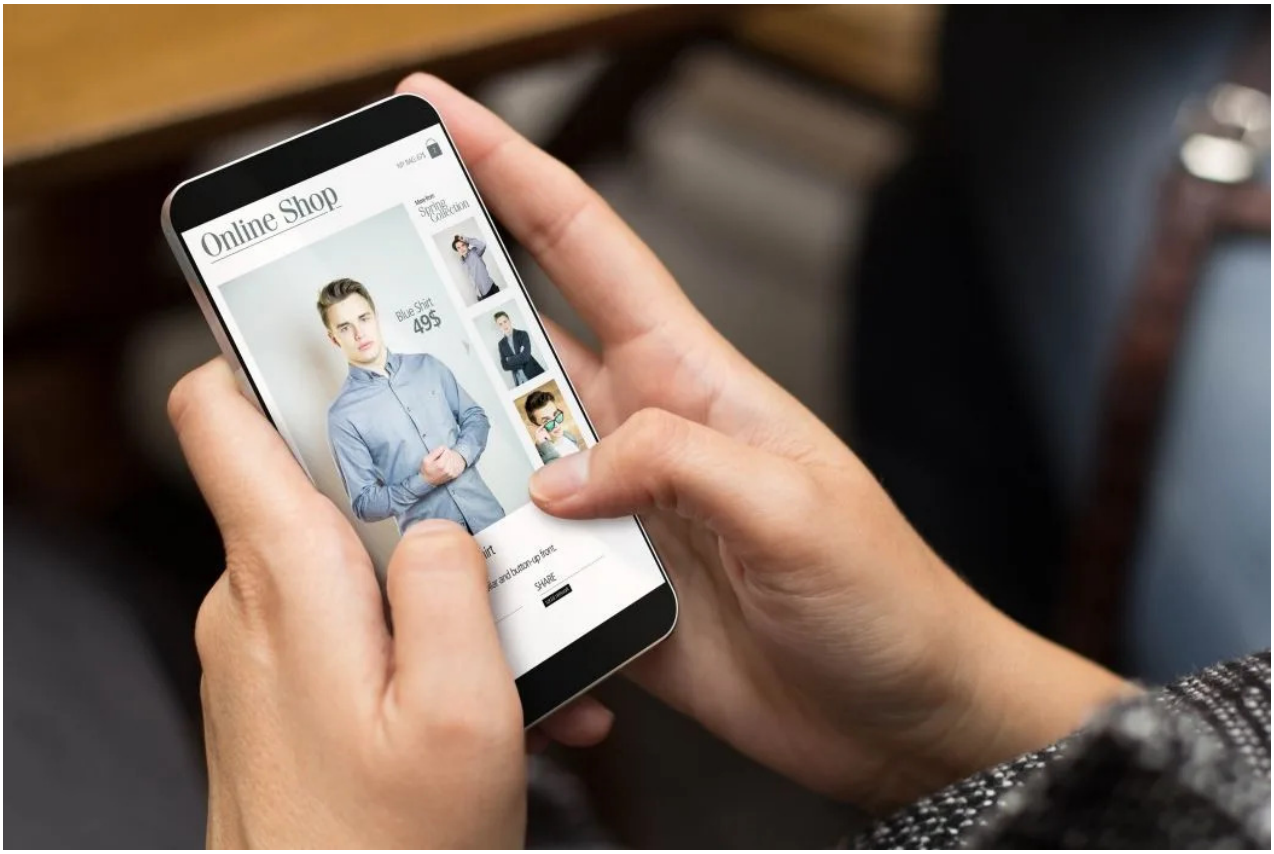
الجوانب الأمنية للتجارة الإلكترونية



تناقلت القنوات الإخبارية خبر المليونير الألماني ستيفن توماس وهو مبرمج يعيش في الولايات المتحدة الأمريكية بسان فرانسيسكو الذي أضاع 220 مليون دولار، بعد أن نسيّ كلمة المرور الخاصة بمحفظته الإلكترونية، وتبقت لديه محاولتان فقط من أصل عشر.

وهذا نموذج لما يمكن أن تحتويه مخاطر التجارة الإلكترونية، لكن تلك المخاطر كثيرة، فما هي؟

التجارة الإلكترونية وتحدياتها

تشكل التجارة الإلكترونية اليوم جزءًا كبيرًا من إجمالي نشاط التجارة التقليدية، فمبيعات التجارة الإلكترونية في جميع أنحاء العالم بلغت 3.53 تريليون دولار عام 2019.

