Nunca digas esta palabra cuando te llame un número desconocido: evitá las estafas

13/09/2024

Las **estafas** virtuales se convirtieron en un problema común en la actualidad. Los estafadores se especializan en engañar a personas desprevenidas mediante diversas tácticas, muchas veces aprovechando el anonimato que proporcionan las llamadas de números desconocidos o marcados como “posible spam”.

Uno de los métodos más utilizados para llevar a cabo estas estafas implica una simple palabra: “sí”. Este artículo explora por qué es crucial evitar esta palabra y cómo protegerse contra tales fraudes.

El riesgo de las estafas virtuales

Cuando un estafador llama y solicita respuestas afirmativas a preguntas aparentemente inofensivas, el objetivo es obtener una grabación del “sí” de la víctima. Esta grabación puede ser utilizada para autorizar transacciones fraudulentas o inscribir a la persona en servicios que no ha solicitado.

Evitá las estafas sabiendo qué palabra no usar.

A veces, las preguntas hechas por los estafadores incluyen confirmaciones de identidad, detalles sobre tarjetas de crédito o aceptación de ofertas. Los estafadores confían en que la víctima, al sentirse cómoda y sin sospechas, responderá afirmativamente, lo que puede poner en riesgo su seguridad financiera y personal.

Las grabaciones de estas respuestas pueden ser presentadas como pruebas de consentimiento en situaciones de reclamos o disputas. Por ejemplo, **si un estafador tiene grabada la palabra “sí” de una víctima**, puede utilizarlo para autorizar cargos en su cuenta bancaria o para inscribirla en suscripciones no deseadas.

Cómo protegerse de las estafas virtuales

Para protegerse de estos fraudes, es fundamental tomar ciertas precauciones. Aquí algunos consejos efectivos:

- **Evitá Responder a Llamadas Sospechosas:** Nunca atiendas llamadas de números desconocidos o que tu servicio telefónico identifique como “posible spam”. Es preferible dejar que la llamada vaya al buzón de voz y analizar su contenido posteriormente.
- **Usá Aplicaciones de Bloqueo de Llamadas:** Existen aplicaciones que pueden bloquear automáticamente llamadas de números no deseados, reduciendo así el riesgo de ser víctima de estafas.
- **No Proporciones Información Personal:** No des ningún dato personal a fuentes que no consideres completamente confiables. Las instituciones financieras y empresas legítimas nunca solicitan información sensible a través de llamadas telefónicas no solicitadas.

- **Protegé tus Cuentas:** Utilizá contraseñas distintas para cada cuenta y activa el doble factor de autenticación para mayor seguridad. Las contraseñas deben ser

robustas, cambiarse con regularidad y no compartirse.

- **Mantené Actualizados tus Dispositivos:** Asegurate de que tu sistema operativo, navegador y aplicaciones estén siempre actualizados para protegerte contra vulnerabilidades.
- **Verificá el Origen de los Correos Electrónicos:** Comprobá que los remitentes coincidan con los dominios oficiales de las entidades o empresas antes de abrir cualquier enlace o archivo adjunto.
- **Evitá Redes Públicas y Desactiva Funciones Innecesarias:** No utilices redes públicas para realizar transacciones importantes y desactiva bluetooth, wifi o NFC cuando no sean necesarios para evitar conexiones automáticas.
- **No Compartas Códigos de Verificación:** No reveles códigos de verificación recibidos por correo electrónico o mensaje de texto, incluso si parece que provienen de una fuente legítima.
- **Utilizá Antivirus y Antimalware:** Tené un buen software antivirus y antimalware para detectar y neutralizar amenazas.
- **Desactivá Funciones de Localización y Multimedia Cuando No se Usan:** Desactivá la ubicación, la cámara y el micrófono cuando no los necesites para evitar que aplicaciones o servicios maliciosos accedan a ellos sin tu consentimiento.

Fuente: La Mañana de Neuquén.