MINISTERIO
PARA LA
TRANSFORMACIÓN
DIGITAL Y DE LA
FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES.

SECRETARÍA GENERAL DE TELECOMUNICACIONES Y ORDENACIÓN DE LOS SERVICIOS DE LA COMUNICACÓN AUDIOVISUAL

SUBDIRECCIÓN GENERAL DE ORDENACIÓN DE LAS TELECOMUNICACIONES

CONSULTA PÚBLICA SOBRE INICIATIVAS NORMATIVAS Y MECANISMOS TÉCNICOS Y OPERATIVOS PARA COMBATIR LAS ESTAFAS DE SUPLANTACIÓN DE IDENTIDAD A TRAVES DE LLAMADAS TELEFÓNICAS Y MENSAJES DE TEXTO FRAUDULENTOS

En los últimos años estamos asistiendo a un incremento exponencial de la cibercriminalidad en la que destacan, en particular, las estafas de suplantación de identidad que suelen comenzar con una llamada o un mensaje de texto en los que el emisor de la comunicación suplanta la identidad de una organización de confianza (entidad bancaria, administración pública, empresa de transporte, etc.) con la clara intención de defraudar, engañando al consumidor para que proporcione información personal y financiera confidencial, facilite sus claves personales o realice alguna acción (acceso a una web, llamar a un número telefónico, ordenar una trasferencia, contratar un servicio, entre otros).

Algunos de los métodos más comunes para llevar a cabo estas estafas son:

- Llamada del personal en nombre de una entidad financiera suplantando su representación, en la que se comunica al consumidor que ha habido movimientos sospechosos de ser fraude en su cuenta bancaria, dándole la oportunidad de transferir su dinero a una “cuenta segura”;

- Llamada o mensaje de texto suplantando a una administración pública, una empresa de servicios públicos o una empresa de transporte, solicitando al consumidor que realice un pago (de una multa de tráfico, de unas tasas de aduana o un impuesto o una factura vencidos), acceda a una notificación o llame a un número de teléfono para concertar una cita o una entrega;

- Llamada suplantando a una empresa de tecnología de la que el consumidor es cliente que solicita acceso al ordenador del consumidor para "solucionar" un problema;

- Llamada suplantando a una empresa de suministros de la que el consumidor es cliente para “informarle” de un cambio en sus condiciones de contratación; para en una segunda llamada – esta vez en nombre de otra empresa de suministros, ofrecerle un cambio de suministrador.

Para engañar a sus víctimas, las estafas de suplantación de identidad suelen incluir una serie de características comunes:

- Apariencia de legitimidad: cuando la estafa se inicia a través de una comunicación electrónica, una forma de ayudar a crear la apariencia de legitimidad, incrementando la posibilidad de que la llamada o el mensaje de texto sea atendido por el consumidor, es suplantar un número de teléfono válido o un alfanumérico de una organización de confianza como emisor de la comunicación.

- Explotación de rasgos personales: en múltiples ocasiones los estafadores cuentan con información sobre el consumidor al que contactan que han obtenido previamente.

- Urgencia: los estafadores habitualmente enfatizan la necesidad de tomar medidas urgentes u ofrecen algo por tiempo limitado.

La confianza de consumidores en la fiabilidad y seguridad del contenido transmitido a través de las comunicaciones electrónicas, el amplio uso que hacen las empresas y organismos de las comunicaciones electrónicas como medio de contactar con sus usuarios, así como la capacidad de estas comunicaciones para llegar a un gran número de personas a un coste relativamente bajo, hacen que el uso de llamadas y mensajes de texto sea un instrumento frecuentemente utilizado en la comisión de este tipo de estafas.

Estas estafas causan importantes daños financieros y económicos a todos los sectores de la sociedad, incluidos los consumidores, las empresas y los organismos públicos. Además, hacen mella en la confianza de los consumidores que, a raíz de la generalización de estas prácticas, desconfían de contestar llamadas y leer mensajes de texto, perjudicando a aquellas empresas y organismos que hacen uso de llamadas y mensajes de texto, legítimamente, como canal de comunicación para facilitar información u ofrecer sus servicios a los consumidores.

