CIENCIA Y TECNOLOGÍA / TENDENCIAS

Ciberestafas en Facebook: eventos ficticios para robar tus datos

El Ciudadano · 9 de noviembre de 2015

Uno de los últimos timos que circulan en Facebook utiliza la imagen de la marca de gafas Ray-Ban para obtener los datos personales de los usuarios

En las últimas semanas está circulando una nueva **estafa** por **Facebook**: una invitación a un evento de **Ray-Ban** que envía alguno de los amigos que los usuarios tienen en la red social. Muchos habrán puesto en duda esta oferta de gafas de la conocida firma, pero otros habrán caído en la trampa. Sí, se trata de un timo y la mejor opción es ignorar la invitación, según informa Kaspersky Lab.

Son muchos los formatos que se utilizan para ciberestafar en las redes sociales, como el vale regalo de la tienda de ropa Zara, entre otros, pero el funcionamiento suele ser el mismo:

1- Crean páginas simulando empresas y utilizan un gancho potente. En este caso, gafas Ray-Ban a menos de 25€.

2- Invitan a compartirlo, porque ¿quién no se fía de la recomendación de un amigo?

3- Llevan a los usuarios a una página de phishing en la que simulan ser la web o un retailer de la marca.

4- Allí solicitan sus datos personales y rematan la estafa… En este caso, simulan incluso ser una tienda online, por lo que te solicitan los datos del pago.

En caso de haber sido víctima de la estafa, el usuario ha de contactar con su banco para tratar de anular el pago y comprobar si han hecho uso de las tarjetas para cancelarlas cuanto antes. Si ha realizado el pago a través de Paypal, debe utilizar los mecanismos de protección del comprador.

Además, puede denunciar la situación a la Guardia Civil y la Policía y difundir la estafa para evitar que otros amigos se vean afectados también.

Cuatro recomendaciones para no caer en estas estafas:

-Ser cauteloso y desconfiar siempre de promociones y concursos.

-En caso de ver una promoción en redes sociales en la que se desee participar, una opción segura es preguntar en el perfil oficial de la empresa en Facebook o Twitter si la promoción es suya y es real.

-Prestar atención a las urls de las web a las que redirige la promoción.

-Mucha atención también con los correos electrónicos. En este caso hay que comprobar remitente y fallos de ortografía. Si viene un adjunto, hay que asegurarse bien antes de descargarlo, es probable que sea *malware*.

Fuente: La Vanguardia

Fuente: El Ciudadano