

# Lucha contra el fraude:

## Las principales estafas de 2022

**Senador Robert P. Casey, Jr. (D-PA)**  
*Presidente*

**Senador Mike Braun (R-IN)**  
*Miembro de Rango*

Noviembre 2023



**Comité Especial del Senado de los Estados Unidos para la Vejez**



# CONTENIDO

<b>Acerca del Comité Especial del Senado de los Estados Unidos para la Vejez</b>	<b>4</b>
<b>Cómo los estafadores están robando el dinero ajeno</b>	<b>8</b>
<b>Las 10 estafas principales de 2022</b>	<b>16</b>
1. Suplantación y fraude de servicios financieros	19
2. Estafas de atención médica y seguros de salud	24
3. Llamadas automáticas pregrabadas y no solicitadas	28
4. Estafas de soporte técnico e informáticas	32
5. Estafas "románticas"	35
6. Estafas de impostores del gobierno	38
7. Estafas de sorteos y lotería	41
8. Robo de identidad	44
9. Estafas de suplantación de identidad comercial y compras	47
10. Estafa a "personas necesitadas" y "abuelos"	50
<b>La línea directa en estos años</b>	<b>53</b>
<b>Número de quejas reportadas a la Línea directa contra el fraude por estado</b>	<b>57</b>
<b>Recursos</b>	<b>61</b>
<b>Notas Finales</b>	<b>76</b>

# **Acerca del Comité Especial del Senado de los Estados Unidos para la Vejez**





**El Comité Especial del Senado de los Estados Unidos para la Vejez, creado en 1961, es el punto focal en el Senado para el análisis y el debate sobre asuntos relacionados con los adultos mayores estadounidenses. El Comité Especial del Senado de los Estados Unidos para la Vejez opera una línea directa gratuita contra el fraude (1-855-303-9470), que sirve como recurso para que los estadounidenses mayores y sus familiares informen actividades sospechosas, y proporciona información sobre cómo denunciar fraudes y estafas a los funcionarios adecuados, incluida la policía.**

**ROBERT P. CASEY, JR., Pensilvania, PRESIDENTE**

KIRSTEN GILLIBRAND, Nueva York

RICHARD BLUMENTHAL, Connecticut

ELIZABETH WARREN, Massachusetts

MARK KELLY, Arizona

RAPHAEL WARNOCK, Georgia

JOHN FETTERMAN, Pensilvania

**MIKE BRAUN, Indiana, MIEMBRO DE RANGO**

TIM SCOTT, Carolina del Sur

MARCO RUBIO, Florida

RICK SCOTT, Florida

J.D. VANCE, Ohio

PETE RICKETTS, Nebraska

Encuentre más información sobre nuestros miembros y su trabajo en [www.aging.senate.gov](http://www.aging.senate.gov).

# MENSAJE DEL PRESIDENTE CASEY Y EL MIEMBRO DE RANGO BRAUN

Estimados amigos:

El Comité Especial del Senado de los Estados Unidos para la Vejez (Comité) se compromete a proteger a los estadounidenses mayores del fraude y crear conciencia para prevenir las estafas.

Este año, celebramos los 10 años de la Línea directa contra el fraude del Comité. Durante la última década, el personal del Comité que opera la Línea directa contra el fraude ha proporcionado a las personas que llaman recursos y orientación para ayudarlas a denunciar incidentes de fraude a los funcionarios adecuados, como las fuerzas del orden público y las agencias gubernamentales.

Casi 11,800 personas de todo el país se han puesto en contacto con la Línea directa contra el fraude desde su creación, incluidas casi 660 personas en 2022. Si usted o un ser querido necesita ayuda para conectarse con recursos, o desea denunciar actividades sospechosas que cree puedan ser fraudulentas, **comuníquese con la línea directa gratuita contra el fraude al 1-855-303-9470**. El personal del Comité está disponible para responder de lunes a viernes, de 9 a.m. a 5 p.m., Hora del este.

En 2022, los principales tipos de estafas reportados al Comité compartieron muchas similitudes con los reportados por la Comisión Federal de Comercio (FTC): las estafas de impostores; y de premios, sorteos y estafas de lotería se citan como algunas de las más reportadas.<sup>1</sup> Aunque muchos de los mismos tipos de estafas se

presentan año tras año, los métodos a través de los cuales los estafadores contactan a las víctimas se han diversificado: la inteligencia artificial (IA) y las redes sociales ahora juegan un papel prominente.

Recientemente, el Comité ha adoptado medidas para hacer frente a los nuevos riesgos de fraude. En mayo de 2023, el Comité envió una carta a la presidenta de la FTC, Lina Khan, solicitando información sobre el creciente predominio de la tecnología impulsada por IA en las estafas, y cómo la FTC está trabajando para enfrentar estos nuevos complots impulsados por IA. El Comité espera trabajar con la FTC y otras agencias relevantes para proteger a los estadounidenses mayores de los fraudes y estafas relacionados con la IA.

El Comité desea agradecer a las numerosas organizaciones de defensa del consumidor, centros comunitarios y funcionarios locales encargados de hacer cumplir la ley, que brindan una asistencia invaluable a los estadounidenses en estos temas. Esperamos que esta guía pueda ser utilizada como un recurso para ayudar a los adultos mayores a hacer frente a las estafas más frecuentes de que son víctimas los estadounidenses en la actualidad. Esperamos aprovechar nuestras iniciativas exitosas para detener las estafas dirigidas a los adultos mayores de nuestra nación.

Sinceramente,



Robert P. Casey, Jr.  
*Presidente*



Mike Braun  
*Miembro de rango*

# Cómo los estafadores están robando el dinero ajeno

Para robar el dinero ajeno, los estafadores confían en métodos de contacto que les permiten llegar a miles de personas de manera fácil y económica, así como en métodos de pago que les ayudan a tener acceso rápido al dinero mal habido sin dejar rastro.





# **ALERTA:** Uso de la Inteligencia Artificial en estafas

**La Inteligencia Artificial (IA) es una tecnología más reciente que permite a las computadoras imitar ciertos comportamientos similares a los humanos, como el habla o la escritura. Por ejemplo, los nuevos chatbots y herramientas de procesamiento del lenguaje pueden responder preguntas detalladas, escribir ensayos convincentes y desarrollar programación informática. Si bien esta tecnología se puede utilizar para hacer el bien, estas poderosas herramientas también pueden ser explotadas por malhechores para hacer que las estafas sean más sofisticadas y convincentes que nunca. En esta sección se describe la tecnología de IA, cómo se puede utilizar en fraudes y estafas, y qué señales de advertencia hay que tener en cuenta.**

## **¿Cómo se usa la IA?**

- **Chatbots:** Un chatbot es un programa informático que simula la conversación humana y suele ser utilizado por las empresas para responder a las consultas de los clientes. Algunas empresas utilizan la tecnología de IA en sus chatbots para permitir a los consumidores interactuar con dichos chatbots de una manera más natural y, como resultado, responder mejor a las consultas de los clientes. Conocidos a veces como "asistentes virtuales", estos procesadores sintéticos impulsados por IA pueden tener operadores verificados como Alexa de Amazon y Ask Julie de Amtrak. Sin embargo, existen chatbots operados por IA no verificados, que podrían usarse maliciosamente para obtener, almacenar y manipular sus datos personales.

