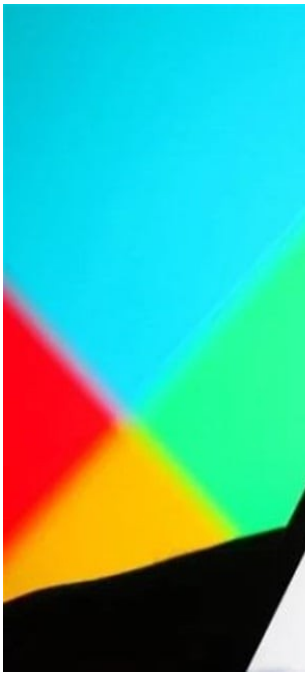
"غوغل" تكشف عن هجوم تصيد احتيالي معقد يهدد حسابات المستخدمين



شهد مستخدمو خدمة البريد الإلكتروني "Gmail" موجة متصاعدة من هجمات التصيد الاحتيالي في الأشهر الأخيرة، والتي تزداد تعقيدا يوما بعد يوم.

وأكدت "غوغل" تعرضها لهجوم "متطور" يستهدف جميع مستخدمي Gmail البالغ عددهم "1.8" مليار مستخدم.

وهذه الهجمات التي تستهدف سرقة كلمات المرور تمكنت من خداع حتى أكثر المستخدمين حذرا، حيث تظهر الرسائل الاحتيالية وكأنها صادرة فعلا عن غوغل، مع عناوين بريدية تبدو رسمية تماما وتتجاوز حتى فحوصات الأمان المعتادة.

والقصة بدأت عندما لاحظ نيك جونسون، وهو مطور في منصة "إيثريوم" للعملات الرقمية، رسالة غريبة في صندوق بريده.

وادعت الرسالة التي بدت، وكأنها إشعار رسمي من غوغل أنه:"تلقى استدعاء قضائيا، ودعته للنقر على

رابط لمعرفة التفاصيل، وما أثار دهشة جونسون أن الرسالة مرت بجميع فحوصات الأمان، بما في ذلك توقيع DKIM الذي يفترض أن يضمن صحة محتوى البريد الإلكتروني، دون أن تظهر أي تحذيرات من Gmail".

وعند النقر على الرابط، وجد جونسون نفسه أمام صفحة تطابق تماما واجهة غوغل الرسمية، مع خيارات مثل "تحميل مستندات إضافية" أو "عرض القضية".

وكل التفاصيل كانت مصممة بعناية لخداع المستخدم وجعله يدخل بيانات اعتماده دون شك. ولحسن الحظ، أدرك جونسون الخدعة قبل فوات الأوان، لكن كثيرين لم يكونوا محظوظين مثله.

وردا على هذه الهجمات المتطورة، خرجت غوغل بتصريح مطمئن أكدت فيه أن:"المستخدمين الذين يقعون ضحية هذه الخدع يمكنهم استعادة حساباتهم خلال فترة تصل إلى أسبوع، بشرط أن يكونوا قد سجلوا مسبقا وسائل استرداد مثل رقم هاتف أو بريد إلكتروني بديل".

وهذه الآلية تسمح للمستخدمين بالإجابة على أسئلة الأمان وإثبات هويتهم لاستعادة الحساب المسروق.

ولكن غوغل شددت على أن:"الوقاية تبقى أفضل من العلاج. وأوصت المستخدمين باتباع إجراءات أمان صارمة، أبرزها تفعيل المصادقة الثنائية واستخدام "مفاتيح المرور" (Passkeys) التي تعتبر أكثر أمانا من كلمات المرور التقليدية".

وهذه المفاتيح المولدة من النظام تتميز بأنها لا يمكن تخمينها أو سرقتها بسهولة، كما أنها مرتبطة بالجهاز نفسه، ما يجعلها عديمة الفائدة إذا حصل عليها المخترقون.

وأما العلامات الدالة على رسائل التصيد الاحتيالي، فأبرزها استخدام العناوين العامة مثل "عزيزي العميل"، وخلق حالة من الإلحاح المصطنع حول مشكلة مزعومة تتطلب إجراء فوريا، وإدراج روابط تبدو رسمية لكنها في الحقيقة تقود إلى مواقع مزيفة.

وتؤكد غوغل أنها:"لن تطلب أبدا من المستخدمين مشاركة كلمات المرور أو رموز التحقق عبر البريد الإلكتروني أو الهاتف".