

رقم قياسي.. 66 مليار دولار إنفاق المستهلكين في المنطقة خلال رمضان



أكدت دراسة بحثية صادرة عن بروف بوينت أن 65% فقط من 20 أفضل متجر للتجزئة في الشرق الأوسط قد طبقت الحد الأدنى من مصادقة الرسائل المستندة إلى المجال وإعداد التقارير والمطابقة، لافتةً إلى أن 35% لا تتخذ أي خطوات لمنع الهجمات السيبرانية. وأشارت الدراسة إلى أن 6 فقط من بين 20 أفضل متجر تجزئة (30%) تطبق سياسة الأكثر صرامة والموصى بها «الرفض» المعمول بها، ما يعني أن 70% لا تحظر مسبقاً رسائل البريد DMARC الإلكتروني الاحتيالية لمنعها من الوصول إلى المستهلكين.

ومع بداية شهر رمضان الذي يشهد المزيد من العروض المخفضة، من المتوقع أن ينفق المستهلكون رقمًا قياسيًا بقيمة 66 مليار دولار على تجارة التجزئة في منطقة الشرق الأوسط وشمال إفريقيا هذا العام. وسوف يواصل ملايين المتسوقين البحث على الإنترنت وسيصلهم الكثير من رسائل البريد الإلكتروني التي تحمل صفقات لا تضاهاى. وهذا بدوره يفسح المجال أمام قراصنة الإنترنت لخداع المتسوقين.

بروتوكول المصادقة على البريد الإلكتروني، في حماية أسماء النطاقات من الهجمات «DMARC» تسهم تقنية السبرانية، وهي تمثل إحدى أبرز الوسائل التي تستند إليها المؤسسات والشركات لحماية رسائل البريد الإلكتروني على هوية المرسل قبل DMARC الواردة والصادرة من التصيد الاحتيالي وغيرها من الأنشطة الاحتيالية. تصادق تقنية السماح للرسالة بالوصول إلى البريد الإلكتروني المقصود؛ بينما يشكل «الرفض» المستوى الأكثر صرامة، والموصى به إعداد وسياسة تمنع رسائل البريد الإلكتروني الاحتيالية من الوصول إلى البريد الإلكتروني «DMARC» به لحماية المستهدف.

وقال إميل أبو صالح، المدير الإقليمي لمنطقة الشرق الأوسط وإفريقيا لدى بروف بوينت: «يشهد قطاع التجزئة في الشرق الأوسط الكثير من الحركة والنشاط، وقد أوضحت الإحصاءات أن أرباح قطاعات البقالة والملابس وتجارة التجزئة الإلكترونية في دول مجلس التعاون الخليجي تتجاوز متوسط الأرباح العالمية لهذه الأنشطة. في الواقع كان إنفاق المستهلكين في السعودية الأعلى في المنطقة بأكثر من 16 مليار دولار. وفي ظل هذا الزخم المتنامي، يجب على تجار «التجزئة في الشرق الأوسط حماية عملائهم وعلامتهم التجارية من الاحتيال عبر البريد الإلكتروني».

وتوصي بروف بوينت المستهلكين باتباع بعض النصائح للبقاء آمنين عبر الإنترنت أثناء التسوق لا سيما خلال شهر رمضان للحصول على صفقات موسمية

استخدم كلمات مرور قوية: لا تعتمد إلى استخدام نفس كلمة المرور مرتين. ضع في اعتبارك استخدام تقنية مدير-1 كلمات المرور لجعل تجربتك عبر الإنترنت سلسة، مع الحفاظ على أمانك. استخدم المصادقة متعددة العوامل لمستويات إضافية من الأمان

احترس من المواقع «الشبيهة»: ينشئ قراصنة الإنترنت مواقع «شبيهة» بمواقع العلامات التجارية المألوفة. قد تباع-2 هذه المواقع الاحتيالية سلعاً مزيفة (أو غير موجودة)، أو تتسبب في تنزيل البرمجيات الخبيثة، أو سرقة الأموال أو بيانات الاعتماد

تفادي هجمات التصيد الاحتيالي المحتملة وهجمات التصيد الاحتيالي: تؤدي رسائل التصيد الاحتيالي إلى مواقع-3 إلكترونية غير آمنة تجمع البيانات الشخصية، مثل بيانات الاعتماد وبيانات بطاقة الائتمان. احترس أيضاً من رسائل التصيد الاحتيالي عبر الرسائل القصيرة - مثل «الرسائل القصيرة» - أو الرسائل عبر وسائل التواصل الاجتماعي

لا تنقر على الروابط: انتقل مباشرةً إلى مصدر الصفقة المعلن عنها عن طريق كتابة عنوان موقع ويب معروف-4 مباشرةً في متصفحك. للحصول على رموز العروض الخاصة، أدخلها عند الخروج لمعرفة ما إذا كانت أصلية

تحقق قبل الشراء: قد يكون من الصعب اكتشاف الإعلانات والمواقع الإلكترونية وتطبيقات الجوال الاحتيالية. عند-5 تنزيل تطبيق جديد أو زيارة موقع غير مألوف، خذ وقتاً لقراءة التقييمات عبر الإنترنت وأي شكاوى من العملاء