- **Clonación de voz:** La clonación de voz utiliza la IA para crear modelos de voz que suenan casi exactamente como la voz real de alguien que quizás conozca. Los estafadores solo necesitan unos segundos de audio para crear estas voces clonadas. Pueden usar estas voces clonadas para hacerse pasar por autoridades o celebridades y pedir favores personales, dinero o consejos de inversión. También se pueden usar en “estafas de emergencia familiar,” que se explicarán más adelante en esta sección.
- **Deepfakes:** Un *deepfake* (o ultrafalso) es un video o imagen generada por IA que se hace para parecer auténtico. Los estafadores pueden utilizar imágenes o videos falsos para manipular a sus objetivos, utilizar tecnología de identificación facial y acceder a datos personales.

## LA IA ACELERA LA EFECTIVIDAD DE ESTAFAS PREEXISTENTES

**A continuación, las estafas con IA a las que debemos prestar atención:**



### **Ataques de phishing facilitados por IA:**

Los ataques de phishing, en los que los estafadores engañan a las personas para que revelen información confidencial, se han vuelto cada vez más sofisticados con el uso de la IA. Mediante el uso de algoritmos operados por IA, los estafadores pueden personalizar rápidamente los correos electrónicos de phishing, imitar diálogos sofisticados y eludir los filtros de correo basura (spam) tradicionales, lo que dificulta que las personas distingan entre comunicaciones genuinas y fraudulentas.



**Estafas de “emergencia familiar”:** En marzo de 2023, la FTC emitió una advertencia sobre el aumento del uso de la IA en complots de “emergencia familiar”, en los que los estafadores convencen a las víctimas de que su familiar está en apuros para obtener dinero en efectivo o información privada.<sup>2</sup> Los estafadores pueden utilizar la clonación de voz y los deepfakes para hacerse pasar por un ser querido que afirma estar en peligro y necesita dinero de inmediato. Este tipo de estafa puede ser extremadamente convincente y provocar miedo en la víctima.



**Estafas “románticas”:** Los estafadores emplean IA para crear y operar perfiles falsos en sitios web de citas y plataformas de redes sociales. Estos perfiles generados por IA pueden parecer genuinos, incorporando a menudo atractivas fotos deepfake y detalles personales convincentes. Luego, los chatbots impulsados por IA simulan una conversación realista para generar confianza, con el objetivo de engañar al objetivo para que envíe dinero.

## Consejos para protegerse:

- Los estafadores son expertos en el uso de un lenguaje inteligente para obligar a los objetivos a compartir información financiera, por lo que cualquier solicitud de transacción debe verificarse minuciosamente.
  - No proporcione información confidencial como su nombre, dirección de su domicilio, Número del Seguro Social o Identificación de Beneficiario de Medicare, ni información bancaria, a un contacto no verificado.
  - No transfiera ni envíe dinero a lugares desconocidos.

- Tenga cuidado con lo que descarga. Al igual que los estafadores, las aplicaciones pueden afirmar ser algo que no son, e intentar acceder a sus datos o instalar malware en su dispositivo.
- No crea todo lo que ve en Internet. Si un video, una llamada, una imagen o un mensaje le parecen inusuales o alarmantes, verifíquelo con una fuente de confianza o un familiar.
- Considere designar una “palabra segura” para uso de su familia que solo se comparta con familiares y contactos cercanos. Si recibe una llamada de un familiar que dice estar en peligro, puede pedirle la palabra de seguridad para garantizar que no se trata de un clon de voz generado por IA.
- No proporcione ninguna información personal o confidencial a un chatbot en línea. Cualquier información que proporcione al chatbot debe tratarse como si fuera información pública.

## MÉTODOS DE PAGO: CRIPTOMONEDAS, PAGOS DE RED ENTRE PARES (PEER-TO-PEER, P2P) Y TARJETAS DE REGALO

**Criptomonedas:** En 2022, la Oficina Federal de Investigaciones (FBI) descubrió que los adultos mayores de 60 años perdieron cerca de \$1.1 mil millones a consecuencia de estafas con criptomonedas, un incremento cercano al 350 por ciento en comparación con 2021.<sup>3</sup>

La criptomoneda es un tipo de moneda digital que por lo general existe solo electrónicamente. Es la preferida por los estafadores porque, al igual que las aplicaciones de pago P2P, obtienen el dinero al instante, y los pagos no suelen ser reversibles. También les da la posibilidad de usar un seudónimo. Los pagos con criptomonedas se pueden utilizar en una variedad de complots, desde estafas falsas de inversión hasta estafas "románticas".

### Consejos para protegerse:

- Ignore las solicitudes para dar sus claves privadas de criptomonedas. Esas claves controlan el acceso a sus criptomonedas y billeteras electrónicas, y nadie las necesita en una transacción legítima.
- Ignore las afirmaciones de retorno de la inversión (ROI) que parecen demasiado buenas para ser ciertas.
- No se comprometa con "gestores de inversiones" que se pongan en contacto con usted y le hagan promesas sobre un buen retorno de la inversión.
- Ninguna celebridad se pondrá en contacto con las personas directamente para vender criptomonedas. No responda a ningún mensaje que pretenda ser de una celebridad.
- No acepte criptomonedas "gratuitas" de desconocidos.
- Tenga en cuenta: Ningún negocio legítimo le exigirá que pague en criptomonedas. Esto siempre es una estafa.

- Para obtener más información sobre las criptomonedas y cómo protegerse de las estafas relacionadas con las criptomonedas, la FTC tiene información útil en <https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams>.

**Pagos por red entre pares (peer-to-peer, P2P):** En 2022, la FTC recibió más de 62,300 denuncias de consumidores que enviaron dinero a estafadores mediante aplicaciones de pago P2P como Cash App, Venmo, o Zelle, con pérdidas que totalizaron \$163.5 millones.<sup>4</sup> Con frecuencia, estos métodos de pago por P2P son usados indebidamente por los estafadores, debido a que obtienen el dinero de forma inmediata, independientemente del sitio en que estén, y a que muchas plataformas no permiten la cancelación de una transacción una vez enviado el dinero.

## **Consejos para protegerse:**

- No envíe dinero a un desconocido. Tómese su tiempo para asegurarse de que le está enviando dinero a la persona adecuada.
- Configure alertas de fraude en su aplicación P2P o con el banco o la tarjeta de crédito que vinculó a la aplicación. Las alertas de fraude pueden informarle si se ha cambiado la información personal o si se han realizado transacciones.
- Los pagos P2P tienen elementos de redes sociales como listas de "amigos." Evite dar información como su dirección, número de teléfono y otros datos personales, e ignore las solicitudes de amistad de personas a las que no conoce.
- Evite hacer transacciones con negocios que aceptan exclusivamente pagos por aplicaciones P2P o tarjetas de débito.
- Al igual que con cualquier otro sitio web financiero, proteja su cuenta con una contraseña segura. Utilice la autenticación de dos factores.

