تحذير هام لمستخدمي □□□□□ من عملية احتيال خطيرة

نخيل نيوز ـ متابعة

تحذر غوغل مستخدمي خدمة □□□□□ من تزايد محاولات الاحتيال الإلكتروني التي تنتحل إشعارات أمنية رسمية، بهدف خداع الضحايا وسرقة بياناتهم الشخصية وكلمات المرور.

وتوضح الشركة أن بعض المستخدمين يتلقون رسائل أو تنبيهات على هواتفهم تدّعي وجود "نشاط مشبوه" في حساباتهم، لكنها في الواقع قد تكون رسائل مزيفة صممها مخترقون لإيهام الضحية بضرورة اتخاذ إجراء عاجل.

وكشف أحد مستخدمي موقع "ريدت" أنه تلقى رسالة تبدو وكأنها من □□□□□ تفيد بأن حسابه تم اختراقه ويحتاج إلى استعادة فورية. وأضاف أنه سبق أن تلقى تنبيهات مشابهة تزعم وجود محاولات تسجيل دخول من دول مختلفة مثل فنزويلا وبنغلاديش.

لكن تبين لاحقا أن هذه الرسائل كانت جزءا من عملية تصيّد احتيالي، حيث تم خداع المستخدم للنقر على رابط قاده إلى صفحة مزيفة تشبه موقع غوغل، بهدف سرقة كلمة المرور ورقم الهاتف.

وتحذر غوغل من أن المهاجمين أصبحوا يقلّدون رسائلها الأمنية الرسمية بشكل متقن لإثارة الذعر ودفع المستخدمين إلى التصرف بسرعة دون تحقق. وتؤكد الشركة أنها لا تطلب أبدا كلمات المرور أو البيانات الشخصية عبر روابط في رسائل غير رسمية.

وفي ضوء هذه التهديدات، توصي غوغل المستخدمين بعدم النقر على أي روابط واردة في رسائل تحذيرية، والتوجه مباشرة إلى حساباتهم عبر الموقع الرسمي للتحقق من أي تنبيهات أمنية.

كما تنصح الشركة بمراجعة "الأحداث الأمنية الأخيرة" داخل إعدادات الحساب، والتي تُظهر أي محاولات تسجيل دخول غير معتادة مع تفاصيل الموقع والوقت، ما يساعد على كشف النشاط المشبوه.

وفي حال ظهور أي نشاط غير مألوف، يمكن للمستخدم اختيار "تأمين الحساب" واتباع خطوات تغيير كلمة المرور فورا.

ويشدد خبراء الأمن على أهمية تفعيل المصادقة الثنائية، وهي ميزة تضيف طبقة حماية إضافية عبر إرسال رمز تحقق إلى الهاتف أو تطبيق المصادقة عند تسجيل الدخول، ما يجعل اختراق الحساب أكثر صعوبة.

وتؤكد غوغل أن الهجمات الإلكترونية على مستخدمي □□□□□ تتزايد عالميا، وأن المحتالين يعتمدون بشكل متكرر على رسائل مزيفة تحمل عبارات مثل "تم منع تسجيل دخول مشبوه" لإقناع الضحايا بالنقر على روابط خبيثة.

كما ينصح خبراء الأمن باستخدام كلمات مرور قوية وفريدة لكل موقع، وتجنب إعادة استخدامها، لأن ذلك يقلل من احتمالية اختراق عدة حسابات في حال تسريب واحدة منها.

ويختتم مختصون تحذيراتهم بالتأكيد على أن أكثر وسائل الحماية فعالية اليوم هي الوعي الرقمي، والتحقق من مصدر أي رسالة قبل اتخاذ أي إجراء.