

Suplantación de Identidad Telefónica (*Spoofing*) y Cómo Evitarla

El término “*Spoofing*” (en inglés) hace referencia a la suplantación de identidad en la pantalla telefónica del usuario. Ocurre cuando quien genera la llamada falsifica, deliberadamente, la información transmitida al identificador de llamadas (*caller ID*, en inglés), con el objeto de ocultar la identidad real de la persona que ha iniciado dicha llamada. *Spoofing* es una maniobra usada para intentar obtener información personal valiosa y luego usarla en actividades ilegales o comercializarla de manera ilegal. Las leyes estadounidenses, incluyendo las normas de la Comisión Federal de Comunicaciones (*Federal Communications Commission*, FCC por sus siglas en inglés), prohíben esta práctica, salvo en ciertas excepciones.

¿Cómo opera el *spoofing*?

La función de identificación de llamadas –mediante la exhibición del nombre y número de quien llama en las pantallas de los equipos telefónicos -- se usa para evitar llamadas no solicitadas. Pero en algunos casos, esta función es manipulada por personas malintencionadas que posan como representantes de bancos, acreedores, compañías de seguros e incluso el gobierno.

Lo que usted puede hacer si piensa que alguien intenta usar *spoofing* en su teléfono

Es posible que usted no note inmediatamente un intento de *spoofing*. Sea cauteloso cuando le pidan dar información que le identifique personalmente.

- Ante cualquier sospecha o llamada inesperada, nunca dé información personal, como números de cuenta, de Seguro Social, el apellido de soltera de su madre, claves de ingreso o cualquier otra información de identificación personal.
- Si recibe consultas sobre su información personal por parte de alguien señalando que representa a una compañía o a una agencia del gobierno, interrumpa la llamada. Luego llame al número telefónico indicado en su recibo de cuentas, en la guía telefónica o en el sitio web de la compañía o agencia gubernamental mencionadas, para verificar la autenticidad de la solicitud.
- Sea precavido si le presionan para que entregue información inmediatamente.
- Si usted mantiene un correo de voz en su servicio telefónico, asegúrese de resguardarlo mediante una clave de ingreso. Algunos servicios de correos de voz se pueden programar para dar a conocer sus mensajes de voz cuando los revisa desde otro teléfono. Un pirata cibernético podría intentar suplantar su identidad usando su número telefónico para obtener acceso a su correo de voz, si usted no lo resguarda con una clave de ingreso.

¿Practicar *spoofing* es ilegal?

De conformidad con la ley de veracidad en las llamadas (*Truth in Caller ID Act*, en inglés), las normas de la FCC prohíben a cualquier persona o entidad la transmisión de información de identificación engañosa o inexacta, usada *con la intención de estafar, causar daño u obtener valores de manera inadecuada*. Si no existe la intención de causar daños, la práctica del *spoofing* no es ilegal. Quienes resulten culpables de *spoofing* ilegal pueden enfrentar multas de hasta \$10,000 (diez mil dólares) por cada transgresión. En algunos casos, el *spoofing* es permitido por tribunales, cuando es usado por

personas que tienen razones legítimas para ocultar su información. Por ejemplo, miembros de las agencias de orden y seguridad que necesitan usarlo en el contexto de sus labores, o en el caso de víctimas de abuso doméstico o de médicos que desean hablar sobre temas de salud privados.

¿Bloquear números telefónicos equivale a practicar *spoofing*?

Bloquear números telefónicos no equivale a practicar *spoofing*. Las normas de la FCC exigen a las compañías telefónicas ofrecer la función de bloqueo de números telefónicos gratuitamente en todas las llamadas entre los estados del país (cada estado dispone sus propias normas para las llamadas locales). Si usted recibe una llamada telefónica de “número desconocido”, significa que se ha bloqueado el número, pero no necesariamente se trata de una llamada *spoofing*. Asimismo, usted puede bloquear la transmisión de su número telefónico cuando efectúa llamadas. En este caso, su número aparecerá como “desconocido” en la pantalla del receptor.

¿Cuáles son las normas de la FCC para los vendedores telefónicos respecto al identificador de llamadas?

Las normas de la FCC exigen específicamente a los vendedores telefónicos:

- Transmitir o exhibir su número telefónico o el de la entidad que representan. Si es posible, deben agregar el nombre de la compañía cuyos productos o servicios están comercializando.
- Exhibir un número telefónico al que usted puede llamar en horas de oficina para pedir que no le llamen más. Esta norma rige incluso para empresas que ya tienen una relación de negocios establecida con usted.

¿Cómo puedo efectuar una denuncia si sospecho *spoofing*?

Si usted recibe una llamada y sospecha que la información en el identificador de llamadas ha sido falsificada o piensa que las normas de protección de privacidad de su número telefónico han sido transgredidas, usted puede presentar una queja ante la FCC. Tiene múltiples opciones para presentar quejas ante la FCC:

- Presente una queja en línea en <https://consumercomplaints.fcc.gov> (en inglés).
- Por teléfono: 1-888-CALL-FCC (1-888-225-5322); TTY: 1-888-TELL-FCC (1-888-835-5322). ASL: 1-844-432-2275.
- Por correo postal (por favor, incluya su nombre, dirección, información de contacto y tantos detalles como pueda sobre su queja):

Federal Communications Commission
Consumer and Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
445 12th Street, S.W.
Washington, DC 20554

Formatos accesibles

Para solicitar este artículo en formato accesible - Braille, letra grande, documento en Word, de texto o de audio – escribanos o llámenos a la dirección o números telefónicos de más arriba o envíe un correo electrónico a fcc504@fcc.gov.

Última edición: 12 de septiembre de 2016

