Digitalizar + Prosperar

PROTEGE TU NEGOCIO CONTRA EL FRAUDE

Cómo estar a la vanguardia en la ciberseguridad

PayPal

¿QUÉ ES LA ECONOMÍA DEL FRAUDE?

Solíamos pensar en el fraude en línea como incidentes aislados, realizados por hackers y estafadores individuales. Pero en los últimos años, este tipo de crimen digital se lleva a cabo cada vez más por redes coordinadas y sofisticadas de ciberdelincuentes. Por esta razón, los negocios deben implementar seguridad con la misma complejidad para protegerse contra el fraude.

La pandemia cambió el juego por completo, especialmente en el eCommerce. El comienzo del COVID-19 provocó un aumento del 60% en el tráfico de Internet y, como resultado, el gasto de los consumidores en línea casi se duplicó.[1] Durante el 2021, las amenazas de fraude fueron peores que nunca. Las tiendas de eCommerce estaban en riesgo de perder más de $20 mil millones por actividades fraudulentas en línea. Esto representó un aumento del 18% en este tipo de delitos en comparación con el año anterior.[1] En medio del estresante escenario de la pandemia, los estafadores se aprovecharon de las víctimas fingiendo ser organizaciones benéficas, correos electrónicos haciéndose pasar por la Organización Mundial de la Salud (OMS) o el Centro para el Control de Enfermedades (CDC), e incluso llamadas automáticas como si fueran organizaciones gubernamentales, familiares angustiados o bancos e instituciones de tarjetas de crédito.[2]

Conforme la economía del fraude continúa creciendo, también lo hace la audacia de los ciberdelincuentes. Están siendo más inteligentes y sofisticados, y ahora tienen un mayor acceso a las herramientas que necesitan para explotar los negocios en línea. Tienen tanto o más conocimiento del mecanismo del eCommerce como las empresas a las que atacan. Esto les permite identificar con precisión las vulnerabilidades de seguridad y aprovecharlas con el elemento sorpresa.[3]

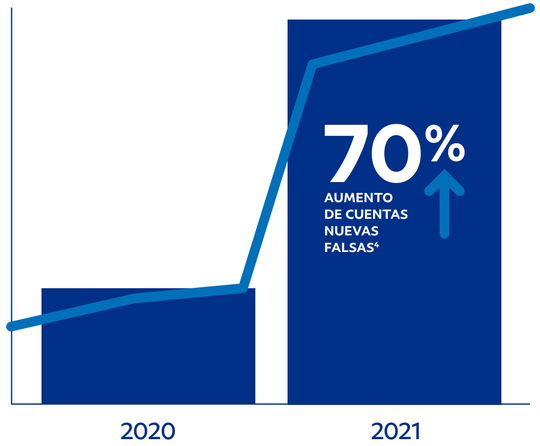
Si bien el fraude está proliferando, los negocios están esforzándose más que nunca para mantenerse al día, pero las expectativas de los clientes no han cambiado. Los compradores en línea siguen esperando una experiencia rápida y sin fricciones, además de una seguridad hermética. Si las compras toman mucho tiempo, requieren demasiados datos o son muy complejas, abandonan sus carritos y siguen adelante. Para las tiendas es todo un reto satisfacer estas expectativas y al mismo tiempo mantener sus negocios seguros ante tantas amenazas en línea.

1. Payments Dive, E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds, 30 de abril de 2021. **2.** CyberCrime Support Network, COVID-19 Scam Alerts, 12 de abril de 2021. **3.** Sift, Exposing the Multi-billion Dollar Fraud Economy, primer trimestre de 2021.

LOS NEGOCIOS ENFRENTAN NUEVOS DESAFÍOS ANTE EL FRAUDE A NIVEL MUNDIAL

AUMENTO DEL FRAUDE DE CUENTAS NUEVAS

En 2021, el registro de cuentas nuevas falsas aumentó en más del **70%**.[4]



PASOS AUDACES HACIA OBJETIVOS MÁS GRANDES

Cada compra fraudulenta tiene en promedio un **70%** más de valor que antes de la pandemia.[5]

AUMENTAN LOS ATAQUES A MÓVILES

50% de todo el tráfico digital fue móvil y la tasa de ataque móvil fue del **24%** en el primer semestre de 2021.[6]

4. Business Wire, 70% Increase in Fraudulent Account Registrations Puts Digital Accounts in the Crosshairs, Arkose Labs Reports, 5 de agosto de 2021. **5.** Retail Week, Every day is now Black Friday – and retailers need to prepare, 4 de noviembre de 2021. **6.** Security Boulevard, Here's How to Fight Diverse Attacks Across Multiple Touchpoints, 8 de octubre de 2021.

