Alerta usuarios de WhatsApp: la nueva modalidad de estafa a través de falsas ofertas laborales

31/08/2023

Los ciberdelincuentes están siempre a la pesca de nuevas víctimas y las estafas virtuales crecen cada vez más en **Argentina**. Ahora hay una **nueva modalidad**, proveniente de México, que ya cobró sus primera víctimas en el país y se corre el riesgo de que se expanda en plataformas de mensajería y redes sociales.

En esta ocasión, se trata de una **falsa oferta laboral** de modo freelance a través de **WhatsApp** en la que los ciberdelincuentes envían mensajes con la propuesta de pagar hasta **más de medio millón de pesos** por día a cambio de darle «Me gusta» a videos de YouTube y publicaciones en Instagram.

Estafas virtuales a través de Whatsapp. Twitter.

La trampa consiste en el **envío de enlaces de videos** o publicaciones para que los usuarios vean, y luego, antes de realizar el primer pago por el "trabajo", el pedido de un **depósito inicial para habilitar el sistema de recompensas.** Cuando la víctima realiza la transferencia, **los delincuentes la bloquean** y ya no hay manera de recuperar el dinero.

Este tipo de estafa comenzó en México. Pero en las últimas semanas ya son varios los usuarios argentinos que recibieron este tipo de propuestas en sus teléfonos. Para que la gente muerda el anzuelo y caiga en la trampa, los ciberdelincuentes les envían **capturas de pantallas en las que muestras las operaciones** y pagos realizados a otros supuestos participantes. Muestran cómo comenzaron ganando poco dinero, hasta llegar a cifras de hasta **600.000 pesos diarios.**

Como funciona la estafa

Según las denuncias de los usuarios en redes sociales, esta nueva modalidad de fraude virtual tiene diferentes versiones. Por lo general, **prometen el pago de 600 pesos por cada dos tareas** que los supuestos »empleadores» asignan. Los »trabajos» consisten en **dar like a un video o empezar a seguir ciertos perfiles en Instagram.**

Así son las nuevas estafas en Whatsapp. Twitter.

Para verificar esto, los usuarios deben enviarles una captura del like. Y luego, para empezar a cobrar, los delincuentes **piden un depósito** que sirve, engañosamente, »para habilitar el sistema y seguir recibiendo tareas». Pero la realidad es que después de esa transferencia, los ciberestafadores **se borran y bloquean a la víctima.**

Otra versión, que también fue denunciada, consiste en solicitar al usuario que se baje una aplicación para pasar los

datos de la cuenta a dónde recibirán los pagos. Con este médico, los ciberdelincuentes **logran acceder a contraseñas y datos bancarios** y consiguen vaciar las cuentas de sus víctimas.

Precauciones a tener en cuenta para evitar esta estafa

- En primer lugar, para detectar este tipo de fraude hay que **prestarle atención a los mensajes**: generalmente **están mal escritos y tienen errores de puntuación y gramaticales**, producto de la mala traducción.
- "Cuando la limosna es grande hasta el santo desconfía", dice el refrán. Es vital dudar de este tipo de propuestas que, **por muy poco esfuerzo, prometen recompensas ridículas** por miles de pesos.
- Es de suma importancia **no revelar información confidencial** (datos bancarios, contraseñas, etc.) por correo electrónico, redes sociales, mensajes de texto, llamadas telefónicas no solicitadas, ni compartirlas por ninguna aplicación.
- **Verificar siempre la dirección URL** de los enlaces antes de hacer clic y no descargar aplicaciones de dudosa reputación. Existen diferentes apps que los delincuentes usan para tomar control de los dispositivos de sus víctimas y acceder a sus home bankings.
- Asegurarse de que la **dirección comience con "https://"** . No navegar por sitios que utilicen el protocolo http y no el https (Protocolo de transferencia de hipertexto seguro).

Fuente – Canal 26