Con el objetivo de prevenir y luchar contra estas estafas y restaurar la confianza de los consumidores, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales ha identificado y analizado una serie de medidas, técnicas y regulatorias, que se someten a Consulta Pública.

Hay que señalar que las estafas son de naturaleza dinámica, pueden ser muy sofisticadas, a menudo, implican varios pasos y utilizan de manera complementaria diversas vías de contacto con las víctimas, por lo que la erradicación de estas prácticas requiere la colaboración, tanto a nivel nacional como internacional, de las empresas participantes en todos los sectores

económicos afectados y la intervención de diferentes organismos públicos en el marco de sus respectivas competencias.

El propósito de esta Consulta Pública es determinar, con las aportaciones que se reciban a la misma, qué paquete de mecanismos técnicos y operativos y de medidas regulatorias, dentro de las competencias de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, es adecuado para prevenir y luchar contra estas estafas y prácticas fraudulentas que se canalizan a través de llamadas y mensajes de texto, y puede acompañar otras medidas que empresas, operadores y otros organismos puedan adoptar.

En relación con las medidas de naturaleza normativa que pudiera resultar adecuado adoptar, el trámite de la presente Consulta Pública viene a dar cumplimiento a lo dispuesto en el artículo 133.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

1. Posibles medidas en el ámbito de la numeración identificativa del origen de las llamadas

En numerosas ocasiones las estafas canalizadas a través de llamadas utilizan la manipulación del CLI[1] identificador de la llamada, para que el número coincida con el número publicitado (o conocido por los usuarios) de una entidad financiera, empresa prestadora de otros servicios o de un organismo público, cuya trazabilidad se dificulta por la participación de estafadores que están localizados fuera del territorio nacional.

La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales desea recabar la opinión de todos los posibles afectados sobre la oportunidad, viabilidad, impacto y requisitos o salvaguardas a considerar en relación con las siguientes medidas, alternativas o p.complementarias entre sí: **(i)** medidas tendentes a restringir el uso de parte de la numeración del plan nacional en llamadas con originación internacional; **(ii)** medidas tendentes a regular un rango de numeración específico para la realización de llamadas de naturaleza comercial prospectiva; **(iii)** establecimiento de “listas DNO” de numeración apta únicamente para la recepción de llamadas;o **(iv)** establecimiento de listas de numeraciones sin uso.

1a)	¿Qué consideración le merece la posible medida regulatoria que obligara a los operadores de comunicaciones vocales disponibles al público a bloquear las llamadas con origen internacional identificadas por un CLI del plan nacional de numeración?

[1] Siglas correspondientes al término anglosajón *Calling Line Identification*. El CLI identifica el número telefónico de la parte que origina la llamada o comunicación.

¿Considera necesario o conveniente excluir de esta medida algún tipo de numeración nacional (p.ej. centros de atención de llamadas ubicados fuera del territorio nacional)? En caso afirmativo, identifique la numeración a excluir y explique las razones.

¿Considera necesario que la medida incluyese otros escenarios, por ejemplo, que el identificador de la llamada con origen internacional estuviese vacío o fuese no válido?

Con la excepción de la numeración móvil que se aborda en la siguiente pregunta,

- ¿existe alguna razón que aconseje una adaptación gradual de esta medida?
- ¿existe alguna razón que desaconseje o impida que los operadores nacionales verifiquen que no se generan fuera de su red llamadas con una numeración que les ha sido asignada y bloqueen las llamadas que no superen esta verificación?

1b) ¿Qué medidas considera necesario adoptar, a nivel de cooperación entre operadores móviles, para identificar el tráfico generado por usuarios en roaming internacional, evitando que las llamadas, legítima y lícitamente originadas por estos usuarios, se vieran perjudicadas por la medida del punto 1a)?

¿existe alguna razón que desaconseje o impida que los operadores móviles nacionales verifiquen, cuando reciban una llamada de origen internacional identificada con una numeración móvil que les ha sido asignada, si el cliente al que corresponde esa numeración está en roaming y, cuando no sea así, bloqueen las llamadas?

