

Kaspersky revela cómo verificar si las tiendas online priorizan la seguridad y no ponen en riesgo los datos de los usuarios

[Multimedia](#)

Con motivo del Día Mundial de los Derechos del Consumidor, Kaspersky recuerda la importancia de tener en cuenta la seguridad en las tiendas y plataformas online a la hora de hacer compras

El comercio electrónico está experimentando un crecimiento significativo en España, con cada vez más ciudadanos optando por las tiendas online para satisfacer sus necesidades de consumo. De hecho, los últimos datos publicados por la [Comisión Nacional de los Mercados y la Competencia](#) (CNMC) revelan que el comercio electrónico en España alcanzó los 20.492 millones de euros en el segundo trimestre de 2023, un 12,7% más en comparación con el mismo periodo de 2022.

Esta tendencia al alza se debe a diversos factores, como la facilidad de realizar compras con un solo clic, la posibilidad de hacerlo desde la comodidad del hogar sin tener que esperar largas colas, y la integración de la tecnología en la vida cotidiana. Esta última permite a los consumidores acceder fácilmente a una amplia gama de productos desde sus smartphones, brindando la flexibilidad de comprar rápidamente desde cualquier sitio y a cualquier hora.

Sin embargo, esta evolución no ha estado exenta de desafíos, particularmente en lo que respecta a la ciberseguridad y la protección de datos, según Kaspersky. Por ello, con motivo del Día Mundial de los Derechos del Consumidor, que se celebra este 15 de marzo, es importante tener en cuenta la seguridad en las compras online. En este sentido, la confianza mutua entre los usuarios y las plataformas o tiendas online desempeña un papel fundamental. Los usuarios deben adoptar medidas de protección, como el uso de contraseñas seguras y la atención a posibles señales de fraude para no caer en estafas como el robo de identidad o el phishing.

No obstante, la responsabilidad de garantizar la protección de los datos personales de los consumidores no solo debe recaer en estos últimos, sino también en las propias plataformas o tiendas online a las que facilitamos datos sensibles, personales y financieros. Por ello, para promover una experiencia de compra online segura y confiable, Kaspersky ofrece algunas claves tanto para los usuarios como para las empresas:

Para los usuarios:

- Comprobar el certificado SSL (indicador de que un sitio web es seguro para comprar). Antes de introducir cualquier información personal en una página web, hay que asegurarse de que tenga ese certificado. Busca el icono del candado en la barra de direcciones del navegador o verifica que la URL comienza con "https://" en lugar de "http://". Además, también es importante ver que la tienda o plataforma tenga una política de privacidad clara que explique cómo se manejarán los datos personales.
- Evitar ofertas demasiado buenas. Si un sitio web parece estar vendiendo ropa de diseño, joyas o aparatos electrónicos por bastante menos que el precio de venta habitual, hay que analizar si no es demasiado bueno para ser verdad. Puede ser que termine pagando por réplicas o productos falsos.
- Buscar una dirección y un número de teléfono. Los sitios web legítimos suelen proporcionar información de contacto, como una dirección física y un número de teléfono. El usuario debe verificar esta información para confirmar la autenticidad del sitio.
- Comprobar errores ortográficos y gramaticales. Por lo general, las marcas se aseguran de que los textos y las imágenes en sus sitios web sean de buena calidad. Si un sitio web está mal escrito y tiene muchos errores ortográficos o gramaticales, puede ser una señal de que no es real. Otros signos de alerta pueden ser las imágenes de mala calidad, que no tenga una política de devolución y que no se puedan dejar opiniones.
- Escribir la URL directamente en la barra de direcciones. Los estafadores de phishing intentan que los usuarios hagan clic en enlaces maliciosos en correos electrónicos o resultados de búsqueda. Esto lleva a sitios web falsos donde los usuarios pueden revelar información sensible a los cibercriminales. Por ello, es mucho más seguro escribir la URL en la barra de direcciones del navegador.
- Evitar usar redes públicas. Es importante utilizar una VPN (red privada virtual) para cifrar los datos cuando se utilice redes Wi-Fi públicas para aumentar la seguridad de sus transacciones online.

Para las plataformas y tiendas online:

- Implementar medidas de seguridad robustas. Es esencial que las tiendas online inviertan en tecnología de seguridad informática de última generación. Esto incluye la adopción de firewalls, sistemas de detección de intrusiones y cifrado de datos. Estas medidas protegen los datos sensibles de los usuarios contra posibles amenazas.
- Garantizar la transparencia. Una política de transparencia en relación con la privacidad de los datos es crucial para generar confianza entre los clientes. Las tiendas online deben proporcionar información clara y accesible sobre sus políticas de privacidad, qué datos recopilan, cómo los utilizan y con quién los comparten.
- Ofrecer métodos de pago seguros. La seguridad en las transacciones financieras es fundamental para una experiencia de compra en línea sin preocupaciones. Las tiendas online deben implementar métodos de pago confiables que minimicen el riesgo de fraude y robo de información financiera. En este sentido, es clave la adopción de pasarelas de pago seguras y el cumplimiento de estándares de seguridad como PCI DSS - normas de seguridad que incluyen requisitos para la gestión de la seguridad, políticas, procedimientos, arquitectura de redes, diseño de software y otras medidas de protección fundamentales-.
- Colaborar con las autoridades. La colaboración con las autoridades y

organismos reguladores es fundamental en la lucha contra el cibercrimen y la protección de los datos de los consumidores. Las tiendas online deben participar activamente en iniciativas para combatir el fraude online, compartir información relevante con las autoridades competentes y cumplir con las regulaciones de protección de datos vigentes.

"Al tiempo que aumenta el uso del comercio online, también surgen desafíos en términos de seguridad y protección de datos. Por eso, es vital que tanto usuarios como plataformas tomen medidas para asegurar una experiencia de compra sin riesgos. La confianza entre ambas partes y la transparencia en el manejo de información son clave para garantizar un entorno seguro en el mundo del comercio electrónico", afirma Marc Rivero, Lead Security Researcher de Kaspersky.
