تحذير... هجوم تصيد خطير يهدد مستخدمي "جيميل" ويسرق بياناتهم

يواجه Gmail أكبر منصة بريد إلكتروني مجانية في العالم تهديدًا خطيرًا، فقد حذر تقرير نشر على صحيفة Sun The ، من رسائل البريد الإلكتروني الاحتيالية التي قد تخدع الأفراد في تمرير تفاصيل الحساب مباشرة إلى أيدي المتسللين

وأكد التقرير أنه:"تنشيط مرشح البريد العشوائي يعد الطريقة الرئيسية لمنع البريد الإلكتروني الاحتيالية، منوهًا أنه في حالة تركك لرسائل البريد الإلكتروني الاحتيالية التي تبدو وكأنها صفحة ويب عادية دون حظر، فقد يتم إرسالها مباشرة إلى صندوق الوارد مما يؤدي إلى تسجيل دخول المستخدم إلى حسابه بشكل طبيعي".

ومن جانبه، قال أحد خبراء الأمن الرقمد:"يمكن أن تكون هذه الهجمات قاتلة للشركة"، فقد صرح جيمس نايت إذا تم استلام هذه الرسائل الإلكترونية، فيجب على الأشخاص توخي الحذر الشديد فيما يفتحونه والروابط التي ينقرون عليها، كما عليك تذكر، فقط لأنها تبدو مثل تسجيل الدخول إلى Gmail أو Office.

وحذر أنه:"على الرغم من طبقة الدفاع الإضافية المفترضة لحساب ما، فإن مجموعة التصيد الاحتيالي تقدم طريقة لخداع الضحية، وهذا يعني أن المتسللين لا يقتصرون على معلومات الحساب فحسب، بل يمكنهم أيضًا اختيار الوصول إلى أسماء المستخدمين وكلمات المرور وأرقام بطاقات الائتمان والمعلومات المصرفية والمزيد".

وفي السابق كان يُعتقد أن أدوات التصيد الاحتيالي لا يمكن أن تكون فعالة إلا من خلال إرسال روابط مشبوهة في رسائل البريد الإلكتروني، لكن Astaroth تقدم طريقة بديلة.

ويُقال إن بائعي الويب المظلم يعززون البرامج الضارة من خلال ستة أشهر من التحديثات التي يتم تسليمها من خلال تطبيق المراسلة المجهول Telegram.

ولسوء الحظ، هذا يعني أن Microsoft قد تحتاج إلى مواصلة عملها للبقاء في صدارة هذا النوع من الهجمات، ويأتي ذلك بعد تحذير عاجل تم إصداره لمستخدمي Gmail وOutlook من الهجوم الذي يسرق كلمات المرور وتفاصيل الحساب، حيث يمكن للصفحة المزيفة أن "تعكس" صفحة تسجيل دخول شرعية بحيث لا توجد تحذيرات، وهذا يسمح للمهاجمين بتجاوز حماية المصادقة الثنائية "بسرعة ودقة ملحوظة".

لذا، حتى إذا تم إرسال رمز SMS لك للوصول إلى حساب بريدك الإلكتروني، يمكن للمهاجمين اعتراضه.