1c) ¿Qué opinión le merece la posible asignación de un rango de numeración específico para la realización e identificación de llamadas comerciales prospectivas y la consecuente prohibición de la utilización para este tipo de llamadas del resto de numeración del plan nacional?

¿En particular, considera adecuado evitar que el rango de numeración móvil sea empleado para identificar los terminales fijos de los centros de atención de llamadas por parte de las empresas de servicios de telemarketing y atención a clientes?

1d) ¿Facilitaría la persecución de algunas de estas estafas, que las plataformas de televenta vinieran obligadas a utilizar numeración asignada a la empresa

en cuyo nombre contactan a los consumidores, previa autorización de esta empresa?

¿Considera que hay otras alternativas que, por ejemplo, puedan facilitar y mejorar el control de la subasignación de numeración y/o la aparición de empresas/operadores que ofrecen plataformas con el objetivo de manipular el CLI?

1e) ¿Qué opina del establecimiento de una lista DNO (Do Not Originate) que prohibiera el uso de las numeraciones en la lista DNO como identificador de llamadas? Por ejemplo, ciertos bancos proporcionan números para que los consumidores se comuniquen con ellos, pero nunca se comunican con un consumidor utilizando el mismo número. En consecuencia, cualquier llamada que utilizara estos números como CLI identificador de la llamada sería irregular (puesto que el CLI habría sido modificado) y con alta probabilidad, fraudulenta.

Las llamadas que, a pesar de la prohibición, se generaran desde estas numeraciones podrían ser bloqueadas o anonimizadas (como “número desconocido”). ¿Qué ventajas o desventajas ve a estas alternativas?

1f) ¿Considera que esta lista DNO debería estar a disposición de cualquier entidad o debería limitarse a la numeración asignada a entidades públicas y entidades financieras en razón de su especial sensibilidad y/o riesgo de ser utilizados para fraudes de mayor impacto económico?

1g) ¿Qué opina del establecimiento de una lista de “numeraciones sin uso” que prohibiera el uso de las numeraciones en dicha lista como identificador de llamadas? Se trataría de rangos de numeración o numeraciones que no hubiesen sido asignados y, en consecuencia, cualquier llamada que utilizara estos números como CLI identificador de la llamada sería irregular (puesto que el CLI habría sido modificado) y con alta probabilidad, fraudulenta.

Las llamadas que, a pesar de la prohibición, se generaran desde estas numeraciones podrían ser bloqueadas o anonimizadas (como “número desconocido”). ¿Qué ventajas o desventajas ve a estas alternativas?

2. Posibles medidas en el ámbito de la numeración y códigos alfanuméricos identificativos de mensajes (SMS[2], MMS[3] o RCS[4])

De manera similar a lo que ocurre con las llamadas, en los servicios de mensajería también asistimos a prácticas de manipulación del CLI con características similares a las llamadas, cuando el identificador del mensaje es un número del plan nacional de numeración.

2a) ¿Qué consideración le merece la posible medida regulatoria que obligara a los operadores de mensajería y de reenvío y almacenamiento de comunicaciones interpersonales basados en numeración a bloquear los mensajes con origen internacional identificados por un CLI del plan nacional de numeración?

Especifique si la extensión de la medida propuesta en el punto 1a) a los mensajes con origen internacional planteara cuestiones técnicas, comerciales o de otra índole diferentes de las que haya señalado en su respuesta a los diferentes apartados del punto 1a).

2b) ¿Qué medidas considera necesario adoptar, a nivel de cooperación entre operadores móviles, para identificar el tráfico generado por usuarios en roaming internacional, evitando que los mensajes de texto, legítima y lícitamente enviados por estos usuarios, se vieran perjudicados por la medida del punto 2a)?

Especifique si la extensión de la medida propuesta en el punto 1b) a los mensajes con origen internacional planteara cuestiones técnicas, comerciales o de otra índole diferentes de las que haya señalado en su respuesta a los diferentes apartados del punto 1b).

Adicionalmente, el origen de los mensajes también puede ser identificado a través de códigos alfanuméricos que también son objeto de suplantación.

2d) ¿Qué beneficios asocia a la creación de una base de datos nacional única con lista exhaustiva de nombres y abreviaturas alfanuméricas a utilizar para identificar a las entidades emisoras de los mensajes?