ANTICÍPATE A LOS CIBERDELINCUENTES

Con las amenazas cibernéticas más complejas y habituales que nunca, las empresas ya no pueden simplemente considerar el fraude como parte del costo de hacer negocios. El año pasado, el comercio omnicanal sufrió un aumento del 50% interanual en las tasas de fraude y un aumento del 9% interanual en el volumen de pedidos fraudulentos.[7]
Los negocios deben centrarse en tener la infraestructura adecuada para protegerse contra el fraude.

5 consejos para mantener tu negocio seguro:

1. Monitorea tu sitio para detectar actividad sospechosa
2. Detén el ciberdelito al momento de pagar
3. Encripta tus datos para mantener seguros los pagos
4. Actualiza tu software para mejorar tu seguridad
5. Conoce tus puntos vulnerables para aumentar la fortaleza digital

7. Sift, Exposing the Multi-billion Dollar Fraud Economy, primer trimestre de 2021.

1 MONITOREA TU SITIO PARA DETECTAR ACTIVIDAD SOSPECHOSA

Las actividades sospechosas pueden costarle tiempo y dinero a tu negocio, pero no siempre son fáciles de detectar. Es importante mantenerse alerta, por eso aquí te ofrecemos algunas formas de vigilar tu sitio.

Ten cuidado con los contracargos excesivos. Los reclamos por compras desconocidas u olvidadas, así como los malentendidos de las políticas de devolución pueden indicar fraudes por contracargos (también conocido como fraude amigable o fraude del titular). El 94% de los negocios aún ve el fraude amigable como un problema.[8]

Puedes identificar las señales que revelen una actividad inusual del comprador buscando un domicilio de un mercado desconocido y poniendo atención en las direcciones de facturación y envío que no coincidan. Además, ten cuidado con las direcciones de correo electrónico sospechosas, los correos electrónicos que no se pueden entregar, los pedidos inusualmente grandes o si hay múltiples tarjetas de crédito utilizadas para un pedido.

Aunque pongas atención en la actividad de tu sitio, nunca está de más acudir a los expertos. De ser posible, deja que un especialista externo se encargue de la administración de los contracargos para que ni tú ni tu equipo tengan que lidiar con el tedioso monitoreo de estos patrones. También existen herramientas que rastrean las direcciones IP de los clientes y te avisan cuando se encuentran en ubicaciones de alto riesgo.

Las capacidades de prevención antifraude y protección al vendedor de PayPal Commerce Platform pueden ayudar con esto al implementar Machine Learning de acuerdo a las necesidades de tu negocio para minimizar los contracargos y te cubre cuando surgen ciertas actividades de fraude.

8. Business Wire, 8 Out of 10 Merchants Have Seen an Increase in Friendly Fraud, According to the 2021 Chargebacks911 Field Report, 2 de junio de 2021.

