Consejos de ciberseguridad para pymes para la campaña navideña

Cada vez más empresas impulsan sus negocios online para adaptarse al nuevo escenario marcado por el Covid-19 y a los nuevos hábitos de los consumidores

La plataforma de pagos PayPal ofrece una serie de consejos imprescindibles para ayudar a las empresas a aumentar la seguridad de sus negocios online

19 de noviembre de 2020 // Madrid, España – La crisis sanitaria ha acelerado repentinamente los planes de digitalización de las empresas, que han multiplicado sus iniciativas en ámbitos como el comercio electrónico. Según datos de PayPal, la plataforma de pagos líder en Europa, en el tercer trimestre de 2020 se registraron 1,5 millones de nuevas cuentas PayPal Business (para empresas) en todo el mundo, más del doble en comparación con la tasa anterior al Covid-19, lo que demuestra que **cada vez más empresas se están adaptando a la pandemia impulsando sus negocios online**.

Dar el salto en el uso de tecnologías digitales aporta muchos beneficios a las empresas, que han sufrido las negativas consecuencias provocadas por el Covid-19 y que buscan cambiar o reinventar sus modelos de negocio para adaptarse a los nuevos hábitos de consumo de los clientes. Sin embargo, el hecho de que cada vez más empresas ofrezcan sus productos y servicios en Internet hace que las necesidades en materia de ciberseguridad aumenten.

En este contexto, la plataforma PayPal, líder en la protección de la privacidad y la identidad de los usuarios, ofrece una serie de **consejos de ciberseguridad para ayudar a las empresas, especialmente a las pymes, a aumentar la seguridad de sus negocios online**, especialmente ahora que se acerca uno de los períodos más importantes del año para los comercios, coincidiendo con la época de compras navideñas y la celebración de reconocidos días a nivel internacional como el Black Friday o el Cyber Monday.

Mantener las plataformas y software actualizados

Es muy importante asegurarse de estar utilizando la última versión del sistema operativo, ya que los proveedores actualizan continuamente su software con parches de seguridad para protegerlo de vulnerabilidades recién descubiertas, así como de los últimos virus y malware.

Asimismo, es importante instalar y actualizar periódicamente software antimalware y antispyware de nivel empresarial (el software antivirus gratuito, de funciones limitadas y apto para el consumidor no es suficiente) para evitar ataques que aprovechen las vulnerabilidades del software obsoleto.

Las plataformas por las que muchas pymes optan para crear su tienda online, como la PayPal Commerce Platform, ya incluyen las últimas actualizaciones y parches de seguridad automáticos que ayudan a resolver cualquier vulnerabilidad de seguridad.

Invertir en herramientas de gestión del fraude

Incluso las herramientas más básicas como el sistema de verificación de dirección (AVS) – que verifica la dirección de facturación almacenada en una tarjeta de crédito para ayudar a aumentar la protección de cargos fraudulentos – y el código de verificación de la tarjeta (CVV) pueden ayudar a minimizar las transacciones fraudulentas sin perder ventas.

Estas son las herramientas más básicas, pero existen otras más complejas como Simility, un servicio de PayPal que combina la Inteligencia Artificial (IA) y el análisis de Big Data para ayudar a las empresas a prevenir intentos de fraude, como el robo de identidad, en tiempo real.

Controlar las transacciones y conciliar las cuentas bancarias diariamente

Verificar y monitorear la actividad financiera de las cuentas bancarias es una de las mejores formas de protegerse contra el fraude. Es recomendable supervisar las cuentas y transacciones en busca de señales de alerta, como información de envío y/o facturación de los clientes errónea o incongruente.

Existen herramientas que rastrean las direcciones IP de los clientes y alertan a los comercios de aquellas que provienen de países conocidos como base para estafadores. Por ejemplo, la plataforma de pagos PayPal incluye 3D Secure (un proceso de autenticación que valida la identidad del usuario cuando utiliza cualquier servicio de pago con el objetivo de reducir el riesgo de fraude).

Desconfiar de mensajes o correos de fuentes desconocidas

Debemos desconfiar si un mensaje de texto o un correo electrónico requiere una acción urgente o inmediata, especialmente si proviene de un remitente extraño o desconocido. Igual de importante es no abrir archivos adjuntos ni hacer clic en enlaces de fuentes desconocidas, incluso si es para "cancelar la suscripción" del remitente. Incluso si un mensaje parece provenir de una fuente de confianza, como un banco, debemos mantener la alerta porque las instituciones financieras nunca solicitarán información de identificación personal en un correo electrónico o mensaje de texto.

Elegir un buen socio de pagos

Una de las formas más efectivas de combatir el fraude en los pagos digitales es tener una herramienta sofisticada de protección contra el fraude. Las empresas pueden obtener una herramienta de protección contra el fraude por su cuenta o pueden optar por un procesador de pagos que ya incluya esa protección, como el caso de las soluciones de PayPal.

PayPal no comparte la información financiera del cliente con los vendedores. De esta manera, los comercios se benefician del cumplimiento del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI por sus siglas en inglés), reducen el riesgo de fraude y ayudan a obtener tasas de conversión más altas al hacer que los pagos a través de PayPal se realicen sin problemas.

Ser más estricto con los requisitos de contraseña de los clientes

Los piratas informáticos emplean programas sofisticados que pueden ejecutar todas las permutaciones de una contraseña. No tardarán en descifrar una contraseña alfanumérica de cuatro dígitos (como "abcd"). Lo ideal es solicitar a los clientes una contraseña alfanumérica de ocho dígitos con al menos una mayúscula y un carácter especial. Los clientes pueden sentirse molestos, pero es mejor estar seguro que sufrir un ciberataque.

Educar a los empleados sobre los métodos de ciberataques existentes

Llevar a cabo un programa de formación en ciberataques dirigido a los empleados involucrados en la recepción, aprobación o envío de los pedidos puede ayudar a evitar ataques. Las empresas deberían recopilar información actualizada sobre las últimas técnicas y tendencias de fraude y compartirla con sus empleados.

En definitiva, es importante monitorear las tendencias de fraude, invertir en herramientas de protección, educar a los empleados y trabajar con socios que pueden ayudar a prevenir el fraude. A menudo, las empresas se sorprenden de lo sencillo que puede ser poner en práctica estas estrategias y muchas veces este proceso comienza con la selección de la plataforma tecnológica adecuada que incorpore todas estas estrategias en un solo paquete.

Sobre PayPal
PayPal se ha mantenido a la vanguardia de la revolución de los pagos digitales durante más de 20 años. La plataforma, que aprovecha la tecnología para hacer que los servicios financieros y el comercio sean más cómodos, asequibles y seguros, permite a más de 350 millones de consumidores y vendedores de más de 200 mercados unirse y prosperar en la economía global. Para más información, visita paypal.com.

Subscríbete a nuestra Newsroom para recibir las ultimas noticias de PayPal en España y síguenos también en Twitter en @PayPalSpain.

Para más información y prensa:

Edelman
Tel: 93 488 12 90
PAYPALES@edelman.com