2e) ¿Considera que esta base de datos debería cubrir los nombres y alfanuméricos utilizados por cualquier entidad o debería limitarse a los

[2] Siglas correspondientes al término anglosajón *Short Messaging Service.*
[3] Siglas correspondientes al término anglosajón *Multimedia Messaging Service.*
[4] Siglas correspondientes al término anglosajón *Rich Communication Service.*

nombres y alfanuméricos de entidades públicas y entidades financieras en razón de su especial sensibilidad y/o riesgo de ser utilizados para fraudes de mayor impacto económico?

2f) ¿Cuál sería el mecanismo adecuado para controlar y verificar el origen de los mensajes que utilizaran un alfanumérico registrado en la citada base de datos nacional como identificador de origen? ¿Sería necesario algún mecanismo de certificación cualificado para los emisores de estos mensajes?

2g) ¿Sería necesario acompañar esta medida de la prohibición de envío de mensajes haciendo uso de los nombres y alfanuméricos registrados en la base de datos sin la previa verificación del origen?

2h) ¿Considera que la llevanza del registro citado en el punto 2d) debe realizarse por un organismo público, un organismo privado o vía cooperación entre los diferentes agentes en la cadena de transmisión de los mensajes?

2i) ¿Qué consideración le merece la prohibición de los mensajes no numéricos con origen internacional?

3. Posibles medidas para evitar que progresen las comunicaciones con manipulación de CLI

Existen diferentes iniciativas, técnicas y operativas, a nivel internacional para impedir la manipulación del CLI[5] que, como se ha visto, es un mecanismo que se utiliza ampliamente para canalizar una mayoría de estas estafas. En general se trata de variantes del denominado STIR/SHAKEN que buscan incrementar la fiabilidad del CLI a través de una compartición de información entre el operador originante y receptor de la llamada, con la participación de una entidad verificadora. Algunos países como Estados Unidos o Canadá han adoptado medidas en esta dirección, aunque aún no existe un estándar internacional.

3a) ¿Conoce de la existencia de alguna solución técnica suficientemente madura para ser adoptada regulatoriamente a nivel nacional? En caso afirmativo, aporte información detallada.

[5] Aunque tanto en España como en la práctica totalidad de los países de nuestro entorno la normativa de telecomunicaciones prohíbe la manipulación de CLI, existe una dificultad práctica, de índole técnico, para identificar cuando una comunicación ha sido objeto de una manipulación del CLI identificador de la misma.

3b)	¿Existiría, en su opinión, la necesidad de crear un grupo de trabajo nacional específico para el desarrollo de esta solución y la necesaria coordinación internacional?

4. Posibles medidas de detección, a través de equipamiento y/o software en la operativa de red, de este tipo de estafas y consecuente bloqueo de comunicaciones electrónicas afectadas.

Como se ha mencionado al inicio de la Consulta Pública este tipo de estafas presentan una serie de características comunes: una de ellas es el carácter masivo de las campañas "defraudadoras" y la repetición de patrones en las diferentes campañas.

Este carácter masivo significa, en la práctica, que una vez reportada una comunicación de contenido fraudulento (o identificada a través de patrones de tráfico y características del contenido de la comunicación), se puede actuar proactiva, rápida y muy eficazmente para frustrar estas campañas fraudulentas evitando que lleguen a otros consumidores las comunicaciones a través de las que se obtienen sus datos personales o se les incita a la acción con la que culmina la estafa.

Actualmente existen mecanismos técnicos que permiten detectar cuando una comunicación está siendo utilizada para llevar a cabo estas estafas, así como bloquear comunicaciones con el mismo contenido. En particular, cuando la vía de comunicación elegida por el estafador es el SMS, dando lugar a las practicas conocidas como "*smishing*", existen técnicas de Inteligencia Artificial de tratamiento de los SMS que, generando un "*hash*"[6], permiten identificar el envío de SMS masivos potencialmente fraudulentos para, con un eventual tratamiento posterior (visualización de mensaje o denuncia de consumidor afectado) determinar si son efectivamente fraudulentos y, consecuentemente, bloquear todos aquellos SMS con el mismo "*hash*" destinados a sus usuarios.

