

حماية الأعمال وضمان جذب العملاء

الكاتب



نيل فيرنانديز

نيل فيرنانديز *

Visa يشهد قطاع التجارة الرقمية نمواً تصاعدياً متواصلاً منذ إجراء أول طلب إلكتروني لشراء فطيرة بيتزا عبر شبكة في 11 أغسطس/ آب 1994، وتشكل طلبات البيتزا عبر الإنترنت حالياً جزءاً صغيراً من حجم التجارة الإلكترونية العالمية. وكما هو معلوم، فقد ساهمت جائحة «كوفيد-19» العالمية مطلع العام الماضي، بتحويلات كبيرة في سلوك المستهلكين في كل أنحاء العالم، حيث اتجهت أعداد متزايدة إلى منصات التجارة الإلكترونية لتلبية حاجتها الملحة إلى المشاركة مع «شرطة Visa تجربة تسوق لاتلامسية مريحة. وقد أظهرت نتائج دراسة «ابق آمناً 2021» التي كشفت عنها دبي» و«اقتصادية دبي» نمواً بمعدل الضعف في مستويات إقبال المستهلكين على المدفوعات الرقمية (البطاقات اللاتلامسية والمحافظ الرقمية) بمعدل 98% منذ بدء الجائحة

وساهم ارتفاع معدلات استخدام المدفوعات الرقمية بمنافع عدة للمستهلكين، لكنه ترافق بمخاوف عدة أبرزها ارتفاع وتيرة الجرائم الإلكترونية. ففي حين يمضي العالم قدماً تجاه خفض حدة تداعيات الجائحة، سارع المحتالون عبر الإنترنت إلى اغتنام هذه الفرصة وابتكار أساليب احتيال جديدة لاستغلال مخاوف المستهلكين لارتكاب عمليات الاحتيال وسرقة أموالهم

وفي دولة الإمارات، قال 39% من المستهلكين إنهم تعرضوا لمحاولات الاحتيال عبر الإنترنت، بينما تعرض نحو الربع (27%) للتصيد الاحتيالي، وأشارت نسبة تقل عن الخمس (19%) إلى التعرض لمحاولات احتيال متعلقة بالبطاقة الائتمانية. ويعني ذلك أن المحتالين يجدون سهولة في الحصول على المعلومات الشخصية واختراق البيانات عبر مواقع الشركات التي يعتمد عليها العملاء ويثقون بها

ويسهم الابتكار التقني في إدارة هذه التهديدات، كما أن المستهلكين أصبحوا أكثر معرفة بما ينبغي فعله لتجنب شبك المحتالين.

فمن اللافت أن وتيرة الهجمات الإلكترونية المتزايدة لم تؤثر في ثقة المستهلكين بالمدفوعات الرقمية. فقد أظهرت نتائج ارتفاع مستويات الثقة لدى 63% من المستهلكين في دولة الإمارات تجاه استخدام البطاقات اللاتلامسية Visa دراسة والمحافظ الرقمية بفضل الابتكارات المتواصلة للارتقاء بأمان المدفوعات الرقمية.

ونظراً لإقبال المستهلكين المتزايد في دولة الإمارات على التسوق عبر الإنترنت واعتماد المدفوعات الرقمية، فقد أصبح هؤلاء يتوقعون تجربة سلسلة وأمنة للتسوق عبر الإنترنت. لذا يتعين على التجار ضمان اطمئنان المستهلكين عند التسوق عبر منصاتهم والتأكد من فاعلية أنظمة الدفع وتوفير أعلى درجات الحماية لبيانات عملائهم من المحتالين، وإلا سيتعرضون لخسارة العديد من الفرص.

وقال نحو 4 من كل 10 مستهلكين مشاركين في الدراسة إنهم يفضلون تغيير المتجر أو التسوق من موقع إلكتروني آخر عند تأخر عملية الدفع عبر الإنترنت.

وقال مستهلك من كل 2 إنه سيتخلى عن عربة التسوق في حال واجه تأخيراً أو خطأ في عملية المصادقة أثناء التسوق عبر الإنترنت.

وسواء كانوا يتطلعون للانتقال بأعمالهم إلى الإنترنت، أو يعملون بالفعل عبر مواقع التجارة الإلكترونية، فمن الأهمية بمكان أن يدرك التجار العوامل التي تسهم بتعزيز ثقة المستهلكين. فقد أظهرت الدراسة أن مواقع التجارة الإلكترونية التي توفر تقييمات العملاء (51%)؛ وتقدم مجموعة متنوعة من خيارات الدفع (41%) وسهولة الاسترداد (42%) حققت أداءً أفضل على صعيد اكتساب مستويات مرتفعة من الثقة بين المستهلكين.