**Tarjetas de regalo:** Las tarjetas de regalo, junto con las tarjetas de crédito y las transferencias bancarias, fueron algunos de los principales métodos de pago utilizados por los estafadores para solicitar y sustraer dinero a los adultos mayores que denunciaron una estafa a la Línea directa contra el fraude. Cuando la víctima envía el número de tarjeta, el estafador utiliza inmediatamente el saldo, lo que dificulta la devolución del dinero.

## **Consejos para protegerse:**

- Si le pagó a un estafador con una tarjeta de regalo, informe de inmediato a la compañía que emitió la tarjeta.
- Si compra tarjetas de regalo para obsequiar o donar a familiares y amigos, hágalo en tiendas que conozca y en las que confíe. Revise las calcomanías protectoras en la tarjeta para asegurarse de que no han sido alteradas.
- Guarde siempre el recibo. Un recibo le ayudará a presentar una denuncia si se extravía la tarjeta de regalo.
- Desconfíe de señales evidentes de estafas como solicitudes para comprar tarjetas en varias tiendas, o para comprar un tipo específico de tarjeta.

# Las 10 estafas principales de 2022

En 2022, la Línea directa contra el fraude recibió 659 nuevas quejas de residentes de todo el país. Estas denuncias elevan el número total de quejas registradas en la Línea directa contra el fraude a casi 11,800 desde 2013.

La Gráfica 1 muestra las 10 principales estafas en 2022. Estas estafas representan casi la mitad de todas las denuncias presentadas a la Línea directa contra el fraude en 2022. Entre otras estafas menos comunes están las de supuestas reparaciones de viviendas, de servicios públicos y de tiempo compartido, entre otras.

Por primera vez desde que el Comité comenzó a operar la Línea directa contra el fraude, las estafas de impostores del gobierno no son el principal tipo de estafa reportada.

# GRÁFICA 1: LAS 10 ESTAFAS PRINCIPALES DE 2022



**Note:** Esta gráfica solo representa las 10 categorías principales de estafas y, por lo tanto, los porcentajes no suman el 100 por ciento. Al seleccionar las 10 categorías principales, se excluyeron las llamadas que no estaban relacionadas con un tipo específico de estafa o fraude (por ejemplo, solicitudes de referencias e información de la Línea directa contra el fraude). Los datos para otras categorías se pueden encontrar en línea en: <https://www.aging.senate.gov/download/2022-spanish-fraud-book-additional-data>.

El Comité reunió detalles adicionales sobre las experiencias de las víctimas adultas mayores. A partir de esta información descubrimos que, en 2022:

- El **30 por ciento** de las personas que llamaron denunciaron haber perdido dinero o propiedades;<sup>5</sup>
- El **18 por ciento** de las personas que llamaron denunciaron fraudes en representación de un adulto mayor.<sup>6</sup>

## Aurelia Costigan

### *Víctima de estafa de suplantación de identidad bancaria*

PITTSBURGH, PENNSILVANIA

"En septiembre pasado, recibí una llamada telefónica del número que aparece en el reverso de mi tarjeta de débito. El hombre dijo que era de Dollar Bank y que había dos cargos por actividades sospechosas en mi cuenta... Me dijo que podía ayudarme a evitar la cancelación de mi tarjeta y emitir una nueva... agregando una cuenta de Zelle que protegería mi cuenta bancaria..."

"Y luego añadió que, para saber que en realidad estaba hablando con Aurelia Costigan, necesitaba algún tipo de identificación... Me preguntó si tenía un número de banca en línea, pero no lo uso... Entonces, dijo que la única otra opción era usar mi número de Seguro Social. Pensé que eso era factible. Supuse que era de mi banco. Llamó desde el número correcto..."

"Y luego, entre 5 y 10 minutos después, mi teléfono comenzó a recibir llamadas sin parar, notificándome de un cargo tras otro... Veintidós, para ser exactos. Entré en pánico, fui al banco... y me di cuenta de que era una estafa."

"Me dijeron que notificara a la policía y presentara una denuncia ante la oficina del Fiscal Estatal... Pero me sentía absolutamente deprimida. No podía dormir. Tenía problemas para comer. Estaba devastada. El dinero que perdí, 1,800 dólares, fue mucho dinero... Pensé que nunca iba a recuperarlo".

"Pero afortunadamente... mi banco pudo recuperar mi dinero: los \$1,800. La Fiscalía Estatal me dijo que era muy afortunada..."

"Pero sé que no todo el mundo tiene esa experiencia. Estos estafadores se salen con la suya todos los días. Las personas mayores como yo, siempre somos confiadas. Pero ahora, le digo a todos: no le den absolutamente ninguna información a nadie por teléfono. Espero que podamos hacer algo para que esto no le ocurra a nadie más".

*Fragmentos del testimonio que la Sra. Costigan proporcionó al Comité para la Vejez en septiembre de 2022.*



# 1. Suplantación y fraude de servicios financieros

**En 2022, la estafa más común reportada a la Línea directa contra el fraude del Comité fue la suplantación y fraude de servicios financieros. Como testificó la Sra. Costigan en septiembre de 2022, los estafadores pueden hacerse pasar por empresas de servicios financieros como bancos, cobradores de deudas o administradores hipotecarios.**

**Por ejemplo, pueden hacerse pasar por cobradores de deudas y tratar de engañar a sus víctimas para que paguen deudas inexistentes. Pueden acosar o amenazar a sus víctimas con penas o penas de cárcel si se niegan a pagar. Las estafas de alivio hipotecario consisten en promesas relacionadas con el refinanciamiento y mentiras sobre los términos de un préstamo. Según la FTC, en 2022 se reportaron más de 116,000 casos de cobro de deudas fraudulentos<sup>7</sup> y más de 24,000 casos de fraude hipotecario.<sup>8</sup> Las advertencias falsas de fraude bancario fueron la estafa de mensajes de texto más reportada en 2022,<sup>9</sup> con un promedio de pérdidas reportado de \$3,000.<sup>10</sup>**

## SEÑALES DE ALERTA

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafa:

### Fraude de suplantación de identidad bancaria

- Usted recibe un mensaje de texto, una llamada telefónica o un correo electrónico que indica que la información de su cuenta se ha visto afectada. Es posible que le pidan información personal como nombres de usuario, contraseñas, PIN y números de Seguro Social para "proteger" su cuenta. También pueden pedirle que transfiera fondos utilizando una aplicación de pago P2P como Cash App, PayPal, Venmo o Zelle.
- Los bancos nunca se comunicarán con usted ni le pedirán que proporcione información personal confidencial por teléfono, mensaje de texto o correo electrónico. Nunca le pedirán que transfiera dinero a nadie, incluido usted mismo, ni le pedirán que proporcione información personal para obtener un reembolso o emitir una corrección.

