

Alerta por el nuevo fraude nigeriano de WhatsApp

La app de mensajería WhatsApp no solo se ha convertido en la favorita de los usuarios para comunicarse con sus seres queridos, compañeros de trabajo o incluso personas desconocidas, sino que también lo es de los ciberdelincuentes debido a las facilidades que les ofrece esta plataforma para llevar a cabo sus estafas.

Esto se debe a que con un presupuesto mínimo, realmente solo necesitan un número de teléfono para robar los datos personales de sus víctimas, e incluso su dinero. Son muchísimas las técnicas que llevan a cabo, y lo peor de todo es que casi cada día surge una nueva variante que si no estamos atentos podemos caer en ella.

Ahora, la Asociación Española de Consumidores alerta de una oleada de mensajes de WhatsApp con falsas ofertas de negocio de inversiones. En el mensaje, que proviene de un número de teléfono con prefijo de Nigeria, nos ofrecen la oportunidad de unirse a un equipo de trabajo donde con tal solo 20-30 minutos al día puedes tener ganancias de entre 350 y 3.500 euros diarios, además de un bono de bienvenida de 800 euros.

Lo mejor de todo es que no se requiere experiencia, aunque en el mensaje no indican en ningún momento de qué se trata este trabajo, pero con la emoción y cegados por esta oportunidad de conseguir dinero fácil y rápido muchos se apresuran a seguir las instrucciones.

Lo que tienes que hacer es enviar un mensaje a la empresa en cuestión, pero no vale en este chat de WhatsApp, sino que tienes que seguir un enlace (fraudulento) para hacerlo, y si picas y pulsas sobre este link se te abrirá un formulario a completar con todo tipo de información privada, que servirá a los atacantes a llevar a cabo más estafas o incluso suplantar tu identidad.

Cómo prevenir esta estafa de WhatsApp

Desconfía de mensajes inesperados: Las empresas legítimas rara vez solicitan información confidencial por SMS.

Verifica la fuente: Si el mensaje dice ser de una empresa que conoces, contacta directamente con la empresa a través de sus

canales oficiales

No hagas clic en enlaces sospechosos: Los enlaces en los mensajes SMS pueden redirigirte a sitios web falsos diseñados para robar tu información.

No respondas al mensaje: Incluso responder con un «NO» o «STOP» puede confirmar a los estafadores que tu número de teléfono es válido, lo que puede llevar a más mensajes de spam o smishing. Instala un filtro de spam para SMS.

Con información de [El Economista](#)