2 DETÉN EL CIBERDELITO AL MOMENTO DE PAGAR

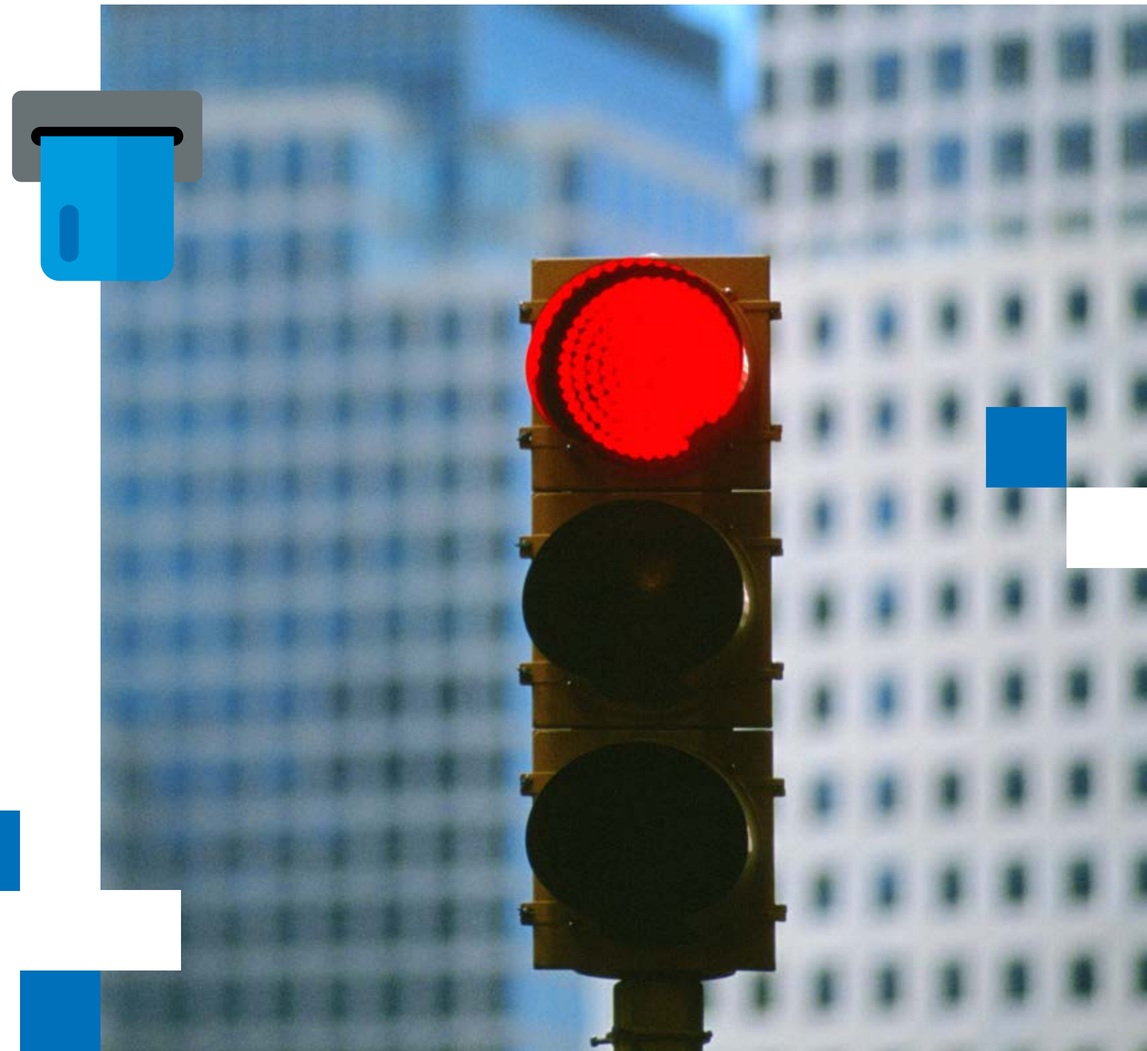
El 59% de los negocios vio un aumento en el fraude debido a transacciones con tarjeta no presente, pero las soluciones de Protección contra el fraude al momento de pagar pueden ayudarte a anticipar este tipo de ataques.[9]

1 de cada 4 comercios se resiste a implementar soluciones de seguridad de pago, pero tomar estos pasos es esencial a medida que los negocios tantean el terreno del eCommerce.[9]

Pedir el código de seguridad de la tarjeta (CVV, por sus siglas en inglés) hace prácticamente imposible para los ciberdelincuentes cometer fraude con tarjeta no presente, ya que las reglas de PCI impiden que los comercios almacenen el CVV junto con el número de tarjeta de crédito. Esto garantiza que el cliente tenga la tarjeta física en su poder para realizar una compra.[10]

El sistema de verificación de direcciones (AVS, por sus siglas en inglés) te ayuda a identificar actividades sospechosas comparando las partes numéricas de la dirección de facturación asociada con la tarjeta de crédito con la dirección registrada en la institución de la tarjeta de crédito. AVS se incluye en la mayoría de los sistemas de procesamiento de pagos, pero es recomendable consultar con tu procesador de pagos para comprobar que sea compatible.

Por último, el control de velocidad es un mecanismo de prevención de fraude que te permite limitar la cantidad de dinero o transacciones que provienen de un cliente por día. Puedes establecer cualquier rango que tenga sentido para tu negocio y recibir una notificación cuando alguien lo supere, o incluso cancelar la transacción automáticamente. Por lo general, esto se hace para evitar estafadores que intentan gastar el máximo posible de las tarjetas de crédito robadas.



9. Payments Dive, Merchants say they're losing revenue to online fraud, FIS report finds, 12 de julio de 2021. **10.** Big Commerce, Ecommerce Fraud Protection for Online Merchants: The Ultimate Guide.

