PayPal

5 pasos para prevenir pagos fraudulentos

Cómo disminuir el riesgo

Los pagos y la actividad fraudulentos pueden afectar a tu negocio y a tus ventas en línea. Al implementar las herramientas y los procesos adecuados, puedes minimizar el riesgo y mantener tu negocio y tus clientes seguros, lo que reduce las posibilidades de que se produzcan comisiones por contracargos y pérdidas de ingresos.

Cómo operan los estafadores

Por lo general, los estafadores en línea usan dos métodos para robar dinero:

Apropiación de cuentas:

un esquema común consiste en que los estafadores envíen correos electrónicos para engañar a los clientes a fin de que revelen los nombres de usuario y contraseñas de sus cuentas. Luego, inician sesión, cambian las contraseñas y realizan compras no autorizadas.

Robo de identidad:

a pesar de que los negocios toman precauciones, los estafadores logran piratear bases de datos para obtener información personal. Los hackers suelen vender números de tarjetas de crédito a otros estafadores, que abren cuentas en línea y usan los números robados para comprar, sin que la víctima se entere.

PayPal © Copyright PayPal 2021.

Cinco pasos para prevenir pagos fraudulentos

Monitorea las transacciones y concilia tus cuentas bancarias todos los días

Nadie conoce los detalles de tu negocio mejor que tú, como quiénes son tus mejores clientes y los patrones de compra. Monitorea tus cuentas para detectar señales de alerta, como facturación, información de envío y ubicación física inconsistentes de los clientes.

Considera poner límites

Establece límites para la cantidad de compras y el valor total que aceptarás de una cuenta en un día. Así podrás reducir tu exposición al máximo en caso de que ocurra un fraude.

Pide el código de seguridad de la tarjeta (CVV, por sus siglas en inglés)

Las reglas de PCI prohíben que se guarde el CVV de un cliente junto con el número de la tarjeta de crédito y el nombre del titular de la tarjeta. Por eso es tan eficaz: es prácticamente imposible que los estafadores lo obtengan a menos que roben la tarjeta física. La mayoría de los procesadores incluyen una herramienta que requiere el CVV como parte de sus plantillas de pago. Úsala.

Ten requisitos de contraseña más estrictos

Los hackers emplean programas sofisticados que pueden ejecutar todas las versiones de una contraseña. Las mejores prácticas actuales requieren una contraseña alfanumérica de un mínimo de ocho dígitos con al menos una mayúscula y un carácter especial.

Mantén tus plataformas y software actualizados

Asegúrate de que usas la versión más reciente de tu sistema operativo (OS, por sus siglas en inglés), ya que los proveedores de OS actualizan su software continuamente para protegerte de las vulnerabilidades que se van descubriendo, así como de los últimos virus y malware.

Una nota importante sobre tu software antivirus

Una buena práctica es instalar y actualizar periódicamente los programas antimalware y antispyware de *nivel empresarial*. Las versiones gratuitas para consumidores por lo general no son suficientes. Si tu sitio está alojado en una solución administrada, los parches de seguridad automáticos ayudan a garantizar que cualquier vulnerabilidad se resuelva rápidamente.

El contenido de este artículo se proporciona únicamente con fines informativos. Siempre debes obtener asesoramiento contable, financiero y legal independiente y profesional antes de tomar cualquier decisión de negocio.

PayPal © Copyright PayPal 2021.