وبسبب فيروس COVID-19، هناك اعتماد متزايد على الإنترنت على الصعيد العالمي، ومن المتوقع أن تصل أعمال التجارة الإلكترونية إلى 4.5 تريليون دولار بحلول عام 2021، وبحلول عام 2022 من المتوقع أن تنمو إلى 6.54 تريليون دولار.

كما تتوقع مجلة Magazine Cybercrime فإن التجارة الإلكترونية ستكون واحدة من أكثر 10 صناعات تتعرض للهجمات خلال الفترة 2019-2022.

وفي حين أن التجارة الإلكترونية تسد الثغرات في السوق، فهي عرضة للهجمات الإلكترونية التي تُشن ضدها بالترتيب، وتؤدي هذه الهجمات في بعض الأحيان إلى انتهاكات واسعة النطاق للبيانات، التي قد تشمل سرقة المعلومات من العملاء أو هوياتهم.

وقد يسعى جواسيس الشركات إلى الحصول على ملكية فكرية يمكن أن تمنح منافسًا ميزة قيّمة على

الشركة المستهدفة، مثل خطط المواقع للمتاجر الجديدة.

ما المقصود بأمان التجارة الإلكترونية؟

المقصود بأمان التجارة الإلكترونية هو حماية جميع أصول التجارة الإلكترونية للشركات من الاستخدام غير المصرح به، فتنفيذ إجراءات حماية وجود الشركات على الإنترنت أو أي تهديد إلكتروني آخر عادة ما يتضمن سلسلة من البروتوكولات لتأمين العميل والمتجر، تتضمن هذه البروتوكلات بعض النصائح لتحسين أمان التجارة الإلكترونية مثل إضافة جدار حماية واستخدام كلمات مرور قوية وتقنية التحقق بخطوتين.

إليك ما تحتاج إلى معرفته عن التهديد الأمني للتجارة الإلكترونية وكيف يمكنك حماية نفسك.

أكثر التهديدات شيوعًا

بالنسبة لشركات التجارة الإلكترونية التي تتعامل في المعاملات النقدية اليومية، يجب أن يصبح الأمن هو شغلها الأول.

وفيما يلي التهديدات الشائعة التي تواجهها مواقع التجارة الإلكترونية:

1- خرق كلمة المرور

أحد أكبر التهديدات الأمنية للتجارة الإلكترونية هو اختراق كلمة المرور، حيث يخترق مجرمو الإنترنت قواعد بيانات المؤسسات وسرقة معلوماتهم الحساسة، ومن أشهر طرق اختراق كلمة المرور"هجوم القاموس" ويقصد به استخدام ملف بسيط يحتوي على كلمات مرور معدة مسبقًا.

2- بريد عشوائي

يخترق مرسلو البريد العشوائي أحيانًا حسابات البريد الإلكتروني للأفراد أو المؤسسات، الذين تعرفهم ثم يستخدمون رسائل البريد الإلكتروني هذه لإرسال رسائل بريد إلكتروني غير مرغوب فيها تهدف إلى اختراق متجر التجارة الإلكترونية الخاص بك على أمل أن تعتقد أنها شرعية.

3- التصيد الاحتيالي

إن تلقي رسائل البريد الإلكتروني المزيفة التي تقول "يجب عليك اتخاذ إجراء" سواء إلى شركتك أم العملاء، هي حيلة شائعة الاستخدام وشكل من أشكال الخدع التي يستخدمها المتسللون.

وهذا النوع من الاحتيال غالبًا ما يحدث عند الشراء من أحد المواقع الإلكترونية مثل أمازون، فإنه يطلب المعلومات الشخصية، وفي النهاية يطلب رقم بطاقة الفيزا كارد، ومن خلاله يسرق النقود.

4- البرمجيات الخبيثة

تم تصميم البرمجيات الخبيثة لأداء مجموعة متنوعة من الوظائف الضارة، فهم قادرون على سرقة المحتوى من موقع الويب، مثل تسعير المنتج والكتالوجات وما إلى ذلك التي ينشرونها على موقع آخر.

يؤثر هذا على تصنيف محرك البحث للموقع، كما بإمكانهم القيام بزيارات متعددة للصفحة في فترة زمنية قصيرة جدًا، وبالتالي إجهاد خوادم الويب، ما يجعل الموقع بطيئًا للمستخدمين الحقيقيين.