فما هي الخطوات المطلوبة من التجار لحماية أعمالهم وعملائهم؟

التحديث المتواصل لكل البرمجيات: احرصوا على تحديث جميع المنصات الرقمية أو التطبيقات المثبتة لديكم. إذ يعمل المحتالون وقراصنة الإنترنت دوماً على استهداف الثغرات الأمنية في برامج الإنترنت الشائعة، ما يستلزم عمليات التحديث والترقية المتواصلة لهذه البرمجيات عند تحديد الثغرات الأمنية.

لتشفير (SSL) حماية صفحات تسجيل الدخول عبر تقنيات التشفير: استخدموا دائماً بروتوكول طبقة المقابس الآمنة صفحات تسجيل الدخول إلى مواقعكم لضمان نقل المعلومات الحساسة مثل أرقام بطاقات الدفع وبيانات تسجيل الدخول بأمان، وبالتالي منع قراصنة الإنترنت من الوصول إلى البيانات الحساسة.

النسخ الاحتياطي لبياناتكم: احتفظوا بنسخ احتياطية لمواقعكم الإلكترونية وملفاتكم بانتظام، لاستخدامها في حال تعذر الوصول إليها نتيجة خلل في نظام التشغيل أو هجمات طلب الفدية. وبينما يتوفر العديد من برامج إدارة المحتوى التي تخزن نسخاً احتياطية تلقائياً، يجدر بكم أيضاً نسخ قواعد البيانات والمحتوى يدوياً.

الاختبارات الأمنية المنتظمة للمواقع الإلكترونية: من الأهمية بمكان إجراء اختبارات أمنية دورية مرة كل ثلاثة أشهر على الأقل، وبعد كل تغيير يطرأ على موقعكم الإلكتروني، ليتسنى لكم تقييم نقاط الضعف المحتملة.

اختيار مزود موثوق لخدمات الاستضافة: تأكدوا من اختيار مزود آمن وموثوق لخدمات الاستضافة، وقادر على تقديم الدعم الفني على مدار الساعة، إضافة إلى احتفاظه بنسخ احتياطية لبياناتكم في خادم بعيد وضمان إمكانية استعادتها بسهولة في حال اختراق موقعكم الإلكتروني.

استخدام كلمات سر قوية ومركبة: لتوفير أعلى درجات الحماية لموقعكم الإلكتروني، ينبغي لكلمات المرور أن تكون قوية ومركبة وتحتوي على أحرف كبيرة وصغيرة وأرقام وعلامات ترقيم مختلفة، كما ينبغي تغييرها بانتظام.

إزالة البيانات غير الضرورية من الموقع الإلكتروني: تمثل كل قاعدة بيانات أو تطبيق أو مكون إضافي على الموقع الإلكتروني نقطة دخول محتملة أخرى للمهاجمين وقراصنة الإنترنت. لذا، احرصوا على حذف أي ملفات أو قواعد بيانات أو تطبيقات غير مستخدمة من موقعكم الإلكتروني.

مراقبة الأصول الشبكية: من الأهمية بمكان اكتشاف أي نشاط غير مصرح به وغير معتاد ضمن شبكتكم الإلكترونية. مراقبة سلامة الملفات) وسجلات الموقع الإلكتروني يعد أمراً بالغ الأهمية (FIM فاستخدام حلول مثل

وتشير المعيطات إلى أن العادات الجديدة التي اكتسبها المستهلكون عقب جائحة «كوفيد-19» ستصبح بمثابة واقع جديد. لذا، سيصبح تحديث استراتيجيات مكافحة الاحتيال ضرورة ملحة للمستهلكين والتجار على حد سواء، لاسيما الذين اعتمدوا التجارة الرقمية والمدفوعات الرقمية، أو نقلوا أعمالهم عبر الإنترنت للمرة الأولى خلال الجائحة

وفي سبيل توفير أقصى درجات الحماية للأعمال وضمان نموها في العالم الرقمي ما بعد الجائحة، يتعين على التجار الارتقاء بإمكاناتهم وتوفير خطط استجابة فعالة لمواجهة الجرائم الإلكترونية، إضافة إلى توعية الأكثر عرضة لخطر المحتالين. فقد نجحت الشركات التي تمكنت من حماية مواردها وعمالها من التهديدات الرقمية سريعة التطور، في تعزيز موقعها واكتساب ثقة المستهلكين في عالم رقمي مترابط، فكانت بذلك أكثر قدرة على استعادة عملائها السابقين

وختاماً، تقع المسؤولية على عاتق الجميع من الشركات والمؤسسات والمستهلكين والتجار، وعلينا جميعاً مواصلة العمل لمكافحة عمليات الاحتيال في المدفوعات

الشرق الأوسط وشمال إفريقيا Visa مدير إدارة المخاطر في *