8 engaños más comunes en Facebook Marketplace durante 2023

ESET, compañía especialista en detección proactiva de amenazas, analiza cuáles son las modalidades de estafa más comunes que se observaron en Facebook Marketplace durante este año y a qué señales deberían prestar atención los usuarios para poder identificarlas y no caer en los engaños de los cibercriminales.

“Marketplace se convirtió en una de las plataformas preferidas para las compras y ventas online. Y, como sucede en tantos otros casos, cuando hay algo que llama la atención y es usado masivamente también atrae a los ciberdelincuentes. Es por esta razón que cada vez son más las estafas y engaños que circulan en esta plataforma.”, señala Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

ESTAFAS MÁS COMUNES

Artículos defectuosos: puede suceder que un vendedor publique un producto con fotos que lo presentan en perfectas condiciones, pero que una vez entregado en realidad esté roto. Esto es particularmente complicado cuando se compran artículos electrónicos, porque por lo general no se pueden evaluar todas sus funciones antes de la compra. Lamentablemente, existen posibilidades de que esto suceda, ya sea por parte a un vendedor sin escrúpulos como por un estafador profesional.

Artículos falsos: hay casos en los que el producto puede que sea una falsificación. La ropa de diseñador, los perfumes, las joyas y los cosméticos son blancos comunes de falsificación. Todos están buscando una buena oferta, pero cuando parecen demasiado buenas para ser verdad, por lo general se trata de un engaño.

Estafas de Google Voice: Marketplace también es aprovechado para realizar fraudes en otras plataformas. Un engaño muy común es intentar robar cuentas de Google Voice o crearlas con el número de teléfono de la víctima. Los estafadores se contactan con un vendedor por el supuesto interés en un artículo para intentar llevar la conversación a una plataforma no monitoreada, como puede ser WhatsApp. Allí le solicitan que comparta un código que le enviarán a su teléfono para verificar que es una persona legítima. Ese código es el de la verificación en dos pasos (2FA) de Google Voice, que una vez en poder de los estafadores pueden

crear una cuenta asociada a ese número de teléfono.

Sobrepago: el estafador se hace pasar por un comprador y reclama a un vendedor que pagó demás por un artículo que compró. Enviará una captura de pantalla donde muestra la supuesta transacción por la compra y solicitará que reintegren la diferencia. Obviamente, en ningún momento se realizó un pago y si el vendedor cayó en la trampa habrá perdido el dinero sin posibilidad de reembolso.

Compra que nunca llega: otro engaño consiste en vender un artículo, cobrar el dinero pero no entregarlo al comprador. Esto solo se aplica a los artículos enviados desde fuera del área local del comprador.

Phishing y Falsos sorteos: una forma de obtener información de las víctimas es enviar correos de phishing con supuestas ofertas y sorteos en la plataforma. La víctima, desprevenida, hará clic en el enlace y completará un formulario con información personal creyendo que así estará participando por artículos de lujo u otras ofertas especiales. Por supuesto, los estafadores solo quieren información personal para cometer fraude de suplantación o robo de identidad.

Estafa de los seguros: quienes venden artículos muy costosos en Facebook Marketplace pueden ser contactados por estafadores que se hacen pasar por compradores dispuestos a pagar el costo por el envío del artículo, y hasta envían una factura falsa como prueba. Solo hay un problema: piden que el vendedor pague un pequeño cargo por un supuesto seguro, que generalmente es un monto pequeño en comparación con el precio del artículo, lo que persuade al vendedor de aceptarlo.

Ofertas engañosas: los estafadores anuncian un producto de alta calidad a un precio tentador, pero en el momento que una persona cree haber sido beneficiada le avisan que el producto ya no está disponible, aunque nunca lo haya estado, y le ofrecerán al comprador un artículo similar por un precio mucho más elevado o una alternativa inferior.

CÓMO DETECTAR ESTE TIPO DE ESTAFAS

Al igual que en ante otras modalidades de engaños en línea, la clave es mantenerse escépticos y en alerta. Para ello, ESET comparte 10 consejos muy útiles a la hora de navegar y/o comprar por Facebook Marketplace:

Inspeccionar los artículos antes, y comprar solo a vendedores locales.

Establecer como punto de encuentro un lugar público, bien iluminado y en lo posible durante el día.

Revisar los perfiles de compradores/vendedores para conocer las calificaciones y mantenerse alerta si los perfiles se han creado recientemente.

Verificar el precio de mercado de los artículos y, si hay una diferencia significativa entre este y el precio de venta, estarse atento al hecho de que puede ser falsificado, robado, defectuoso, etc.

Tener cuidado con las ofertas y obsequios, y nunca ingresar datos personales para acceder a ellos.

Solo usar métodos de pago confiables a través de Facebook Messenger (PayPal, Facebook Checkout), ya que ofrecen una forma de disputar un pago. Los estafadores suelen solicitar tarjetas de regalo (gift cards) así como transferencias bancarias y pagos a través de diferentes servicios.

Mantener la conversación en Facebook: a los estafadores les gusta mudar la charla a otra plataforma donde resulta más fácil estafar a las personas, porque allí no habrá nada que respalde a la víctima.

En caso de ser vendedor, nunca enviar artículos antes de que se haya realizado el pago.

Cuidado con los cambios en el precio de cotización.

No enviar códigos de verificación (2FA) a posibles compradores.

Si sucede lo peor y hay sospechas de que ser víctima de un fraude, se debe denunciar al vendedor y reportarlo de inmediato en Facebook Marketplace.

“Por todo lo mencionado anteriormente es necesario adoptar buenas prácticas de seguridad, prestar atención a los indicios de que una oferta puede tratarse de una estafa, e informarse sobre las metodologías que utilizan los cibercriminales para perpetrar sus ataques. Así, es posible que los usuarios eviten comprarse un problema”, concluye Gutiérrez Amaya, de ESET Latinoamérica.

Con información de altadensidad.com