3 ENCRIPTA TUS DATOS PARA MANTENER SEGUROS LOS PAGOS

Los datos no cifrados son el mejor amigo de los ciberdelincuentes. Les brinda fácil acceso a números de tarjetas de crédito, contraseñas y más. Aunque están cambiando hacia objetivos de mayor valor, muchos criminales en línea todavía buscan estas oportunidades fáciles para aprovecharse de ellas.

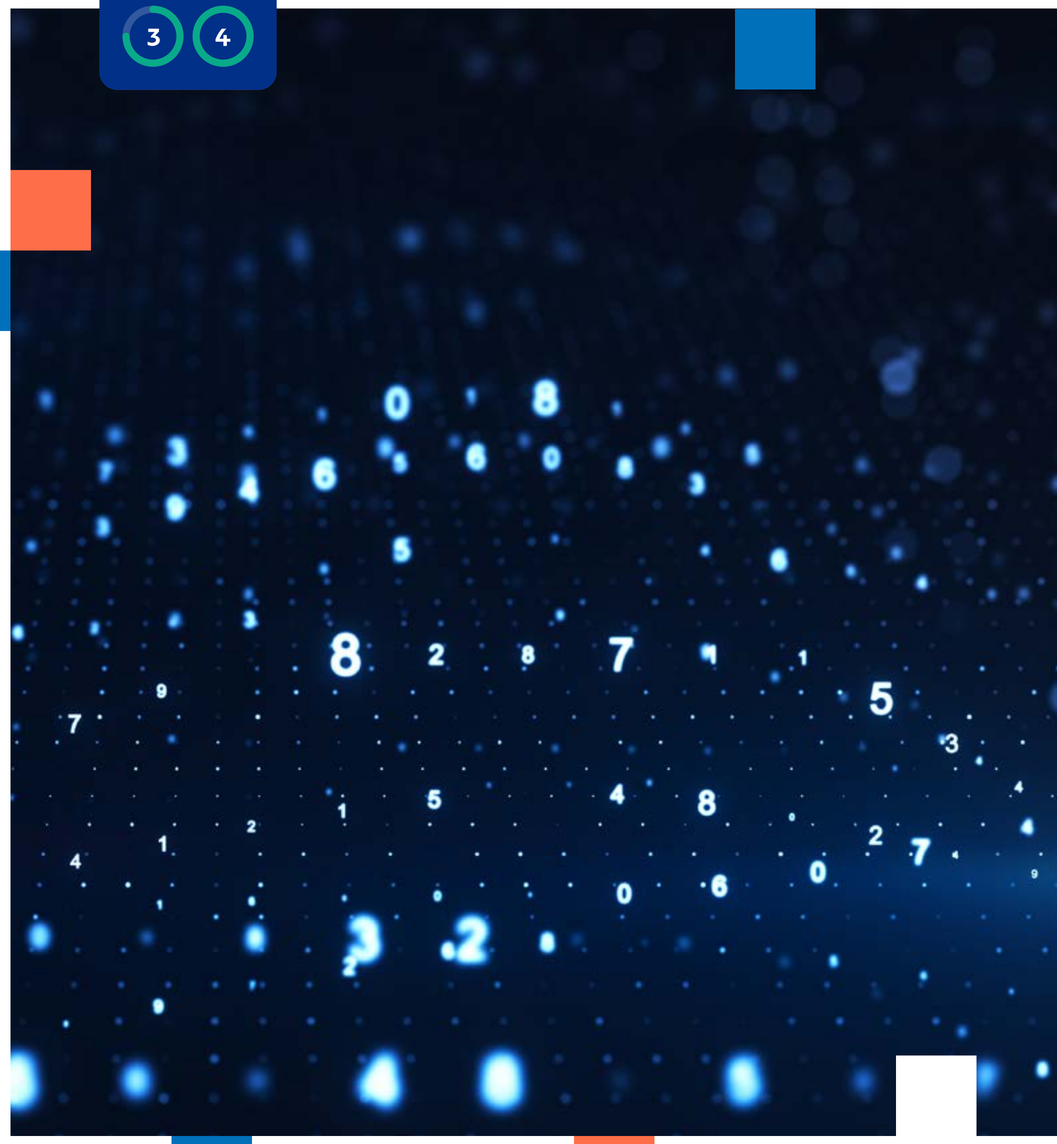
Todos los días se envía una gran cantidad de datos confidenciales por Internet, por lo que la posibilidad de que caigan en manos equivocadas es alta, pero hay medidas que puedes tomar para asegurarte de que esto no perjudique a tu negocio ni a tus clientes.

