أشهر التهديدات السيبرانية لمواقع التجارة الإلكترونية، وطرق مكافحتها

أهم طرق مكافحة تهديدات أمن التجارة الإلكترونية

التشفير:

حيث يتم تحويل بيانـــات المستخـــدم من نص عادي إلى نص مشفـــر لا يمكن قراءته إلا بعد فك تشفيره.

التعامل مع بطاقات الدفع الآمنة:

حصر التعامل مع بوابات الدفع الشائعة والموثوقة، مثل payfort و PayTab و مُيسّر وبوابات الدفع الأخرى للمؤسسات.

تأمين موقع الويب الخاص بك بشهادة SSL:

تشفر جميع المعلومات التي يرسلها المستخدمون على موقعك وتصعّب على المتسللين التنصت عليها أو تحديد معانيها في حالة التنصت عليها.

استخدم برامج الحماية من البرمجيات الضارة:

ويجب تحديثها بشكلٍ مستمر على كل جهاز مستخدم في بيئة العمل (بما في ذلك أجهزة الحاسب الآلي والهواتف الذكية والأجهزة اللوحية) لحماية أنظمة تجارتك الإلكترونية من البرمجيات الضارة.

النسخ الاحتياطي لبياناتك:

لمنع فقدان البيانات بسبب عطل في الأجهزة أو هجمات إلكترونية.

تدريب الموظفين بشكل جيد:

لا بد أن يكون طاقم العمل على دراية بالقوانين والسياسات المتعلقة بحماية معلومات المستخدم، وتحذيرهم من مشاركة بيانات اعتماد تسجيل الدخول، ومراجعة الموظفين الذين يمكنهم الوصول إلى معلومات العميل الحساسة.

وبمجرد أن يقدم الموظف استقالته، فعليك أن تمسح تفاصيله وتلغي كل إمكانيات وصوله لبيانات العملاء والمنشأة.

توعية عملائك:

قد تحدث بعض الثغرات الأمنية من جانب العميل، فقد يستخدم كلمات مرور ضعيفة أو قد يقدم معلومات حساسة لمواقع التصيّد الاحتيالي.