أفضل ممارسات الأمن السيبراني في التجارة الإلكترونية

1 خذ بعين الاعتبار استخدام خيارات تحقق إضافية:

فّعل خاصية التحقق المتعدد العناصر للهوية عند توفر ذلك في الأنظمة أو التطبيقات ذات العلاقة بتسجيل دخول عملائك وذلك لحماية المستهلكين الذين تتعامل معهم في التجارة الإلكترونية. مثل تسجيل اشترك في خيارات التحقق الإضافية (مثل رسائل البريد الإلكتروني) التي تقدمها تطبيقات التجارة الإلكترونية ومواقعها (ويشمل هذا حسابات مواقع التواصل الاجتماعي).

2 تحكّم بعدد حسابات مسؤولي الأنظمة:

امنح موظفي تجارتك الإلكترونية أقل مستوى من صلاحيات المستخدم المطلوبة للقيام بمهامهم الوظيفية وامنح صلاحيات مسؤول النظام بحذر شديد، حيث يتمتع حساب مسؤول النظام بصلاحيات خاصة للقيام بتغييرات في النظام لا يمكن لحسابات المستخدمين الآخرين القيام بها.

3 حدث تطبيقاتك بانتظام على جميع الأجهزة:

أكثر الطرق كفاءة في الحماية ضد البرمجيات الضارة والفيروسات هي إبقاء جميع أجهزة وتطبيقات تجارتك الإلكترونية (خاصًة أنظمة التشغيل) محدثَة بآخر التصحيحات الأمنية.

4 استعن بمواقع موثوقة لعرض إعلاناتك:

اعمل على حماية إعلاناتك من النقرات الاحتيالية وذلك عن طريق عرض إعلاناتك على مواقع موثوقة والتي تعرف أنها مصدر لعملاء حقيقيين.

5 اطلع على التهديدات السيبرانية أولاً بأول:

اشترك بالتنبيهات والإنذارات السيبرانية لتبقى على اطلاع بمستجدات الأمن السيبراني والتهديدات النشطة من خلال متابعة آخر التحديثات والمستجدات من منظمات موثوقة (مثل المركز الوطني الإرشادي السعودي للأمن).

الجزء الرابع من سلسلة الأمن السيبراني في التجارة الإلكترونية