La aplicación de esta técnica permitiría tanto una actuación reactiva (una vez que hubiera denuncias) como proactiva y preventiva (por la vía de aplicación de algoritmos evolutivos de Inteligencia Artificial). Esto representa, en opinión de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, una

[6] Códigos alfanuméricos generados por diferentes algoritmos, con el fin de que sirvan de equivalente informático a una huella digital del SMS.

oportunidad para luchar contra estas prácticas, que merece especial atención y análisis, precisamente por la eficacia potencial que ofrece.

Así lo han reconocido **legisladores de otros Estados Miembros de la Unión Europea que han adoptado leyes que dan cobertura al acceso al contenido de los SMS por los operadores con la finalidad de evitar el fraude**:

- En **Bélgica**, la ley General de Telecomunicaciones[7], en su artículo 125.1.7º[8], introducido en diciembre de 2021, ha excepcionado el *smishing* del principio general del secreto de las comunicaciones.

  Sobre la base de esta excepción se han lanzado diferentes iniciativas entre las que destaca, a los efectos de esta Consulta Pública, la denominada *Stop phishing SMS*[9] que establece que el algoritmo a utilizar por los operadores en sus plataformas para la detección de mensajes fraudulentos debe incluir el análisis del contenido del SMS[10], de URL[11] y metadatos. Las plataformas desarrolladas bajo esta iniciativa están

[7] Loi relative aux communications électroniques.

[8] *Art. 125.§ 1 No es aplicable lo dispuesto en el artículo 124 de esta ley y en los artículos 259bis y 314bis del Código Penal: […]*
7° cuando los actos sean realizados por los ***operadores*** *con el* ***objetivo exclusivo de combatir el fraude cometido mediante mensajes utilizando números de teléfono****, como mensajes SMS o MMS, y en las siguientes condiciones:*
a) Que los actos se limiten al examen mecánico de mensajes para establecer fraude. La intervención humana está autorizada exclusivamente para verificar el correcto funcionamiento de los algoritmos informáticos;
b) que los operadores sean transparentes frente a los usuarios finales, de modo que quede claro que los mensajes pueden ser examinados mecánicamente como parte del proceso lucha contra el fraude;
c) que los datos en cuestión sólo puedan ser tratados por personas encargadas por el operador para luchar contra el fraude;
d) que el tratamiento de los datos en cuestión se limite a los actos y a la duración necesarios para combatir el fraude o hasta el final del período en el que es posible iniciar acciones judiciales;
Si el examen *mencionado en el apartado 1, 7°, a),* ***revela fraude, los operadores tomarán medidas concretas para combatir el fraude, tales como como bloquear mensajes*** *o sustituir en los mensajes URL que hacen referencia a un sitio Internet fraudulento por un mensaje de advertencia o una URL con un mensaje de advertencia.*

[9] https://www.bipt.be/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/65da55c1694562e84bef7f6eeb69757ac67ad9cf/appel_-candidature_stop_phishing_sms.pdf

[10] A través de palabras-clave, malware, presencia de URLs de redireccionamiento, etc.

[11] Especificando métodos de análisis de URL, nombres de dominio, links a paginas fraudulentas (incluidos en SMS). Como mínimo, se exige (i) análisis de fiabilidad basado en el nombre del dominio, su antigüedad y si aparece en listas antiphishing y (ii) comprobación de si se descarga algún malware al acceder a la URL.

operativas desde octubre de 2023 y, según fuentes púbicas, arrojan ya resultados muy prometedores[12].

- En **Polonia,** en agosto de 2023 se aprobó la Ley sobre la lucha contra el abuso en las comunicaciones electrónicas[13] excepciona del secreto de las comunicaciones el tratamiento que tenga el objetivo de detectar, prevenir y combatir los abusos en las comunicaciones electrónicas y autoriza a los operadores a analizar el contenido de los SMS para compararlos con los patrones de mensajes fraudulentos publicados por el CSIRT NASK[14] y consecuentemente bloquearlos.

  La citada ley también permite a los operadores bloquear mensajes SMS distintos de las plantillas desarrolladas por CSIRT NASK, utilizando un sistema que permita su identificación automática.

