمن الأجهزة والمعلومات الشخصية.

كيف تعمل الخدعة؟

تبدأ العملية بتعليقات مزيفة يوصي أصحابها المستخدمين بالبحث عن مصطلحات مثل "KEK3" أو "GOG6" على Google، ما يؤدي إلى صفحات إلكترونية تدّعي القدرة على فك تشفير مفاتيح شبكات "WiFi".

وتُقدم هذه الصفحات واجهة خادعة، تسأل المستخدمين أسئلة تبدو احترافية، مثل نوع الشبكة وقوة الإشارة.

وفي الخطوة الأخيرة، يُطلب من المستخدمين مشاركة رسالة ترويجية في 15 تعليقًا على فيسبوك لاستكمال الإجراء، لا تساهم هذه الخطوة فقط في نشر الاحتيال على نطاق أوسع، بل تنتهي بإعادة توجيه المستخدم

إلى صفحات ضارة قد تحاول تثبيت برامج خبيثة على الجهاز.

الأثر الأمني

وتشير التقارير إلى أن هذه الصفحات تحتوي على تعليمات برمجية خبيثة، قد تؤدي إلى سرقة المعلومات الشخصية أو اختراق الحسابات، أو حتى فتح الباب أمام الوصول غير المصرح به إلى الشبكات.ورغم أن برامج مكافحة الفيروسات الحديثة قد تعيق بعض هذه التهديدات، فإن تجاهل التحذيرات يزيد مخاطر الإصابة.كيفية تجنب الوقوع في الفخ

يجب أن يكون المستخدم حذرًا من الوعود الزائفة التي تبدو جيدة للغاية، والامتناع عن مشاركة المحتوى المشبوه على وسائل التواصل، واستخدام برامج مكافحة الفيروسات الحديثة لتجنب البرمجيات الضارة.

كما يجب التثقف حول أساليب الاحتيال الرقمي لتجنب الوقوع ضحية لها، والتحقق دائمًا من شرعية الروابط قبل فتحها.