### Fraude en el cobro de deudas

- La persona que le llama dice que irá a la cárcel si no paga la deuda que describe. Es ilegal que los cobradores de deudas amenacen con arrestar a alguien por no pagar sus deudas.
- La persona que llama no le dirá a quién le debe dinero. Los cobradores de deudas legítimos siempre le dirán quién es el acreedor, incluso si usted no se lo pregunta.
- Los cobradores de deudas legítimos brindan tiempo suficiente para pagar su deuda y trabajarán con usted para lograrlo. Los estafadores lo presionarán para que pague mientras lo tienen al teléfono.

## **Fraude de Alivio Hipotecario**

- La persona que llama y presenta la oportunidad de una hipoteca no ha sido referida a usted por amigos y familiares de confianza.
- Se le presiona para que firme documentos sin la oportunidad de consultar a un abogado.
- Hay secciones en blanco en los documentos que se le pide que firme. Estas secciones en blanco pueden ser completadas por el estafador después de que usted haya firmado.
- Se le presiona para que pague por adelantado antes de recibir cualquier servicio.

## **PASOS PARA PREVENIR Y RESPONDER**

### **Fraude de suplantación de identidad bancaria**

- No confíe en el identificador de llamadas. Los estafadores pueden "falsificar" su identificador de llamadas o la información transmitida a su identificador de llamadas para ocultar su identidad o permitirles hacerse pasar por una persona o empresa.
- No haga clic en enlaces ni responda a mensajes de texto inesperados.
- Si recibe una llamada, un mensaje de texto o un correo electrónico sospechoso, cuelgue y no responda al mensaje de texto o correo electrónico. Llame directamente a su banco o institución financiera utilizando información de contacto verificada, como el número de teléfono que aparece en el sitio web del banco o en el reverso de su tarjeta bancaria.

## **Fraude de cobro de deuda**

- Pida una carta de validación de deuda por escrito. Los cobradores de deudas están obligados por ley a enviarle información detallada sobre la deuda a pagar. Los estafadores se opondrán a esta solicitud.
- Pregúntele a la persona que lo llama el nombre del cobrador y el de la agencia de cobro de deudas para la que trabaja. Si dicen que trabajan con la policía o con un abogado, pida su número de placa, agencia o bufete de abogados. Los estafadores pueden objetar o tener problemas para responder a estas solicitudes.

## **Fraude hipotecario**

- Antes de firmar cualquier documento, consulte con un abogado para asegurarse de que se trata de una hipoteca legítima. Si la persona que intenta que firme agresivamente se opone a que consulte a un abogado, puede ser un estafador.
- Asegúrese de leer detenidamente todos los documentos antes de firmar. Si tiene preguntas, hágaselas a la persona que intenta que firme. Si ignora sus preocupaciones, puede ser un estafador.

**Denuncie todas las llamadas o mensajes sospechosos a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en <https://reportfraud.ftc.gov/>.**

## MÁS INFORMACIÓN

- La Asociación de Banqueros de los Estados Unidos (American Bankers Association) tiene más información sobre estafas de suplantación de identidad bancaria en <https://www.banksneveraskthat.com/>.
- La FTC proporciona más información acerca de estafas relacionadas con préstamos y cobros de deudas en <https://consumer.ftc.gov/credit-loans-debt>.
- La Oficina del Contralor de Moneda (Office of the Comptroller of the Currency, OCC) proporciona más información acerca de estafas en <https://www.occ.treas.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/index-fraud-resources.html>.



## 2. Estafas de atención médica y seguros de salud

Las decisiones sobre la atención médica y la cobertura de seguro pueden ser complejas. Los estafadores se aprovechan de esta complejidad haciéndose pasar por el programa Medicare, los planes comerciales de seguro médico y los proveedores de atención médica, o vendiendo “planes de salud con descuento” que no brindan una cobertura adecuada. También pueden solicitar información personal o financiera “a cambio de” beneficios. La Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) revela que las llamadas fraudulentas relacionadas con la salud dirigidas a adultos mayores tienden a aumentar durante el período de inscripción abierta de Medicare, que se extiende de octubre a diciembre.<sup>11</sup>

### DENUNCIAS A LA LÍNEA DIRECTA CONTRA EL FRAUDE

*Un residente de Massachusetts recibió una llamada de una persona que decía representar al “Centro para el Departamento de Verificación de Medicare”, que no existe. La persona que llamó le dijo que necesitaba una nueva tarjeta de Medicare. Sin embargo, cuando se le pidió su número de identificación de empleado varias veces, la persona colgó.*

## SEÑALES DE ALERTA

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafa:

- Una persona que llama haciéndose pasar por un empleado del gobierno le dice que se le cobrará una tarifa para obtener una tarjeta de Medicare.
- Se le solicita por llamada telefónica, correo electrónico o mensaje de texto información personal o financiera para "verificar" su seguro médico.
- Se le ofrece ayuda para navegar por el Mercado de Seguros Médicos, a cambio de una tarifa.
- Se le ofrece un plan médico de "descuento" con poca información y/o falta de reseñas legítimas en línea, y su médico no participa en el plan.
- Un vendedor le da respuestas vagas cuando usted le pregunta sobre detalles específicos relacionados con la cobertura de seguro que la persona está vendiendo.

## PASOS PARA PREVENIR Y RESPONDER

- Nunca proporcione información personal por teléfono.
- Revise detenidamente todas las facturas médicas para detectar cualquier servicio que no haya recibido. Comuníquese con su proveedor de seguros para hablar del tema.
- Visite fuentes confiables, como [Healthcare.gov](https://www.healthcare.gov) o [Medicare.gov](https://www.medicare.gov), para comparar planes, cobertura y precios.
- Exija ver una declaración de beneficios o una copia completa de la póliza de seguro que está considerando antes de tomar cualquier decisión.

- Investigue cualquier compañía que ofrezca cobertura de salud y, si el vendedor afirma que el plan se proporciona a través de una aseguradora importante, confirme directamente con dicha aseguradora.
- Los servicios que ofrecen ayuda legítima con el Mercado de Seguros Médicos (Health Insurance Marketplace) conocidos también como "navegadores" o "asistentes," no le cobrarán. Visite <https://www.healthcare.gov/find-assistance/> directamente para solicitar ayuda. Las personas elegibles para beneficios del Medicare pueden solicitar ayuda a sus Programas Estatales de Ayuda con los Seguros Médicos (State Health Insurance Assistance Programs, SHIPs) en <https://www.shiphelp.org/>.
- Denuncie todas las llamadas o mensajes sospechosos a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en <https://reportfraud.ftc.gov/>.