5- هجمات رفض الخدمة الموزعة DDoS

تهدف هجمات رفض الخدمة الموزعة (DDoS) إلى تعطيل موقع الويب الخاص بك والتأثير على المبيعات الإجمالية.

لا تحدث بعض الثغرات الأمنية من جانب واحد (الشركة) بل قد تحدث من الجانب الآخر (العميل)، فقد

يستخدم كلمات مرور ضعيفة أو قد يقدم معلومات حساسة

أهم طرق مكافحة تهديدات أمن التجارة الإلكترونية

هناك طرق عدة لمعالجة هذه التهديدات أهمها ما يلي:

1. التشفير:

عند تمكين التشفير على خادم التجارة الإلكترونية الخاص بك، يتم تحويل بيانات المستخدم من نص عادي إلى نص مشفر لا يمكن قراءته إلا بعد فك تشفيره.

2. التعامل مع بطاقات الدفع الآمنة

تصبح العديد من شركات التجارة الإلكترونية ضحية للاحتيال على بطاقات الائتمان وبطاقات الخصم بسبب استخدام بوابات دفع غير موثوقة، سيسمح لك معظم منشئي المتاجر عبر الإنترنت بالتعامل مع العشرات من بوابات الدفع الشائعة.

بما في ذلك PayPal وStripe وبوابات الدفع الأخرى للمؤسسات، لذلك لا يوجد عذر لعدم استخدام إحدى بوابات الدفع الموثوقة.

كذلك التعامل مع منصات التجارة الإلكترونية القوية مثل PrestaShop وMagento وWooCommerce إحدى منصات التجارة الالكترونية القوية الشائعة.

3. تأمين موقع الويب الخاص بك بشهادة SSL

تشفر شهادة SSL جميع المعلومات التي يرسلها المستخدمون على موقع التجارة الإلكترونية الخاص بك وتجعل من الصعب على المتسللين التنصت على هذه البيانات أو تحديد أي معنى لها في حالة التنصت عليها.

4. استخدام برامج مكافحة الفيروسات

تتيح لك برامج مكافحة الفيروسات الجيدة معرفة ما إذا كان أحد المتطفلين يحاول تثبيت فيروس أو برنامج ضار على جهاز الكمبيوتر الخاص بك.

كما يخبرك إذا قمت بزيارة موقع قد يكون ضارًا أو إذا تلقيت ارتباطًا سيئًا في رسالة بريد إلكتروني غير مرغوب فيها.

5- النسخ الاحتياطي لبياناتك

فقدان البيانات بسبب عطل في الأجهزة أو الهجمات الإلكترونية شيء محتمل الحدوث، وإذا لم تنسخ بياناتك احتياطيًا بانتظام، فأنت معرض لخطر فقدانها نهائيًا.

يجب أن تفعل ذلك بنفسك ولا تثق في أي شخص آخر للقيام بذلك نيابة عنك.

6- تدريب الموظفين بشكل جيد

لا بد أن يكون طاقم العمل على دراية بالقوانين والسياسات المتعلقة بحماية معلومات المستخدم، كما لا يجوز أن يشاركوا بيانات اعتماد تسجيل الدخول، ولا بد من مراجعة الموظفين الذين يمكنهم الوصول إلى معلومات العميل الحساسة.

وبمجرد أن يقدم الموظف استقالته، امسح تفاصيله وألغ كل إمكانية وصوله لمنعه من ارتكاب جريمة إلكترونية ضد عملك.

7- توعية عملائك

لا تحدث بعض الثغرات الأمنية من جانب واحد (الشركة) بل قد تحدث من الجانب الآخر (العميل)، فقد يستخدم كلمات مرور ضعيفة أو قد يقدم معلومات حساسة عن مواقع التصيد الاحتيالي وفي أيدي المتسللين.

إذا كان أحد المتاجر يبيع في الغالب على المستوى الوطني، وتتدفق جميع الطلبات المفاجئة من مختلف دول العالم، فقد يكون ذلك علامة على سلوك احتيالي

كيفية كشف الاحتيال في التجارة الإلكترونية

منع الاحتيال عبر الإنترنت مرهون بتفسير إشارات الاحتيال، لا سيما مع زيادة شعبية الطلب عبر الإنترنت.

