Instituto Mexicano de
Contadores Públicos

Boletín de la Comisión de Prevención de Lavado de Dinero y Anticorrupción

En congruencia con los objetivos estratégicos del IMCP, la Comisión de Prevención de Lavado de Dinero y Anticorrupción elabora este boletín informativo con el propósito de mantenerlos actualizados en materia de Prevención de Lavado de Dinero y Anticorrupción.

Noviembre de 2025
Número 160

Informe de Europol sobre suplantación de identidad telefónica

Número falso, daño real: Europol insta a tomar medidas contra la suplantación de identidad de llamadas

C.P. y PCLD Genaro Eliseo Gómez Muñoz
Integrante de la Comisión de Prevención de Lavado de Dinero y Anticorrupción del IMCP

La gravedad de la amenaza

Europol ha emitido un contundente llamamiento a la acción, instando a una respuesta europea coordinada y robusta para combatir la suplantación de identidad telefónica, conocida en inglés como *call spoofing*.

Esta técnica delictiva, que consiste en falsificar la información del identificador de llamadas (como el número de teléfono) para que parezca provenir de una fuente legítima y de confianza, se ha consolidado como una herramienta principal para el *fraude en línea y las estafas de ingeniería social.*

La magnitud del problema es alarmante

Esta práctica está generando un daño económico y social considerable. A escala mundial, las pérdidas financieras atribuidas directamente a la suplantación de identidad en llamadas se estiman en *850 millones de euros anuales.*

El método y el impacto en las víctimas

Las tácticas de los delincuentes son directas y efectivas. Las llamadas telefónicas y los mensajes de texto (SMS) siguen siendo el centro de ataque predominante, representando casi 64% de todos los casos de fraude denunciados.

Al ocultar eficazmente su verdadera identidad y ubicación geográfica, los estafadores logran sus objetivos de varias maneras:

- Engañan a las víctimas para que revelen información personal sensible (datos bancarios, contraseñas, números de identificación).
- Inducen a las víctimas a transferir fondos directamente a cuentas controladas por los criminales.
- Obtienen acceso remoto a los dispositivos (teléfonos, computadoras) y cuentas personales de las víctimas.

Este error de la identidad complica de manera extraordinaria la labor de las fuerzas del orden, dificultando enormemente el rastreo de los perpetradores y su posterior enjuiciamiento.

Una amenaza transfronteriza y organizada

La suplantación de identidad en llamadas no es un delito menor o aislado; es una amenaza sin fronteras utilizada de forma creciente por redes de delincuencia organizada que operan en múltiples jurisdicciones.

Los estafadores adoptan diversas identidades falsas para ganarse la confianza de la víctima, haciéndose pasar por bancos, agencias gubernamentales (como la policía o hacienda) o incluso por familiares en apuros.

En una vertiente aún más peligrosa, la técnica se utiliza para realizar llamadas falsas de emergencia desde el domicilio de una víctima (*swatting*), provocando una respuesta masiva e innecesaria de los servicios de emergencia.

Las investigaciones de Europol revelan la preocupante emergencia de un modelo de negocio conocido como "suplantación de identidad como servicio" (*Spoofing-as-a-Service*). Este modelo proporciona a delincuentes de menor nivel herramientas listas para usar que les permiten imitar a entidades de confianza, como instituciones financieras o fuerzas del orden. Estas redes a menudo operan desde

el extranjero, aprovechando lagunas jurisdiccionales para evadir la detección y la acción judicial.

El desequilibrio insostenible y el llamamiento de Europol

Europol destaca un desequilibrio actual que considera insostenible: la suplantación de identidad es extremadamente fácil de cometer desde un punto de vista técnico, pero desproporcionadamente difícil de investigar.

La agencia insta a adoptar medidas concretas que inviertan esta situación. El objetivo debe ser encarecer y complicar técnicamente el proceso para que los delincuentes se oculten tras identidades falsificadas. Simultáneamente, se debe capacitar a los investigadores para que puedan actuar con rapidez y eficacia a nivel transfronterizo.

Un estudio reciente de Europol, realizado en 23 países, arrojó resultados preocupantes: se identificaron dificultades significativas para implementar medidas efectivas contra la suplantación telefónica. Esto significa que una población total de aproximadamente 400 millones de personas en estas regiones sigue siendo vulnerable a este tipo de ataques.