## MÁS INFORMACIÓN

- La FTC proporciona información y consejos adicionales en <https://consumer.ftc.gov/articles/spot-health-insurance-scams>.
- La FCC tiene más información sobre las estafas al Medicare en <https://fcc.gov/older-americans-and-medicare-scams>.
- Los Centros de Servicios de Medicare y Medicaid (Centers for Medicare & Medicaid Services, CMS) tiene recursos para denunciar estafas reales o intentos de estafa en <https://www.medicare.gov/basics/reporting-medicare-fraud-and-abuse>.
- El Departamento de Salud y Servicios Humanos de los EE.UU. (U.S. Department of Health and Human Services) mantiene un listado extenso de información para prevenir estafas en <https://oig.hhs.gov/fraud/consumer-alerts/>.



### 3. Llamadas automáticas pregrabadas y no solicitadas

Las llamadas automáticas pregrabadas y no solicitadas son las quejas principales que recibe la FCC,<sup>12</sup> y ocupan el tercer lugar en las más comunes reportadas a la Línea contra el fraude. Las llamadas automáticas se pueden realizar desde cualquier parte del mundo y, a menudo, contienen un mensaje creado por una voz pregrabada, robótica o generada por IA. Las personas que realizan llamadas automáticas pueden intentar vender un producto o servicio, y pueden “falsificar” (spoof) o imitar un número local o un número de una empresa con la que usted está familiarizado.

#### **DENUNCIAS A LA LÍNEA DIRECTA CONTRA EL FRAUDE**

*Una mujer residente en Maine recibió un mensaje de voz no solicitado de alguien que decía ser de su departamento de policía local. La persona que llamó dijo que su cuenta bancaria incurriría en cargos si no devolvía la llamada.*

## SEÑALES DE ALERTA

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafa:

- Usted contesta el teléfono y la persona que llama, o una grabación, le pide que presione un botón si no quiere recibir ese tipo de llamadas. A menudo, los estafadores usan este truco para identificar objetivos potenciales.
- Recibe una consulta de alguien que representa supuestamente a una empresa o agencia gubernamental. Cuando usted cuelga y llama al número de teléfono "verificado" por esa persona u organización, no hay registros de esa supuesta llamada.

## PASOS PARA PREVENIR Y RESPONDER

- Es posible que no pueda saber de inmediato si una llamada entrante es falsificada. Tenga en cuenta lo siguiente: el hecho de que el identificador de llamadas muestre un número "local" no significa necesariamente que la persona que le llama resida en su localidad.
- No responda llamadas de números desconocidos.
- No responda a ninguna pregunta, especialmente aquellas que se pueden responder con un "Sí".
- Nunca proporcione información personal como números de cuenta, números de Seguro Social, nombre de soltera de la madre, contraseñas u otra información de identificación como respuesta a llamadas inesperadas, o si tiene alguna sospecha.
- Si experimenta fraude o pérdida monetaria por una llamada automática, comuníquese lo antes posible con la FCC al 1-888-225-5322 y la FTC al 1-877-382-4357. También puede presentar una queja en línea en <https://reportfraud.ftc.gov/>.

## MÁS INFORMACIÓN

- La FCC ha publicado consejos para ayudar a los consumidores a evitar la suplantación de identidad en <https://www.fcc.gov/consumers/guides/spoofing-and-caller-id>.
- La FTC proporciona antecedentes útiles sobre las llamadas automáticas pregrabadas en <https://consumer.ftc.gov/articles/robocalls>.

## Polly Fehler

### *Víctima de estafa de "soporte técnico"*

SENECA, CAROLINA DEL SUR

"El 13 de abril, estaba usando mi nueva computadora portátil en una red Wi-Fi pública y de repente apareció una ventana emergente en la pantalla de inicio; un gran triángulo naranja parpadeante que alertaba de que mi computadora estaba afectada... Inmediatamente llamé al número que aparecía en la pantalla."

"Respondió una voz tranquilizadora que decía ser un representante de Microsoft. Me dijo que comprara un software de protección por 299 dólares..."

"Recibí otra llamada del mismo hombre que dijo que estaba llamando para ver cómo estaba el programa... Para realizar una prueba del software, tuve que darle acceso completo. Durante esta 'prueba,' la pantalla se llenó de mensajes. Y volvió a ocurrir: una alerta que afirmaba que mi computadora había sido comprometida..."

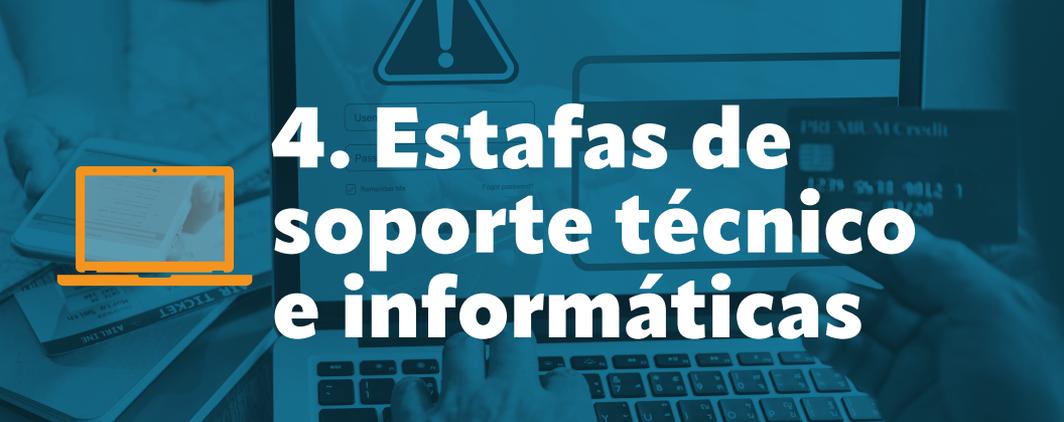
"Luego... abrió una ventana que mostraba mi cuenta corriente... Tenía un saldo de \$26.000; \$20.000 más de lo que debería tener... No tenía ni idea de dónde venía ese dinero... El estafador estaba furioso, exigiendo que si no devolvía el dinero de inmediato, Microsoft me demandaría... Estaba aterrorizada..."

"Me dijo que transfiriera los \$20,000 a una subsidiaria de Microsoft en Vietnam... Después de completar la transferencia bancaria, llamé a USAA... Me dijeron... que me habían estafado..."

"... Después de sufrir esta estafa, estaba sola y deprimida, e incluso perdí los deseos de vivir."

"Estoy aquí hoy porque soy una sobreviviente... Espero que podamos evitar que otros caigan en esta miseria sin igual, salvando a otros de caer en la oscuridad que conlleva perder la autoestima y los ahorros para la jubilación en un clic."

*Fragmentos del testimonio que la Sra. Fehler proporcionó al Comité para la Vejez en septiembre de 2022.*



## 4. Estafas de soporte técnico e informáticas

Las estafas por computadoras son producto de malhechores que fingen estar asociados con una compañía de tecnología conocida como Microsoft, Apple o Dell. Como testificó la Sra. Fehler, pueden usar tácticas como afirmar falsamente que la computadora de la víctima ha sido infectada con un virus, o solicitar que la misma les proporcione información personal y/o acceso remoto a su computadora. También pueden solicitar el número de una tarjeta de crédito o de cuenta bancaria para que puedan “facturar” por sus servicios de eliminación del virus.