Otros reguladores, como Ofcom, reconocen la existencia de estas técnicas de filtrado, su uso por los operadores y los beneficios derivados para evitar prácticas de fraude[15].

Medidas como la técnica de *hash* que se indicaba al principio de este apartado u otros mecanismos de funcionamiento similar plantean ciertas dudas sobre su posible impacto y afectación de derechos fundamentales de los ciudadanos. Por este motivo, la Secretaría considera necesario abrir un debate de índole técnico y jurídico en relación con estas medidas y mecanismos técnicos para determinar su viabilidad, oportunidad y, en su caso, requisitos y salvaguardas que, desde las diferentes perspectivas su adopción e implementación pudiera requerir.

4a)	¿Considera que la adopción de medidas como la técnica de hash expuesta requiere de una modificación normativa para su implementación en España?

[12] Solo Proximus reportaba haber bloqueado en las dos primeras semanas de funcionamiento de su plataforma más de 3 millones de SMS (230.000 SMS/día)
https://www.proximus.com/fr/news/2023/20231024-proximus-stops-three-million-suspicious-text-messages.html

[13] Zwalczanie nadużyć w komunikacji elektronicznej. - Dz.U.2023.1703 - OpenLEX

[14] Computer Security Incident Response Team del National Research Institute

[15] Policy Positioning Statement de 23/02/2022 “Tackling scam calls and texts”: *4.3 For example, mobile network operators either have introduced or are in the process of introducing technology that can detect the key traits of scam texts sent over their networks, allowing them to block more suspicious messages. (“SMS filtering”).*
https://www.ofcom.org.uk/__data/assets/pdf_file/0018/232074/statement-tackling-scam-calls-and-texts.pdf

4b)	En caso afirmativo, ¿qué consideración le merece la posibilidad de excepcionar del secreto de las comunicaciones las situaciones de las estafas originadas por mensaje corto de texto, permitiendo a los operadores la aplicación de filtros y el bloqueo de los mensajes que, de acuerdo con la aplicación de determinados algoritmos, se identificaran como fraudulentos? ¿Considera necesaria la intervención pública en el diseño de los algoritmos a utilizar? Indique, en su caso, alternativas.
4c)	¿Considera necesario o conveniente adoptar algún tipo de salvaguardas para que la excepción no interfiera con la protección de la privacidad y datos personales (p.ej. acceso automatizado, generación de identificadores de mensajes para el análisis del tráfico que, una vez generados no permita adquirir conocimiento del contenido, etc.)? Especifique, en su caso, qué salvaguardas, identificando – cuando sea posible- su coste, impacto y viabilidad.

5. Posibles medidas de retirada y bloqueo de páginas web

Se someten a consulta algunas medidas que han sido adoptadas en otros Estados Miembros y que vienen a facilitar el bloqueo de páginas web que se utilizan también en estas estafas y cuya adopción en España podría requerir la colaboración de otros organismos.

5a)	Para los casos en los que al consumidor, vía SMS o e-mail, se le solicita el acceso a una página web que, al acceder, recaba sus datos y claves personales, ¿resultan eficaces, para combatir las estafas identificadas, los procedimientos y mecanismos actuales de retirada por propietarios y operadores de servicios de hosting; y de bloqueo de páginas web por prestadores de servicios de acceso a internet?
5b)	¿Qué utilidad atribuiría a un mecanismo de lista negra de URLs para advertir a los usuarios que no es un sitio seguro?
5c)	¿Acompañaría un mecanismo como el apuntado en el punto 5b) de una obligación a los prestadores de servicios de acceso a internet de bloquear esas páginas web?
5d)	¿Acompañaría un mecanismo como el apuntado en el punto 5b) de una obligación a los operadores de comunicaciones interpersonales basados en numeración de bloquear los mensajes que incluyan esas URLs?

6. Otras posibles medidas

Dado el carácter abierto de esta Consulta Pública se invita a los participantes a aportar otras propuestas que no hayan sido abordadas en este texto, especialmente, pero no exclusivamente, en aquellas que resulten competencia de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

6a)	¿Existe alguna medida adicional que considerara necesario abordar por parte de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales?