

# SPOOFING Y LAS ESTAFAS EN BANCOS

BOLETÍN INFORMATIVO ARLC/FT/FPADM Y OTROS ILÍCITOS



FUENTE:ANTILAVADODEDINERO / ALTONIVEL

La forma en que los criminales estafan a los usuarios es esta, con algunas variantes: El cliente recibe una llamada cuyo número es, presuntamente, de su banco. El delincuente dice que la cuenta del usuario ha sido vulnerada y pide datos para crear otra cuenta de 'seguridad' para trasladar los recursos; o en otros casos, le dicen al cuentahabiente que se pidió un préstamo a su nombre y fue transferido a otra cuenta, obviamente el usuario dice que no solicitó ningún crédito y, entonces, le pide devolver el préstamo, poniéndolo en otra cuenta.

En ambos casos se trata de un engaño, pero los clientes son más proclives en caer porque la llamada que reciben tiene el número del banco y, en ocasiones, el defraudador tiene los datos del cliente.

## ¿Qué es 'spoofing'?

Este fraude telefónico, que ha afectado a muchos clientes bancarios, se llama 'Spoofing' y ciertamente no es nuevo. Desde 2018 o antes ya se tenían registros de estafas mediante esta técnica.

El 'spoofing' consiste en robar la identidad del banco o institución hackeando el identificador de llamadas para que aparezca el nombre o número del banco del que la víctima es cliente.

**EN LOS ÚLTIMOS DÍAS, SE HAN DIFUNDIDO VARIAS QUEJAS DE USUARIOS POR INTENTOS DE FRAUDE, O ESTAFAS CONSUMADAS MEDIANTE TÉCNICAS SOFISTICADAS PARA ENGAÑAR A LOS CLIENTES, HACIÉNDOLES CREER QUE LAS LLAMADAS QUE RECIBEN SON DE SU INSTITUCIÓN FINANCIERA.**

Con el spoofing, los delincuentes usan información manipulada para hacerse pasar por representantes de bancos, aseguradoras, tiendas u otras instituciones para obtener información personal del cliente y así sacar dinero o hacer compras con sus cuentas y tarjetas.

Esta técnica es efectiva porque muchas veces se ganan la confianza de las víctimas pues, al ver que el número en la pantalla de su celular es el mismo del banco, piensan que efectivamente les hablan de la institución financiera, y les dan la información que les piden.

### **¿Insiders en los bancos?**

Además de usar esta técnica de suplantación de identidad, lo que más les ha sorprendido a muchos clientes es que los defraudadores tienen sus datos, es decir, su nombre y saben que son clientes del banco.

También hay otros casos en los que los defraudadores, ya con la información bancaria de la víctima, hicieron varios movimientos en sus cuentas, todos repetidos e inusuales, sin que el banco los detuviera.

Se afirma que estos fraudes se realizan con la colaboración de un 'Insider', es decir, una persona dentro de la institución bancaria con acceso a la información de los clientes.

Aunque no se ha podido comprobar la sospecha antes mencionada, muchos clientes se preguntan cómo los defraudadores tienen sus datos, aunque también es cierto que muchos de estos eligen números al azar y usan la misma historia de que su cuenta ha sido vulnerada, esperando que más de uno caiga en la trampa.

### **¿Cómo evitar caer en el spoofing?**

Según los testimonios de muchas personas, han perdido grandes cantidades de su dinero o inclusive sus ahorros. Desafortunadamente, las personas de la tercera edad componen una buena parte de las víctimas al caer en este tipo de estafas.

Es posible que no identifiquemos al momento un intento de 'spoofing', pero podemos combatirlo con estas sencillas acciones.

Si te llaman de un número que parece ser tu banco...

Primero pregúntate, ¿para qué me están llamando? Si no solicitaste algo de tu institución, no tendrían por qué llamarte, ni tú tienes un motivo para contestarles.

Segundo, si contestas el teléfono, desconfía de lo que te digan. Si afirman que hay movimientos inusuales en tu cuenta y te piden datos para supuestamente ayudarte, cuelga inmediatamente, no te enganches en su historia.

Tercero, mantén la calma. Estos estafadores son muy persuasivos y pueden convencer a muchos, hasta al más perspicaz. Al decirte que alguien hizo movimientos o compras con tu cuenta, nos invade una sensación de peligro y queremos resolverlo en el momento, ahí es cuando los delincuentes se aprovechan de las personas. Pero aún cuando creas en verdad que tu cuenta bancaria haya sido vulnerada, mantén la calma, no cedas a presiones y, por ningún motivo, des tus datos personales.

Por último, llama tú al banco. Si no caes en la trampa y cuelgas, seguramente el estafador volverá a llamar. No contestes y llama personalmente al banco y explícales la situación, así podrás saber si en verdad hubo movimientos inusuales, o se trataba de una estafa.