En una estafa similar, la víctima elegida puede ver una ventana emergente en la pantalla de su computadora que advierte sobre una amenaza a la seguridad, e instruye al usuario para que se comunice con un agente de soporte técnico que es en definitiva el mismo estafador. La FTC informa que, en 2022, los adultos mayores fueron seis veces más propensos a denunciar pérdidas de dinero a causa de estafas de soporte técnico, en comparación con las personas más jóvenes.<sup>13</sup>

## SEÑALES DE ALERTA

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafa:

- Recibe una alerta indicando que hay un virus en su teléfono y debe llamar a un número determinado para resolver el problema.
- Un estafador le dice que la única solución para salvar su dinero de la amenaza de un hacker o pirata informático es transferirle a él los fondos de su cuenta para eliminar el supuesto virus.
- Si dice que prefiere solucionar el problema yendo usted mismo a una tienda convencional o contactando una empresa, el estafador que llama intentará convencerlo de que la acción del virus está cronometrada, y que solo él puede ayudarlo.

## PASOS PARA PREVENIR Y RESPONDER

- Si recibe una alerta indicando que su teléfono o computadora tiene un virus, no llame al número proporcionado en el aviso. Por el contrario, llame al número telefónico oficial de soporte técnico de su dispositivo (por ejemplo, Apple o Microsoft).
- Si una persona le llama diciendo que su dispositivo ha sido pirateado o afectado por un virus, anote el número telefónico, cuelgue y bloquéelo.
- Nunca proporcione información personal o financiera a una persona que llame inesperadamente.
- No le dé acceso remoto a un dispositivo o cuenta a menos que se haya puesto en contacto primero con esa empresa y sepa que es legítima.

- Reporte todas las llamadas o mensajes sospechosos a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea a <https://reportfraud.ftc.gov/>.

## MÁS INFORMACIÓN

- Para obtener más detalles sobre las estafas de soporte técnico, el Better Business Bureau tiene información útil en <https://www.bbb.org/article/news-releases/16553-bbb-tip-tech-support-scams>.
- La FTC proporciona información adicional sobre cómo detectar y evitar las estafas de soporte técnico en <https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams>.



## 5. Estafas "románticas"

Las redes sociales, los sitios de citas y otras aplicaciones son vías que los estafadores utilizan para comunicarse con sus víctimas, generar confianza y crear relaciones amorosas. Estos estafadores se enfocan en personas que buscan compañía y, a menudo, se apresuran a confesar su pasión o enamoramiento. Además, pueden pedir dinero para costear la solución de asuntos familiares, boletos de avión, gastos médicos, tarifas de aduana o documentos de viaje. Con frecuencia, el malhechor "vive en el extranjero". La FTC informa que en 2022, cerca de 70,000 consumidores denunciaron haber sido víctimas de las estafas "románticas", con pérdidas reportadas que totalizaron \$1.3 mil millones.<sup>14</sup>

### DENUNCIAS A LA LÍNEA DIRECTA CONTRA EL FRAUDE

*Una mujer residente en Pensilvania llamó a la Línea directa contra el fraude para denunciar una estafa romántica dirigida a su madre. La persona que llamó dijo que su madre envió casi \$20.000 en tarjetas de regalo a alguien que se hacía pasar por Johnny Depp.*

## SEÑALES DE ALERTA

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafa:

- La persona nunca le contacta por videollamada ni se encuentra con usted personalmente.
- No tienen amigos en común en las redes sociales, y su identidad es difícil de rastrear en línea.
- Afirman estar enamorados antes de conocerle en persona.
- Planean visitarle, pero siempre recurren a una excusa de último minuto explicando por qué no pueden hacerlo.
- Solicitan que el dinero se envíe mediante criptomonedas, transferencia bancaria o tarjeta de regalo.

## PASOS PARA PREVENIR Y RESPONDER

- Si la persona siempre se niega a hacer videollamadas o reunirse con usted en persona, bloquéela.
- Nunca envíe dinero o regalos a alguien que no haya conocido personalmente.
- Hable con su familia y amigos, o con alguien en quien confíe, para pedir consejo.
- Póngase en contacto con su banco de inmediato si cree que envió dinero a un estafador.
- Reporte todas las llamadas o mensajes sospechosos a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en <https://reportfraud.ftc.gov/>.

## MÁS INFORMACIÓN

- El Servicio Secreto de los Estados Unidos proporciona consejos sobre cómo evitar las estafas románticas en <https://www.secretservice.gov/investigation/romancescams>.
- La FTC proporciona información y recursos para denunciar en <https://consumer.ftc.gov/articles/what-know-about-romance-scams>.



## 6. Estafas de impostores del gobierno

**Históricamente, las estafas de impostores del gobierno eran las principales reportadas a la Línea contra el fraude. En 2022, pasaron al sexto lugar porque aparentemente los delincuentes se están haciendo pasar cada vez más por otras entidades como negocios e instituciones financieras. En esta variante, los malhechores se identificarán como un representante de una agencia federal como la Administración del Seguro Social (SSA) o el Servicio de Impuestos Internos (IRS). Pueden amenazar con afectar los beneficios de una persona, o exigir que se les envíe dinero para “pagar impuestos o tarifas.” Entre los diferentes tipos de estafas de impostores del gobierno, las relacionadas con el Seguro Social fueron las más reportadas a la línea directa.**

## **DENUNCIAS A LA LÍNEA DIRECTA CONTRA EL FRAUDE**

*Una mujer residente en Delaware informó que su exesposo fue contactado por un estafador que se hizo pasar por una agencia gubernamental. A la víctima se le dijo que su número de Seguro Social se había visto comprometido y se le indicó que enviara \$22,000 para resolver el problema. La víctima envió dinero en efectivo a través de UPS. Afortunadamente, la persona que llamó pudo ponerse en contacto con UPS a tiempo y detener la entrega.*

## **SEÑALES DE ALERTA**

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafa:

- Recibe una llamada telefónica, o un mensaje de texto o correo electrónico solicitando confirmar la información que la agencia gubernamental ya debe tener, como una dirección o el Número de Seguro Social.
- La persona que llama o envía el mensaje por correo electrónico amenaza con afectar sus beneficios, le pide que transfiera dinero, que lo deposite en una tarjeta de débito prepagada o tarjeta de regalo, o le dice que envíe efectivo o cheque utilizando un servicio de entrega nocturna. También puede pedirle que pague con criptomonedas o mediante la aplicación P2P.
- Está siendo presionado para tomar una decisión rápida y urgente, a veces dentro de un día o semana.

## PASOS PARA PREVENIR Y RESPONDER

- Cuelgue el teléfono o no responda al mensaje de correo electrónico o de texto.
- Nunca dé ni confirme información financiera o confidencial en respuesta a llamadas inesperadas, o si tiene alguna sospecha.
- No confíe naturalmente en un nombre o un número. Los estafadores pueden usar nombres aparentemente oficiales para que confíe en ellos. Para que su llamada parezca legítima, también pueden usar tecnología que oculta su número de teléfono verdadero.
- Una agencia gubernamental nunca le pedirá que transfiera dinero, proporcione su Número de Seguro Social o envíe fondos mediante una tarjeta de regalo.
- Llame directamente al número de la agencia federal y espere a hablar con un representante de servicio al cliente, para verificar la llamada o el mensaje de correo electrónico que recibió.
- Reporte todas las llamadas o mensajes sospechosos a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en <https://reportfraud.ftc.gov/>.

## MORE INFORMATION

- La FTC proporciona consejos sobre cómo detectar y evitar estafas de impostores en <https://consumer.ftc.gov/features/imposter-scams>.

02  
49  
15

## 7. Estafas de sorteos y lotería

Las estafas de sorteos tienen la intención de robar a los adultos mayores haciéndoles creer que han ganado una lotería o un premio, y solo necesitan “dar algunos pasos” para obtener sus ganancias. A menudo, el estafador solicita que la víctima pague una tarifa o impuesto para cobrar sus ganancias o mejorar sus probabilidades de ganar. Los delincuentes pueden advertirle a la persona que no le comunique la noticia a nadie, ya que será “una sorpresa” para sus amigos y familiares. También pueden pedir que envíe dinero mediante tarjetas de regalo, transferencia bancaria electrónica, pagos vía aplicaciones P2P, giro postal o criptomonedas, para reclamar el premio. Estos métodos de pago son de uso común por los estafadores, porque resulta difícil recuperar el dinero una vez realizada la transacción. En 2022, la FTC descubrió que las víctimas reportaron pérdidas por \$302 millones a consecuencia de supuestos premios, sorteos y otras estafas relacionadas con la lotería.<sup>15</sup>

## **DENUNCIAS A LA LÍNEA DIRECTA CONTRA EL FRAUDE**

*Un veterano de Georgia llamó a la Línea directa contra el fraude para informar que pagó miles de dólares para cobrar \$1.2 millones de una estafa de sorteos. Los estafadores le dijeron que le devolverían lo que pagó.*

## **SEÑALES DE ALERTA**

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafa:

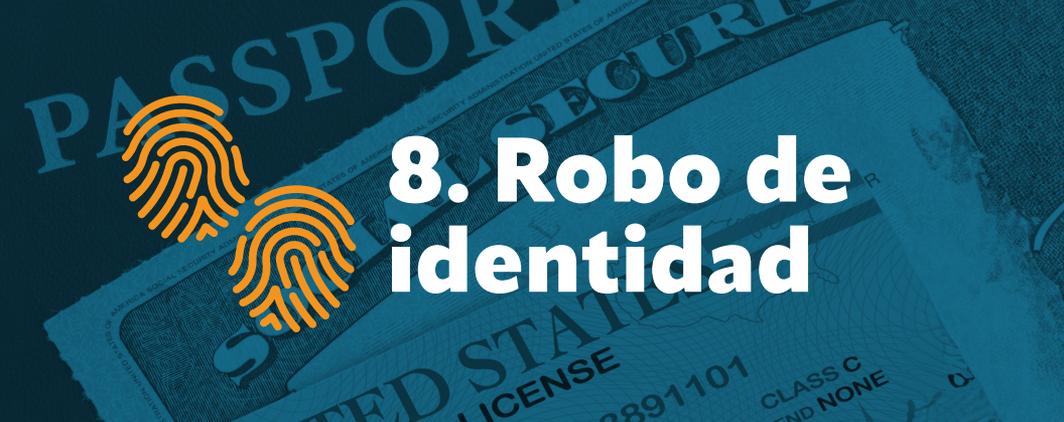
- Usted recibe una llamada o mensaje diciéndole que ha ganado un premio, pero para reclamarlo debe pagar un "impuesto" o "tarifa de procesamiento".
- La persona que dice que usted ha ganado un premio trata de convencerle de que la familia y los amigos preocupados están celosos o equivocados.
- Se le pide que pague el "impuesto" o la "tarifa de procesamiento" transfiriendo dinero, o enviándolo por correo postal o mediante tarjeta de regalo, aplicación P2P, o criptomonedas.
- Se le pide que le mienta a su banco sobre el motivo del pago (por ejemplo: "Dígale a su banco que este dinero es para su hermana").

## PASOS PARA PREVENIR Y RESPONDER

- Si recibe una llamada diciendo que ha ganado un premio y la persona que llama menciona un "impuesto" o "tarifa," escriba el número, cuelgue y bloquéelo.
- No responda las cartas, mensajes de texto o de correo electrónico donde le dicen que ha ganado un premio si mencionan un "impuesto" o "tarifa" para reclamarlo.
- Reporte cualquier llamada, correo electrónico o postal sospechoso a la FTC o a la policía local. También puede presentar una queja en línea en <https://reportfraud.ftc.gov/>.

## MÁS INFORMACIÓN

- El Better Business Bureau tiene consejos sobre cómo identificar y evitar estas estafas en <https://www.bbb.org/article/news-releases/16923-bbb-tip-sweepstakes-lottery-and-prize-scams>.
- La FTC proporciona más información sobre estafas de premios, sorteos y lotería en <https://consumer.ftc.gov/articles/fake-prize-sweepstakes-lottery-scams>.

The background image shows a blue-tinted collage of a passport and a driver's license. Two orange fingerprints are overlaid on the documents. The passport text includes 'PASSPORT' and 'UNITED STATES OF AMERICA'. The driver's license text includes 'UNITED STATES', 'LICENSE', '3891101', and 'CLASS C END NONE'.

## 8. Robo de identidad

**Las estafas de robo de identidad se producen cuando un delincuente obtiene y utiliza indebidamente los datos personales de su víctima. Un objetivo común para el robo de identidad es el acceso autorizado a la cuenta bancaria de una persona. También puede consistir en robar números de Seguro Social, dirección personal o incluso información de atención médica. Los estafadores pueden retirar dinero, ingresar solicitudes falsas de préstamos o reclamar beneficios como el del Seguro Social o desempleo en nombre del adulto mayor. En 2022, la FTC recibió más de 1.1 millones de denuncias de robo de identidad.<sup>16</sup>**

### **DENUNCIAS A LA LÍNEA DIRECTA CONTRA EL FRAUDE**

*Una mujer residente en Carolina del Sur se puso en contacto con la Línea directa contra el fraude para denunciar que su información personal estaba siendo utilizada en otro estado, y que alguien estaba cobrando ingresos como si fuera ella. También informó que su puntaje de crédito había disminuido como resultado.*

## SEÑALES DE ALERTA

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafa:

- Usted recibe una llamada o mensaje no solicitado donde se le pide información personal.
- Usted nota actividad inusual en su reporte de crédito o cuenta bancaria, o nuevas líneas de crédito o préstamos a su nombre.
- Usted recibe facturas médicas desconocidas por procedimientos que no le realizaron, o trastornos de salud inexactos en su historia clínica.
- Usted no recibe los beneficios, como el del Seguro Social o un reembolso de impuestos, a pesar de que su cuenta dice que los fondos fueron enviados.

