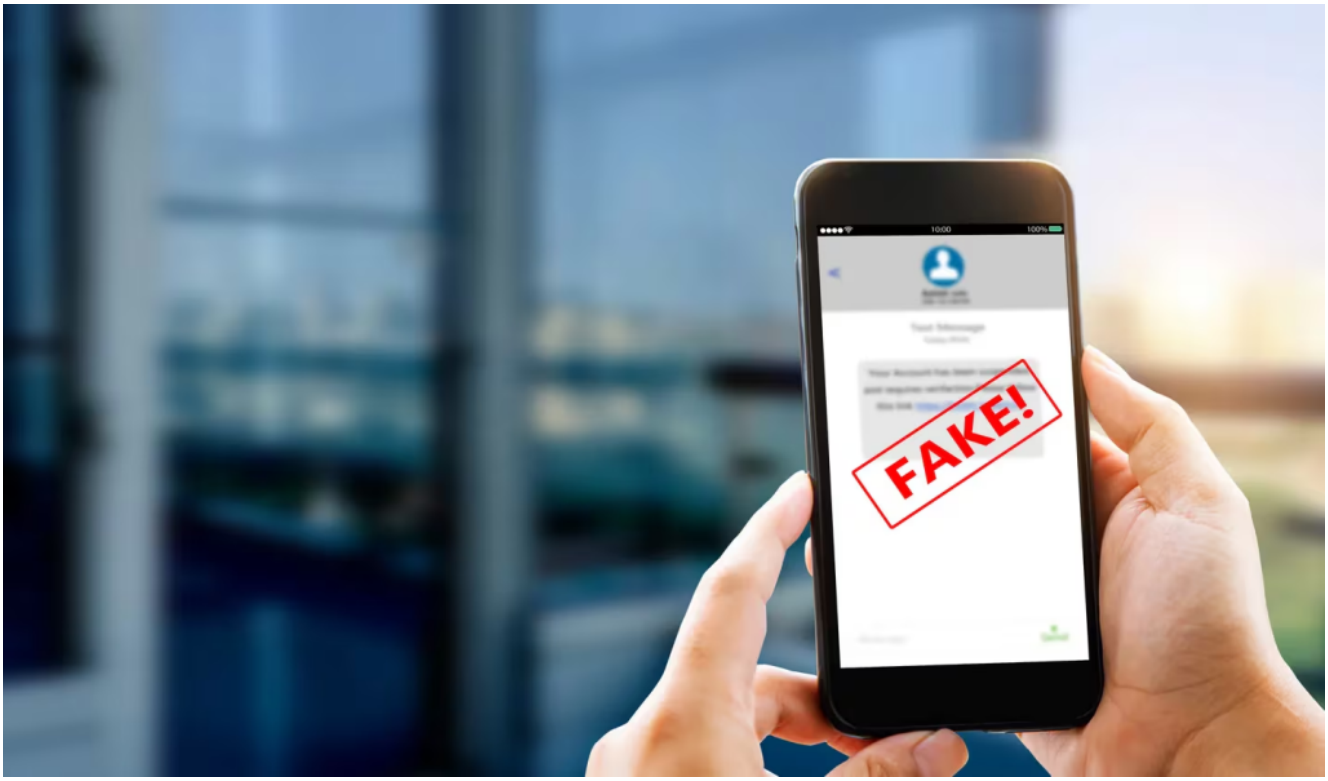
Qué es el Vishing: la nueva estafa que se lleva a cabo por WhatsApp

19/06/2024

Si bien la tecnología abrió las puertas para facilitar la vida en muchos aspectos, también trajo a colación nuevas formas de estafa. En el último tiempo, con el aporte de la inteligencia artificial, delincuentes cibernéticos crearon un nuevo modus operandi: el vishing.

Este fraude **combina la clonación de voces mediante inteligencia artificial y el engaño digital**, afectando ya a centenares de argentinos y miles de personas alrededor del mundo.

Según una encuesta reciente de McAfee, una compañía de software especializada en seguridad informática, indica que e**l 77% de las víctimas de vishing terminan enviando dinero a los estafadores**.



¿Cómo es el modus operandi de esta técnica de estafa?

Según informaron varias víctimas, una persona **se comunica con ellos a través de una llamada por WhatsApp, presentándose como un empleado de su banco** o una entidad confiable.

Al obtener la atención de la víctima **le hace creer que necesita alguna acción inmediata en su cuenta bancaria**. De esta forma es guiada para que le proporcione el código que le llega mediante mensaje de texto. En ese momento es cuando los ciberdelincuentes **toman el control y cometen el fraude**.

En el último tiempo, se registraron varios casos de este tipo de estafa. Según detallaron medios locales de Jujuy, la titular de la Unidad de Delitos Económicos Complejos (UDEC), Ana Inés Salinas Odorisio, dirigió una serie de allanamientos en la provincia relacionados con estafas telefónicas.

A través de estos procedimientos, pudieron dar con la detención de varias personas involucradas en una asociación

ilícita que empleaba técnicas de vishing para persuadir a sus víctimas de transferir dinero, utilizando los fondos para recargas telefónicas y compras personales.

¿Cómo evitar caer en la trampa?

La pérdida monetaria es solo una de las consecuencias del vishing. Otra, quizás más grave a lo largo del tiempo, es **el uso de tu identidad para otras estafas a otros usuarios**.

Los especialistas dan algunas **recomendaciones para evitarlas y no pasar un mal momento**.

- Ante un llamado sospechoso, **verificá siempre las fuentes**. Si se menciona a un conocido o familiar, contactarse por otra vía para saber si es real la situación. Lo mismo con un banco o cualquier otra empresa.
- **Desconfiar de la procedencia del llamado**. Si resulta dudoso, terminar la comunicación rápidamente.
- Comunicate con la empresa mencionada por los estafadores para seguir los canales oficiales y **denunciá lo sucedido**.
- **No ingresar datos personales en sitios utilizando enlaces que llegan por correo electrónico**, podrían ser fraudulentos. Tener cuidado con los enlaces sospechosos y **asegurarse siempre de estar en la página legítima** antes de ingresar información de inicio de sesión. **Leer cada correo electrónico recibido con cuidado**.
- **No brindar ningún dato personal** (usuarios, claves, contraseñas, pin, Clave de la Seguridad Social, Clave Token, DNI original o fotocopia, foto, ni ningún tipo de dato), **por teléfono, correo electrónico, red social, WhatsApp o mensaje de texto**.

En la página web de algunos bancos, empresas y otras instituciones **hay instrucciones sobre estas amenazas**, listado de las más frecuentes y otros consejos para prevenir las estafas. Es cuestión de estar atentos y no brindar nunca datos sensibles a través de estas vías.

Fuente: TN