Publicado en Madrid el 26/10/2020

Esta es la seguridad que brindan los principales métodos de pago online a los datos bancarios

Manuel Prieto, CEO de Easy Payment Gateway, recuerda la importancia de que el usuario conozca las ventajas e inconvenientes de cada una de estas soluciones para que las transacciones sean lo más seguras posibles

A pesar de que el ecommerce ha experimentado un crecimiento extraordinario a raíz del COVID-19, muchos usuarios siguen preocupados por la seguridad de sus datos a la hora de realizar un pago en Internet. Pero ¿sabe realmente el usuario qué protección brindan a su información las diversas soluciones de pago que tiene a su disposición?

“Nunca antes hemos tenido tantas opciones a la hora de abonar una transacción online. A la tarjeta de crédito y al contrarrembolso hoy se le añaden las monedas virtuales, apps e, incluso, servicios de terceros. El usuario debe conocer las ventajas y los inconvenientes de cada una de estas alternativas para que sus transacciones sean lo más seguras posibles”, asegura Manuel Prieto, CEO del agregador de servicios de pago y gestión del fraude europeo Easy Payment Gateway.

Por ello, y con motivo del Mes Europeo de la Ciberseguridad, el experto hace un repaso de los métodos más utilizados en las compras online y los aspectos a tener en cuenta para que las transacciones sean lo más seguras posibles:

- Monedas virtuales. Las criptomonedas se han convertido en el medio de pago preferido por algunos como alternativa al dinero tradicional. Las operaciones abonadas con las criptomonedas deben ser verificadas y registradas en un libro público con la cantidad y el domicilio del monedero virtual del remitente y del destinatario. Asimismo, están basadas en una sofisticada combinación de técnicas criptográficas, lo que proporciona un elevado grado de seguridad para comprar con total tranquilidad.

- Plataformas de pago. Las plataformas de pago como PayPal o Amazon Pay, que actúan como intermediarios entre el cliente y el vendedor, evitan que el usuario tenga que proporcionar sus datos, como el número de su tarjeta de crédito, a aquellos los sitios web en los que realiza sus compras. Esto es interesante cuando el usuario adquiere productos o servicios en sitios con los que no está familiarizado. No obstante, es importante señalar que, aunque no tiene que introducir sus datos en cada una de las webs, sí que deben que compartirlas con la plataforma, por lo que es conveniente que conozca las medidas de seguridad y las garantías que ofrece cada una de ellas en caso de fraude.

- Tarjetas bancarias. Esta es la forma de pago más extendida en el comercio electrónico en España. El estudio de IAB de 2020 revela que un 85% de los usuarios elige este método para abonar sus compras online. A su favor tienen que es un medio perfectamente conocido por el cliente y que se utilizan de forma habitual en el día a día. Igualmente, con la aprobación de la directiva europea sobre servicios de pagos electrónicos (PSD2), el usuario tiene que verificar su identidad con un código enviado a su smartphone, una clave que solo conoce él o un parámetro biométrico como la huella dactilar. Además,

el CEO de Easy Payment Gateway señala que “este método puede ser, incluso, más seguro si se utiliza la tecnología de tokenización. Se trata de un sistema que convierte los datos más sensibles del titular de la tarjeta en un código único (token) para cada transacción, de manera que se evita que los datos bancarios sean interceptados o robados por ciberdelincuentes”.

-Smartphone. El móvil se ha convertido en una extensión del usuario y son cada vez más quienes realizan sus compras a través del smartphone, que brinda la comodidad de adquirir lo que se necesite desde cualquier lugar en el que se disponga de conexión a Internet. La variedad de apps -tanto de empresas como Amazon como de las entidades bancarias- junto con el hecho de que toda la información financiera esté vinculada al dispositivo, hace tremendamente cómodo y sencillo su uso. Sin embargo, conviene no configurar estas apps o realizar compras a través de las mismas si se está conectado a redes wifi públicas, en las que es fácil ser víctima de una suplantación. Manuel Prieto también recomienda reforzar la seguridad del dispositivo con contraseñas complejas o métodos biométricos, que impidan el acceso a los datos bancarios almacenados en el smartphone en caso de pérdida o sustracción.

Para reforzar al máximo la seguridad e integridad de los datos facilitados por sus clientes, las empresas también deben contar con estrictas medidas de seguridad o empresas que, como Easy Payment Gateway, ofrecen asesoría en este sentido. “Los negocios tampoco deben olvidar que ellos mismos pueden ser víctimas de fraude por parte de algunos ciberdelincuentes a través de tarjetas bancarias robadas o sin fondos. Para ello, ofrecemos sencillas reglas que ayudan a reducir este tipo de fraude entre un 40 y un 75%”, concluye el CEO de la compañía.

Datos de contacto:
Everythink PR
651366974

Nota de prensa publicada en: Madrid

Categorías: Nacional Internet General Digital Software Seguridad