Las fuerzas del orden de los países consultados destacaron tres obstáculos principales:

- La escasa cooperación por parte de los operadores de telecomunicaciones.

- La fragmentación de las regulaciones entre los distintos países miembros.
- La falta de herramientas técnicas adecuadas para identificar y bloquear sistemáticamente las llamadas falsificadas.

Hacia una respuesta europea coordinada: las tres prioridades

Para rectificar estas deficiencias, Europol y sus socios han identificado tres prioridades estratégicas que requieren una acción inmediata y armonizada:

- *Normas técnicas armonizadas.* Es imperativo desarrollar e implementar mecanismos comunes a escala de la UE. Estos mecanismos deben permitir rastrear eficazmente las llamadas fraudulentas, verificar la autenticidad de los identificadores de llamadas legítimos y bloquear activamente el tráfico engañoso antes de que llegue al usuario.
- *Mayor colaboración transfronteriza.* Se debe fortalecer la cooperación operativa entre las fuerzas del orden, los organismos reguladores nacionales y la industria de las telecomunicaciones. El objetivo es compartir información y pruebas de manera rápida y eficiente, superando las barreras burocráticas actuales.
- *Convergencia regulatoria.* Las normas nacionales deben armonizarse. Esto incluye crear marcos legales que permitan el rastreo legal de llamadas en investigaciones, aclarar los usos

legítimos (si los hubiera) del enmascaramiento del identificador de llamadas y promover la adopción de herramientas antifraude de eficacia probada en todo el bloque.

Conclusión y amenazas futuras

Si bien estas medidas son esenciales, Europol advierte que los delincuentes inevitablemente se adaptarán.

La vigilancia debe ser constante, ya que emergen nuevas amenazas, como las estafas de duplicación de tarjetas SIM (SIM *swapping*), el uso de servicios prepago-anónimos y el *smishing* (*phishing* por medio de SMS).

Las medidas propuestas por Europol respaldan la estrategia general ProtectE, reforzando la capacidad colectiva de Europa para combatir la delincuencia organizada y proteger a sus ciudadanos.

Europol concluye que solo mediante una colaboración sostenida entre múltiples actores (públicos y privados) podrá Europa restablecer la integridad de sus redes de comunicación y reducir el creciente daño causado por esta forma de fraude.

México

El *Spoofing* telefónico en México

Sin embargo, el problema de la suplantación de identidad telefónica (conocido comúnmente como *spoofing* o *vishing*) es una amenaza real y muy frecuente en México.

Aunque el informe de Europol no lo cubre, el *modus operandi* es prácticamente idéntico.

¿Cómo opera el *spoofing* en México?

- *Suplantación bancaria (muy común).* Los delincuentes falsifican el número de teléfono oficial de un banco (como Banamex, BBVA, Santander, etcétera). Te llaman indicando un supuesto "cargo no reconocido" o un "intento de acceso a tu cuenta" para generar urgencia y robar tus contraseñas, NIP o datos de tu tarjeta.
- *Suplantación de gobierno.* Fingen ser de instituciones como el Servicio de Administración Tributaria (SAT), la Comisión Federal de Electricidad (CFE) o la Lotería Nacional, usualmente para decirte que tienes un adeudo que debes pagar de inmediato o que ganaste un premio y necesitas dar tus datos bancarios.
- *Extorsión y secuestro virtual.* Utilizan números locales o desconocidos (que pueden estar enmascarados) para afirmar que tienen a un familiar secuestrado o para exigirte "derecho de piso".

Autoridades relevantes en México

En México, la principal entidad que emite alertas sobre este tipo de fraudes financieros es la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).

La CONDUSEF ha advertido repetidamente sobre el *spoofing* telefónico y el *vishing*, subrayando que los bancos *nunca* solicitan datos sensibles (como contraseñas, NIP o códigos de seguridad CVV) por teléfono.

Recomendaciones clave (similares a las de Europol)

- *Colgar de inmediato.* Si recibes una llamada sospechosa, incluso si el número parece legítimo, cuelga.
- *Verificar por tu cuenta.* Busca el número oficial del banco o institución (en tu tarjeta o en su sitio web oficial) y llama tú mismo para verificar si la situación que te reportaron que era real.
- *No entregar datos.* Nunca proporciones contraseñas, NIP, números de tarjeta o códigos de seguridad por teléfono.

Link

https://www.europol.europa.eu/media-press/newsroom/news/fake-number-real-damage-europol-urges-action-against-caller-id-spoofing