Cómo funciona “Spoofing”, la estafa virtual para vaciarte la cuenta bancaria 5 en segundos

19/04/2026

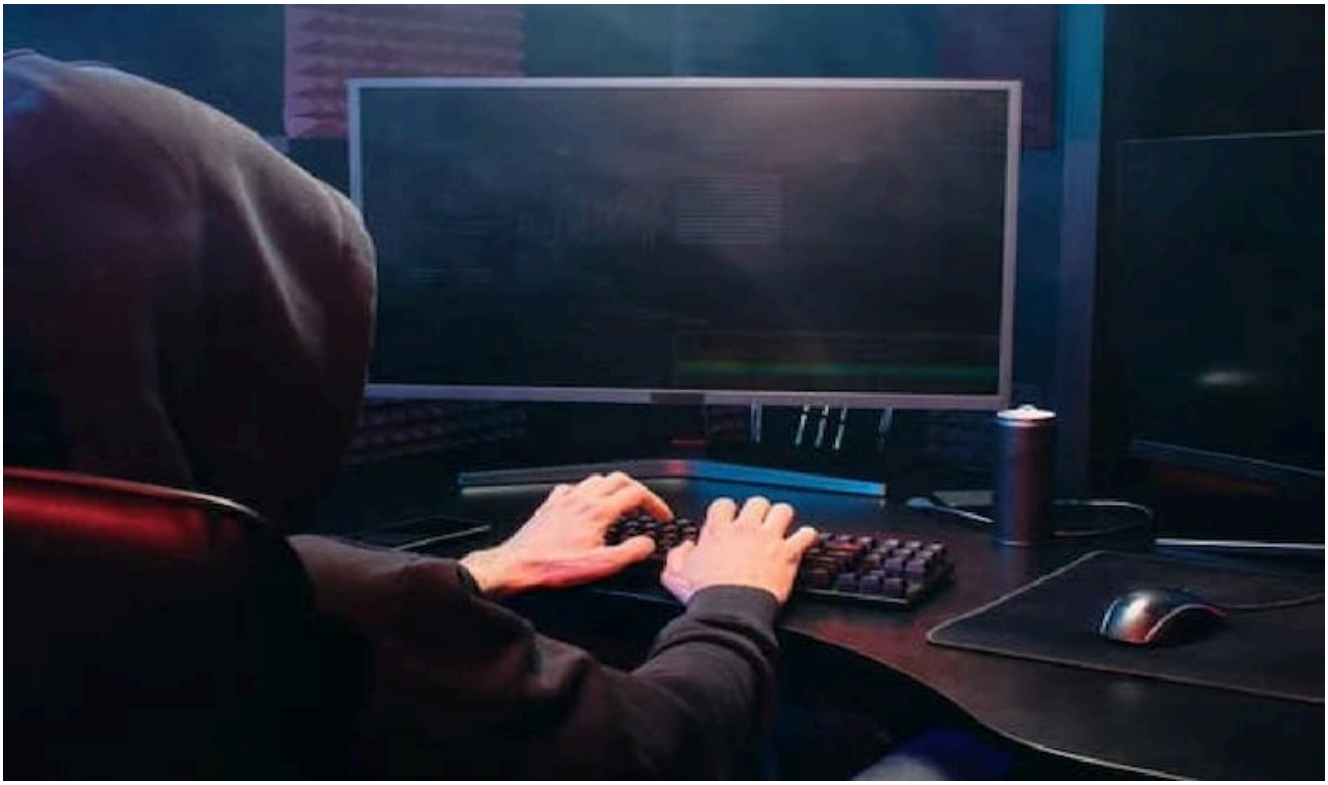
El **spoofing** es una de las modalidades de fraude digital que más preocupa en la Argentina. Se trata de una técnica en la que **los delincuentes se hacen pasar por personas, empresas o entidades reconocidas** para engañar a sus víctimas y robarles información sensible.

El objetivo de estos ataques es claro: **obtener datos bancarios, contraseñas o instalar software malicioso** en los dispositivos de los usuarios. Los especialistas advierten que el spoofing es cada vez más sofisticado y abarca distintas formas de engaño.

Cómo funciona el spoofing y por qué es tan peligroso

El spoofing es un concepto amplio que incluye **diversas técnicas de suplantación de identidad**. Puede aparecer en campañas de **phishing** (correos electrónicos falsos), **smishing** (mensajes de texto fraudulentos) y hasta en **llamadas telefónicas** que parecen venir de bancos o empresas conocidas.

En todos los casos, el atacante busca generar una **sensación de urgencia**: pide que la víctima complete una gestión rápida o aproveche una oferta exclusiva. Así, logra que la persona **ingrese datos personales en sitios web que simulan ser oficiales**, pero en realidad están controlados por los estafadores.



Los delincuentes buscan quedarse con tu dinero (Foto: Pexels).

La variedad de estos ataques sorprende por su alcance. Los delincuentes pueden usar **números de teléfono falsos** que aparecen en la pantalla del celular como si fueran de una entidad legítima. También existen variantes que

involucran **direcciones IP, sistemas de DNS, datos biométricos o GPS**. Todo está pensado para que la víctima confíe y caiga en la trampa.

Las páginas de destino suelen estar diseñadas para **imitar la estética de sitios reales**, lo que facilita el robo de dinero o información bancaria. Muchas veces, estas maniobras se combinan con el **pharming**, una técnica que redirige al usuario a páginas falsas sin que lo note.

Consejos clave para protegerse del spoofing

La principal defensa ante el spoofing es la **desconfianza metódica**. Si recibís una llamada de un banco que te pide datos personales, **no los brindes**: las gestiones bancarias nunca se hacen por teléfono a pedido de terceros. Es fundamental preguntar la identidad de quien llama y cortar la comunicación si hay dudas.

En el caso de los **mensajes de texto o correos electrónicos**, nunca hagas clic en enlaces directos. **Ninguna empresa seria solicita datos personales por mensaje**. Lo recomendable es **ingresar la dirección web manualmente en el navegador** y verificar que la URL sea la oficial.

Si un mensaje genera presión o urgencia para pagar una supuesta deuda, **mantené la calma y evitá actuar impulsivamente**. Ante comunicaciones extrañas de conocidos, prestá atención a la redacción: los ciberdelincuentes suelen cometer errores al imitar el estilo de las personas o empresas que suplantan.

Evitá darles tu información personal antes de comunicarte de forma directa con la empresa (Foto: Adobe Stock).

Qué hacer si sospechás de un intento de spoofing

- **No respondas ni brindes información personal.**
- **Cortá la comunicación y contactá directamente a la empresa o persona por canales oficiales.**
- **No ingreses a enlaces ni descargues archivos de mensajes sospechosos.**
- **Verificá siempre la dirección web antes de ingresar datos.**
- **Reportá el intento de fraude a las autoridades o a la entidad afectada.**

La prevención y la atención a los detalles son fundamentales para evitar caer en estas trampas digitales. **La seguridad informática depende, en gran parte, de la cautela de cada usuario.**

Fuente: TN