



Suplantación de Identidad

Los estafadores telefónicos a menudo ocultan su identidad al utilizar técnicas ilegales de suplantación de identidad para enviar información falsa a la pantalla de su identificador de llamadas. Para engañarlo y que usted responda la llamada, los estafadores pueden utilizar números y códigos de área locales que le resulten familiares. O bien, pueden hacerse pasar por una empresa con la que usted hace negocios, una empresa de servicios públicos o un organismo gubernamental.

A continuación, se presentan algunas buenas maneras para evitar ser engañado.

- No responda las llamadas provenientes de números desconocidos.
- Si responde y no es quien esperaba, no espere, cuelgue.
- Si la persona que llama le pide que pulse un botón para dejar de recibir llamadas, simplemente cuelgue.
- Nunca asuma que el identificador de llamadas de una llamada inesperada es legítimo. Cuelgue y vuelva a llamar a un número que pueda verificar en una factura, un estado de cuenta o un sitio web oficial.
- Sea desconfiado. Los timadores pueden ser muy convincentes: Pueden hacer preguntas inofensivas, sonar amenazantes, o a veces parecer demasiado buenos para ser verdad.
- No dé números de cuenta de información personal, números de Seguro Social ni contraseñas, ni responda preguntas de seguridad.
- Tenga mucho cuidado si está siendo presionado para efectuar un pago inmediato.
- Consulte a su compañía telefónica por herramientas de bloqueo de llamadas para teléfonos fijos o aplicaciones para dispositivos móviles.
- Denuncie las estafas de suplantación de identidad ante la policía, la Comisión Federal de Comunicaciones (FCC) y la Comisión Federal de Comercio (FTC).



Avoid Spoofing Scams

Phone scammers often disguise their identity by using illegal spoofing techniques to send false information to your caller ID display. To trick you into answering, spoofers may use local area codes and numbers that look familiar. Or they may impersonate a company you do business with, such as a local utility, or even a government agency.

Here are some good ways to avoid being spoofed:

- Don't answer calls from unknown numbers.
- If you answer and it's not who you expected, don't hang on, hang up.
- If a caller asks you to hit a button to stop getting calls, just hang up.
- Never assume an unexpected call is legitimate. Hang up and call back using a number you can verify on a bill, a statement, or an official website.
- Be suspicious. Con artists can be very convincing: They may ask innocuous questions, or sound threatening, or sometimes seem too good to be true.
- Don't give out personal information – account numbers, Social Security numbers or passwords – or answer security questions.
- Use extreme caution if you are being pressured for immediate payment.
- Ask your phone company about call blocking tools for landlines or apps for mobile devices.
- Report spoofing scams to law enforcement, the FCC and the FTC.