La tecnología de cifrado de extremo a extremo te prepara para estas situaciones al convertir los datos en un código secreto antes de enviarlos por Internet. También es un requisito para cualquier empresa que almacene o comparta datos debido a las leyes locales de privacidad y protección de datos.[11]

Ve aun más allá y procura tener conexiones HTTPS seguras utilizando configuraciones sólidas de seguridad de la capa de transporte (TLS, por sus siglas en inglés). Las configuraciones TLS son el estándar actual de la industria y permiten que tu información viaje por Internet de forma segura.

Verifica que tu socio de pagos se tome la seguridad de tus datos tan en serio como tú al cumplir con los estrictos requisitos de protección de datos.

La plataforma de pagos PayPal está respaldada por algunos de los mejores cifrados de extremo a extremo. Desde conexiones TLS y HTTPS hasta la fijación de claves, estas prácticas cumplen con estrictos requisitos que protegen los datos en tránsito y en reposo.



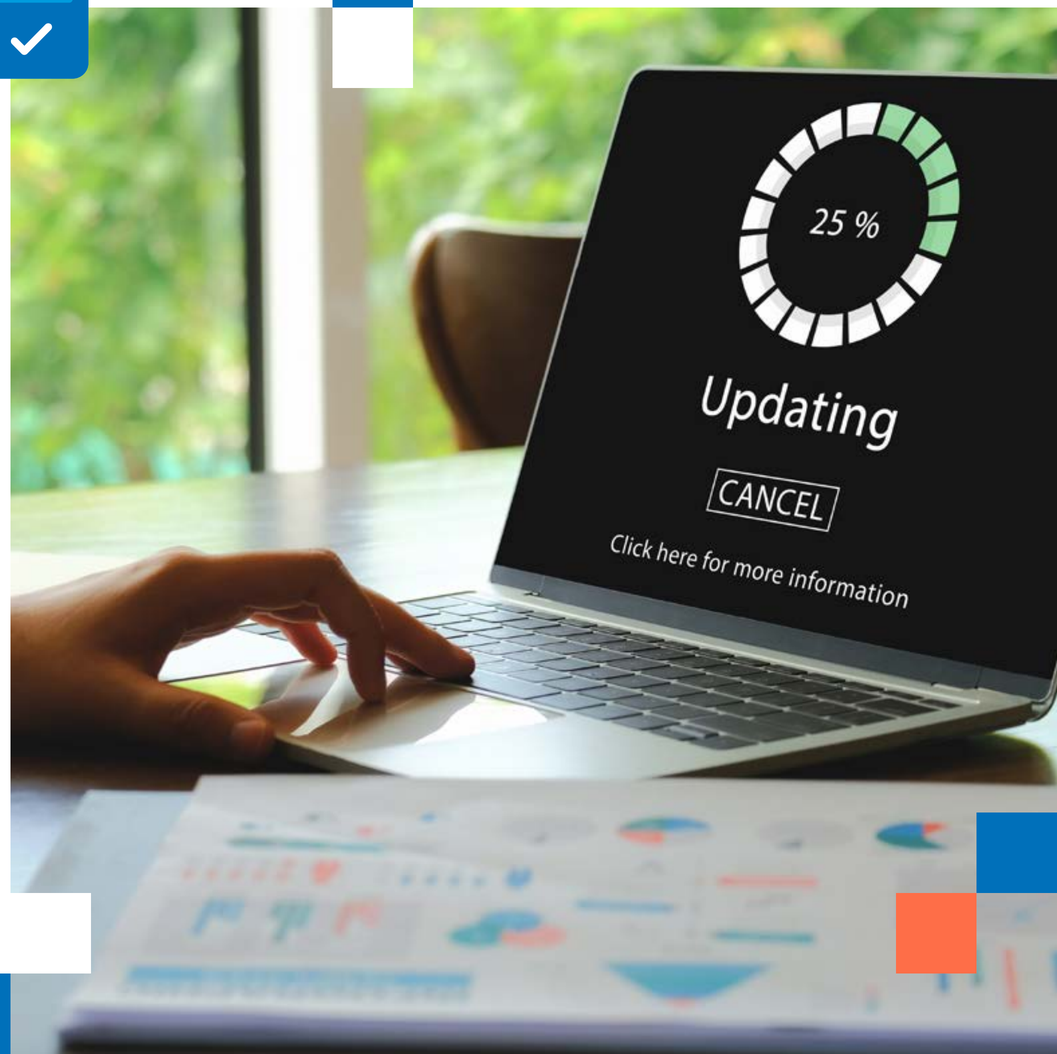
11. Insurance Business Magazine, Ten ways to protect your business from cyber attacks, 20 de marzo de 2021.