فيما يلي 10 علامات حمراء وهي إشارات للمخاطر التي تحددها إستراتيجيات منع الاحتيال والكشف عنها مسبقًا:

1- التسوق لأول مرة

يحب المحتالون الوصول إلى مواقع الويب التي لم يسبق لهم زيارتها من قبل، وبمجرد وصولهم إلى الموقع، سينتقلون من خلال التنكر على أنهم متسوقون لأول مرة.

تعد شبكة البيانات ضرورية لكشف معلومات عن الشراء والعميل لإعطاء نظرة ثاقبة للمتسوق لأول مرة.

2- الشحن السريع

يحب المحتالون الشحن السريع والتعجيل بشحن مشترياتهم، حتى إن كان سعر الشحن باهظًا، نظرًا لأن البطاقة المسروقة لها عمر قصير، ويعرف المجرم أن الوقت ضده.

3- موقع غير عادي

إذا كان أحد المتاجر يبيع في الغالب على المستوى الوطني وتتدفق جميع الطلبات المفاجئة من مختلف دول العالم، فقد يكون ذلك علامة على سلوك احتيالي.

4- كمية كبيرة من نفس المنتج

إذا تلقت الشركات طلبًا يحتوي على عدد كبير من نفس العناصر، إذ يميل المحتالون إلى إصدار أوامر كبيرة وسريعة، وكذلك ارتفاع عدد الطلبات إلى فوق المتوسط، حيث يمكن إلغاء البطاقات المسروقة في أي وقت.

5- عناوين شحن متعددة

يقوم المحتالون أحيانًا بإصدار أوامر إلى عناوين شحن متعددة باستخدام عدة بطاقات مسروقة، كل منها موضوع باسم مختلف.

إذا كان حساب العميل يحتوي على عناوين شحن متعددة مرفقة به، فهذه علامة حمراء.

6- عنوان الشحن/الفوترة لا يتطابق مع عنوان IP

تتمثل فائدة متاجر التجارة الإلكترونية في أنه يمكن للشركات تتبع التفاصيل الدقيقة لطلب العميل: من عناوين الفواتير والشحن الخاصة بهم، وصولًا إلى عنوان IP الخاص بهم، وإذا لم تتطابق كل هذه الأشياء، فهذه علامة حمراء.

7- بطاقات متعددة من عنوان IP واحد

إذا تم تقديم الطلبات من نفس عنوان IP، لكن من عدة بطاقات مختلفة، لأنه من غير المعتاد أن يكون لدى العملاء أكثر من بطاقة واحدة، يجب اعتبار العديد من البطاقات المختلفة – خاصة إذا تم استخدامها في نفس الوقت – مريبة.

8- معاملات وطلبات متعددة في فترة زمنية قصيرة

إذا اكتشفت الشركات سلسلة من الطلبات يتم تقديمها في تتابع سريع، فقد يشير ذلك إلى الاحتيال.

وفي كثير من الأحيان، لا يسرق المحتالون المعلومات من بطاقة واحدة، بل يستخدمون بطاقات متعددة بدلاً من ذلك، فإذا تم تقديم طلبات متعددة ببطاقات مختلفة، سواء عبر معاملة واحدة أم عدة معاملات، فقد يشير ذلك إلى احتيال.

9- عناوين البريد الإلكتروني الجديدة

يستخدم معظم المستهلكين نفس عنوان البريد الإلكتروني لبعض الوقت، بينما غالبًا ما ينشئ الفاعلون السيئون عناوين بريد إلكتروني جديدة لكل معاملة في محاولة للتحايل على فحوصات السرعة الأساسية وتحليل الارتباط.

10- ربط إشارات احتيال متعددة

من خلال ربط هوية العميل بأكثر من عامل من عوامل الخطر المذكورة أعلاه، يمكن أن توفر نقاط البيانات المتعددة أدلة قوية تساعد المحللين على تحديد ما إذا كانت عملية الشراء مشروعة أو ما إذا كان هناك سبب للريبة.

إذا فشلت في إتقان أمان التجارة الإلكترونية، فستصبح عرضة لهذه الانتهاكات، فإنك تعرض بيانات العملاء الحساسة للخطر وتعاني من فقدان المبيعات وثقة العملاء وسمعة علامتك التجارية، وفي النهاية انخفاض الإيرادات والخسارة والإفلاس.

رابط المقال: https://www.noonpost.com/39565/