

تحذير من عمليات الاحتيال في الحجوزات السياحية في موسم العطلات



دبي: «الخليج»

يسعى المحتالون عبر الإنترنت لاستغلال الإقبال المتزايد على موسم العطلات، لاسيما مع بلوغه الذروة، وفي ضوء بحث المسافرين في جميع أنحاء العالم عن أنسب الوجهات لقضاء العطلة وأرخص أماكن الإقامة وأفضل الأسعار لرحلات الطيران. لاحظ باحثو «كاسبرسكي» تزايد محاولات الاحتيال، والمتمثلة بنشر العديد من صفحات التصيد على الويب تحت ستار خدمات السفر، كحجوزات الطيران والفنادق. ويعرض الباحثون بعض مخططات الاحتيال المنتشرة التي تستقطب الضحايا، والنصائح المفيدة في التخطيط لعطلة آمنة، في سبيل مساعدة المسافرين على تجنب الوقوع ضحايا لعمليات الاحتيال.

بائعو التذاكر المزيفة •

غالباً ما يهتم عشاق السفر بالحصول على صفقة جيدة عند سعيهم لشراء تذكرة الطائرة أو القطار. وهناك العديد من مواقع الويب المزيفة التي تزعم أنها تتيح للمستخدمين فرصة شراء تذاكر طيران رخيصة، وعادةً ما تكون هذه المواقع صفحات تصيد متقنة الصنع تحاكي خدمات شركات الطيران الشهيرة ومواقع بيع تذاكر الطيران الرسمية المعروفة،

بل إن بعضها يعرض تفاصيل الرحلات الحقيقية التي يحصلون عليها من مواقع رحلات الطيران وحجوزات الفنادق. وبالطبع فإن القائمين على هذه المواقع يسرقون أموال مستخدميها ويستغلون معلوماتهم الشخصية في أغراض خبيثة، كبيع التفاصيل المصرفية ومعلومات التعريف إلى جهات أخرى على شبكة الإنترنت المظلمة.

• سحبات وهمية

هناك أيضاً الكثير من الصفحات المزيفة التي تحاول جذب المسافرين بسحوبات وهمية على تذاكر طيران وبطاقات هدايا، حيث يُمنح المستخدمون فرصة المشاركة في استطلاع قصير يدخلون فيه بياناتهم الشخصية مقابل الحصول على خصم كبير على تذكرة طيران مزعومة. وينتهي الأمر بوصول المعلومات الشخصية للضحايا وتفاصيل بطاقتهم المصرفية في أيدي المحتالين من دون مقابل، كما هو الحال مع كلّ العروض التي تبدو جيدة إلى درجة يصعب تصديقها.

وعلاوة على ذلك، ينتهي الاستطلاع عادةً بطلب توزيع الموقع بين الأصدقاء لاستلام الجائزة. وفي مثل هذه الحالات، يستخدم مجرمو الإنترنت الضحايا أنفسهم كأداة لتوسيع عملياتهم الاحتيالية وجعلها تبدو أكثر مصداقية، نظراً لورود الروابط المؤدية إليها من أشخاص يعرفهم المستخدمون. وإذا تتبع المستخدم الرابط بعد ذلك وحاول الحصول على جائزته، فغالباً ما يجد أن عليه سداد مبلغ من المال أولاً، وما إن يفعل حتى يختفي المجرمون وتتبخر الآمال بكسب أي شيء.

• إيجارات وهمية

وتتضمن التكتيكات الشائعة لخداع المسافرين خدمات تأجير وهمية لمواقع الإقامة تقدّم عروضاً مغرية كإقامة في شقة فاخرة من غرفتي نوم بالقرب من وسط عاصمة أوروبية مقابل 500 يورو فقط شهرياً، أو استئجار منزل كامل من أربع غرف نوم مع مسبح ومدفأة مقابل 1,000 يورو فقط في الشهر. بل إن هناك تقييمات للمكانين تصف قضاء العطلة فيهما بالرائع، ما يشجّع المسافرين على الدفع لحجز الإقامة، لكن ينتهي الحال بذهاب أموالهم سدى إلى المحتالين.

• صفحة تصيد

وأشار ميخائيل سيتنيك خبير الأمن لدى «كاسبرسكي»، إلى صعوبة التخطيط لقضاء إجازة والحصول على أنسب الأسعار لتذاكر السفر وأماكن الإقامة، مؤكداً أن المحتالين يستغلون هذا الأمر في جذب المستخدمين الذين سئموا صعوبة العثور على صفقات مناسبة. وقال: «عاد السفر إلى طبيعته بعد عامين من القيود التي فرضتها الجائحة على العالم، والأمر نفسه ينطبق على عمليات الاحتيال المتعلقة بالسفر التي تستهدف المسافرين بخدمات الحجز الوهمية للرحلات وأماكن الإقامة. وبالإمكان تجنّب هذه المحاولات تماماً، بالتشكيك في العروض السخية جداً؛ إذ ينبغي الابتعاد عن العرض إذا كان يبدو جذاباً إلى درجة يصعب تصديقها».

ويوصي خبراء كاسبرسكي المسافرين باتباع التدابير التالية لحماية أنفسهم أثناء التخطيط لقضاء إجازة:

*التدقيق في رابط الموقع قبل إدخال أية معلومات حساسة كبيانات تسجيل الدخول وكلمة المرور. فإذا كان هناك خطأ يجعله لا يبدو مثل العنوان الأصلي المفترض، أو أن هناك بعض الرموز الخاصة في URL كتابي ما في تهجئة عنوان العنوان بدلاً من الأحرف، فينبغي الخروج من الموقع. وفي حال استمرار الشكّ يمكن التحقق من شهادة الموقع بالنقر URL على أيقونة القفل الموجودة على يسار عنوان

تجنّب إجراء حجوزات السفر والإقامة إلا من خلال المواقع الرسمية التابعة لمقدمي الخدمات الموثوق بهم. ويوصى بإدخال عنوان موقع الويب يدوياً في شريط العناوين.

* تجنّب النقر على الروابط الواردة من مصادر غير معروفة (سواء برسائل البريد الإلكتروني أو تطبيقات المراسلة أو شبكات التواصل الاجتماعي).

* زيارة الموقع الرسمي لشركة السفر أو الطيران للتأكد من أنها تقدّم العرض السخي المزعوم في رسالة البريد الإلكتروني أو على وسائل التواصل الاجتماعي. مع وجوب التحقق بعناية من الروابط التي يقود الإعلان إليها.

* استخدام حل أمني جيّد للحماية من رسائل البريد الإلكتروني غير المرغوب فيها وهجمات التصيد.

"حقوق النشر محفوظة" لصحيفة الخليج. © 2024