4 ACTUALIZA TU SOFTWARE PARA MEJORAR TU SEGURIDAD

El software obsoleto es una de las formas más fáciles de que los ciberdelincuentes ingresen a tus sistemas.[12] Estas son algunas de las medidas que debes tomar a fin de cerrar las puertas que no sabías tener abiertas para el crimen digital.

Aunque mantener actualizado tu sistema operativo (OS, por sus siglas en inglés) es una forma simple y eficaz de agregar una capa de protección a tu negocio, el 95% de los sitios web aún se ejecutan con software obsoleto con vulnerabilidades conocidas.[13] Los proveedores de OS actualizan continuamente sus sistemas con parches de seguridad para mantenerse a la vanguardia de las amenazas, los virus y el malware más recientes. Cualquier actualización del OS, por pequeña que sea, puede tener un gran impacto en la seguridad de tu negocio.[12]

El software antimalware y antispyware de nivel empresarial es otra forma de prevenir ataques que se dirigen a vulnerabilidades de software obsoleto, y también debes mantenerlos actualizados de forma regular.[14] También vale la pena señalar que el software gratuito, limitado y básico para los clientes es insuficiente debido a sus funciones y cobertura limitadas para las necesidades comerciales, lo que posiblemente te salga más caro a largo plazo.



12. Business 2 Community, Top 5 Risks of Using Outdated Software in Your Company, 14 de junio de 2021. **13.** Cybernews, 95% of websites run on outdated software with known vulnerabilities, 18 de marzo de 2021.
14. Business 2 Community, 6 Ways to Keep Your Business Data Safe, 26 de octubre de 2021.

5 CONOCE TUS PUNTOS VULNERABLES PARA AUMENTAR LA FORTALEZA CIBERNÉTICA

Los ciberdelincuentes son los ladrones del futuro. Saben cómo aprovechar la tecnología y la innovación, pero como un carterista de la vieja escuela, se enfocan en los puntos vulnerables de la víctima. Por ejemplo, cuando el tráfico de Internet aumentó en el espacio de los videojuegos y las criptomonedas, los ciberdelincuentes sabían que los equipos de seguridad se verían demasiado abrumados por este incremento como para atraparlos a todos.[15]

Los ciberdelincuentes usan estrategias sofisticadas para realizar ataques extremadamente rentables, por lo que estar informado y preparado es clave. Conoce tus vulnerabilidades y, lo más importante, no subestimes a los criminales digitales.

Un punto débil con el que la mayoría de los negocios pueden identificarse son los eventos de compras estacionales de mayor tráfico como el Hot Sale y El Buen Fin. Aumentan las ventas, pero también las distracciones y los ciberdelincuentes saben que estas son un factor a su favor.

En el otro extremo del espectro, el tráfico inusualmente bajo puede representar otro punto vulnerable. Cuando el sector del transporte experimentó una caída significativa en el tráfico debido a COVID-19, los ciberdelincuentes fueron tras las cuentas inactivas de los clientes para obtener los puntos de recompensa y los datos de pago.[15]

Implementar las protecciones adecuadas durante tus temporadas altas te permite disfrutar de tus ganancias en paz, y mantener la guardia cuando el negocio va lento le quita oportunidades a los estafadores.

15. Sift, Exposing the Multi-billion Dollar Fraud Economy, primer trimestre de 2021.

REFUERZA TU SEGURIDAD DIGITAL CON PAYPAL

El aumento del eCommerce y el ciberdelito catapultó la seguridad digital al primer plano en todo el mundo. Conforme el fraude continúa volviéndose más sofisticado y frecuente, tener un socio de pagos confiable ya no es opcional, sino esencial. PayPal te brinda tranquilidad con cada transacción. Nuestra poderosa red procesa de forma segura más de 10 millones de pagos al día y se vuelve más inteligente con cada transacción. Obtén las herramientas que necesitas para vender de forma segura y confiable en todo el mundo.

Empezar ahora →