مجرمون سيبرانيون يستغلون الصراع في فلسطين لينشروا رسائل ومواقع إلكترونية احتيالية

الاثنين 23 أكتوبر 2023 05:48 م

رصدت شركة كاسبرسكي احتيالاً يستغل الصراع في فلسطين ورغبة الناس في مساعدة المتضررين منه لخداع الضحايا المحتملين، حيث يوهم المجرمون السيبرانيون الضحايا بأنهم يجمعون التبرعات ليسرقوا الأموال منهم. حتى الآن، قام المجرمون بنشر أكثر من 500 رسالة إلكترونية احتيالية وأنشؤوا مواقع إلكترونية احتيالية لتسريع عملية تحويل الأموال. لذا تحث كاسبرسكي المستخدمين على توخي الحذر واتخاذ خطوات وقائية للتحقق من موثوقية متلقي تبرعاتهم.

كثيراً ما تظهر أعمال خيرية مزيفة أو احتيالية، وغالباً ما تحدث عبر استغلال الكوارث الحقيقية أو حالات الطوارئ لاستدراج الضحايا. ومن المؤسف أن الصراع في فلسطين يُعد واحداً من هذه الحالات المُستغلة. حيث لاحظ خبراء كاسبرسكي تزايداً كبيراً في عدد الرسائل الإلكترونية الاحتيالية المُرسلة باللغة الإنجليزية، التي تخدع المستخدمين لكسب تبرعات يظن الضحايا أنهم أرسلوها إلى المتضررين من الصراع. إذ اكتشفت حلول كاسبرسكي الأمنية أكثر من 540 رسالة إلكترونية من هذا القبيل.

ولاستغلال تعاطف الناس مع المتضررين ورغبتهم في المساعدة، يستخدم المحتالون تقنيات الهندسة الاجتماعية المتقدمة في محاولة لاستدراج الضحايا لتقديم تبرعات مزيفة. إذ ينتحل المحتالون هوية منظمات خيرية ويستخدمون لغة مؤثرة لإغراء المستخدمين للنقر على رابط ينقلهم إلى موقع إلكتروني احتيالي يطلب منهم التبرع. ويجدر ذكر أن هذه الرسائل المخادعة تأتي من عناوين مختلفة.

في هذا الشأن، يقول أندريه كوفتون، وهو خبير أمني في شركة كاسبرسكي: "يحاول المحتالون أن يكتبوا إصدارات نصوص مختلفة في هذه الرسائل الإلكترونية لتتجنب فلاتر الرسائل المزعجة. على سبيل المثال، يستخدمون عبارات متنوعة تحث على التبرع مثل: "نستجدي تعاطفكم وإحسانكم" أو "نرجو طيبة قلوبكم وكرمكم"، ويستبدلون كلمات مثل: "المساعدة" بمرادفات مثل: "الدعم" و"الإعانة" وما إلى ذلك. كما يقومون بتغيير الروابط وعناوين المرسِلين باستمرار. ومع ذلك، تحمي حلول الأمن السيبراني القوية من هذه المناورات".

تقود الروابط المُدرجة في هذه الرسائل إلى موقع إلكتروني احتيالي يقدم شرحاً بسيطاً عن الصراع، ويعرض صوراً، ويشجع المستخدمين على إرسال التبرعات. ويسهّل المحتالون تحويل الأموال عن طريق تقديم خيارات للدفع بعملات مشفرة مختلفة مثل: البيتكوين، وإيثريوم، وتيثر، ولايتكوين.

بالإضافة إلى ذلك، اكتشف خبراء كاسبرسكي صفحات إلكترونية احتيالية أخرى تشترك بعناوين المحفظات نفسها التي يستخدمها المحتالون، إذ تدّعي هذه الصفحات أنها تجمع المساعدات لمجموعات مختلفة في منطقة النزاع.

وصايا خبراء كاسبرسكي لتجنب هذه العمليات الاحتيالية:

للأسف، يمكن أن تتكاثر مثل هذه الصفحات الاحتيالية بسرعة، وتظهر بتصاميم مختلفة لاستهداف مجموعات متنوعة. لذلك، يُفضَّل فحص صفحات التبرع بدقة قبل تحويل الأموال؛ لتجنب عمليات الاحتيال. فغالباً ما تفتقر المواقع المزيفة إلى المعلومات الأساسية عن منظمي الأعمال الخيرية، أو المستفيدين منها، أو الوثائق الشرعية، أو طرق إنفاق التبرعات. يجدر بك تنفيذ التدابير الأمنية التالية؛ لتجنب هذه العمليات:

تحقق من موقع المنظمة الخيرية ومعلوماتها الثبوتية، فجميع المنظمات الخيرية المشروعة مسجلة. يمكنك التأكد من معلومات المنظمة الثبوتية عن طريق البحث عنها في قاعدة بيانات معروفة.

تواصل مباشرة مع المنظمات الخيرية التي ترغب في التبرع أو تقديم الدعم عبرها. وللتبرع عبر الإنترنت، اطبع عنوان موقع المنظمة الخيرية يدوياً بدلاً من النقر على رابط.

في حال دارت شكوكك حول المنظمة التي قمت بفحصها، اعتمد المنظمات المعروفة التي تقدم الدعم الإنساني مثل: وكالات الإغاثة التابعة للأمم المتحدة.

تذكر أنه ليس مرجحاً أن يتصل بك المتضررون مباشرة لطلب الدعم، وخاصة إن كانوا غرباء عنك؛ لذا، تذكَّر أن تتوخى الحذر من مثل هذه الطلبات.

انتبه جيداً. فقد يبدو الموقع الإلكتروني المزيف مطابقاً تقريباً لموقع خيري حقيقي، وقد يكون الفارق الوحيد بينهما هو وجود معلومات

تحدد وجهة التبرعات. وغالباً ما يشير وجود الأخطاء الإملائية أو النحوية في المواقع الإلكترونية إلى كونها مزيفة.
توخَّ الحذر عند التبرع عبر منصات التواصل الاجتماعي، إذ تُعد منصات التواصل الاجتماعي وسيلة مفيدة لتطلب المنظمات الخيرية عبرها التبرعات. لكن لا تفترض أن أي طلب تبرعات عبر فيسبوك، أو إكس (تويتر سابقاً)، أو إنستاجرام، أو يوتيوب هو طلب شرعي لمجرد إعجاب أحد أصدقائك به أو مشاركته. خذ الوقت الكافي للتحقق من المنظمة قبل التبرع من خلالها.