## PASOS PARA PREVENIR Y RESPONDER

- Si alguien le pide su Número de Seguro Social o información personal por teléfono, cuelgue. Si afirman ser de funcionarios de una compañía o agencia legítima, vaya al sitio web oficial de esa organización y llame a su línea oficial para verificar.
- No haga clic en enlaces de correo electrónico ni abra archivos adjuntos, incluso si el mensaje procede aparentemente de una empresa que conoce. Si lo hace, puede poner en peligro su información personal. Si desea visitar el sitio web escrito en el mensaje de correo electrónico, hágalo manualmente en una pestaña de búsqueda (search tab) separada.
- Actualice las contraseñas de sus cuentas, especialmente si sospecha o se entera de que su banco o compañía de tarjetas de crédito fue pirateada. No utilice la misma contraseña para acceder a todas sus cuentas.

- Suscríbase a alertas por mensajes de texto y correo electrónico, especialmente aquellas que le informen sobre actividades inusuales.
- Reporte todas las llamadas, mensajes o correspondencia sospechosa a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en <https://reportfraud.ftc.gov/>.

## MÁS INFORMACIÓN

- Se puede encontrar más información sobre el robo de identidad en el sitio web del Departamento de Justicia en <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud>.
- Reporte las denuncias de robo de identidad y encuentre recursos de recuperación en <https://www.identitytheft.gov>.



## **9. Estafas de suplantación de identidad comercial y compras**

**Los estafadores no solo se hacen pasar por agencias gubernamentales. También pueden fingir que son funcionarios empresariales. Estos delincuentes pueden alertar sobre la existencia de compras no autorizadas o actividad sospechosa en la cuenta empresarial de una persona. Los falsos empresarios también pueden proporcionar números de teléfono falsos a clientes desconocedores. Los estafadores solicitan información personal o financiera del individuo para “resolver” el problema y, en su lugar, obtener acceso a su cuenta. Según la FTC, en 2022, los adultos mayores sufrieron pérdidas por \$271 millones a causa de estafas de suplantación de identidad comercial, o sea, cerca de un 80 por ciento más en comparación con 2021.<sup>17</sup>**

## **DENUNCIAS DE LA LÍNEA DIRECTA CONTRA EL FRAUDE**

*Una mujer residente en Nueva York recibió una llamada de su proveedor de Internet informándole que el pago estaba pendiente. Cuando la persona que llamó colgó, la mujer se comunicó directamente con su proveedor de Internet, el cual le informó que su cuenta estaba vigente y que la llamada probablemente era una estafa.*

## **SEÑALES DE ALERTA**

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafa:

- Cuando usted desea averiguar sobre un reembolso, la persona que llama dice que debe proporcionarle acceso remoto a su computadora o cuenta.
- Un "representante comercial" le dice que se le reembolsó "accidentalmente" demasiado dinero a su cuenta y le pide que devuelva la diferencia.
- Recibe una llamada o un mensaje de correo electrónico donde se indica que se realizaron compras no autorizadas con su cuenta o que la misma fue pirateada. El "representante comercial" le sugiere que deberá comprar una tarjeta de regalo y enviar fotografías de los números de la parte posterior de la tarjeta para obtener acceso a su cuenta nuevamente.

## PASOS PARA PREVENIR Y RESPONDER

- Vaya al sitio web de la compañía o a su cuenta directamente para encontrar la información de contacto real.
- No proporcione acceso remoto a un dispositivo o cuenta a menos que se haya puesto en contacto primero con esa empresa y sepa que es legítima.
- Las empresas legítimas nunca requerirán que pague exclusivamente con tarjeta de regalo, aplicaciones P2P ni criptomonedas.
- Reporte todas las llamadas, mensajes o correspondencia sospechosa a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en <https://reportfraud.ftc.gov/>.

## MÁS INFORMACIÓN

- La Oficina Federal de Investigaciones (FBI) proporciona información sobre estafadores haciéndose pasar como empresas legítimas en <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise>.



## 10. Estafa a "personas necesitadas" y "abuelos"

Los delincuentes pueden hacerse pasar por familiares o amigos en estafas a "personas necesitadas" o "abuelos." Los impostores pueden hacerse pasar por un nieto o un oficial de la policía que ha detenido al nieto de la víctima. También pueden usar la IA para clonar la voz de una persona conocida por la víctima para afirmar que confronta un problema y necesita dinero para enfrentar una emergencia como salir de la cárcel, pagar una factura de hospital o salir de un país extranjero. Los estafadores juegan con las emociones y engañan a los miembros de la familia preocupados para que les transfieran dinero. El FBI reporta que desde enero 2020 a junio 2021, las víctimas de este tipo de estafas denunciaron pérdidas por \$13 millones.<sup>18</sup>

### INFORMES DE LA LÍNEA DIRECTA CONTRA EL FRAUDE

*Una mujer residente en Pensilvania llamó a la Línea directa contra el fraude para informar que recibió una llamada de alguien que decía ser su nieto. Dijo que habían tenido un accidente automovilístico y que necesitaban dinero para llegar a casa. La mujer sabía que su nieto no tiene auto, por lo que se dio cuenta de que era una estafa y colgó.*

## SEÑALES DE ALERTA

Estas son señales comunes de que puede estar siendo víctima de este tipo de estafas:

- La persona que llama le pide que envíe dinero de inmediato y ofrece detalles específicos sobre cómo hacerlo. Puede sugerirle que envíe el dinero mediante una tarjeta de regalo o transferencia bancaria.
- El “nieto” o el “oficial de la policía” que llama le pide que mantenga el incidente en secreto, a pesar de la supuesta urgencia de la situación.
- La persona que llama lo apresura y le pide que tome decisiones inmediatas con poca o ninguna información.
- La persona que llama asegura estar en una situación o lugar que no corresponde al comportamiento general de la persona por la que se hace pasar.

## PASOS PARA PREVENIR Y RESPONDER

- Cuelgue y llame a su familiar o a un amigo genuino para verificar que no ha ocurrido ningún problema.
- Si la persona afirma ser un oficial de la policía, cuelgue y llame a la agencia de orden público correspondiente para verificar la identidad de la persona y cualquier información que haya proporcionado. Tenga en cuenta que las agencias policiales nunca contactarán a un familiar para solicitar el pago de una fianza en representación de otra persona.
- Analice el incidente con familiares y amigos de confianza, incluso si le han dicho que lo mantenga en secreto.
- Verifique su configuración en redes sociales y limite la información que usted proporciona en línea. Los delincuentes pueden intentar hacer uso de detalles personales para enfocarse mejor en su estafa y hacerla mucho más convincente.

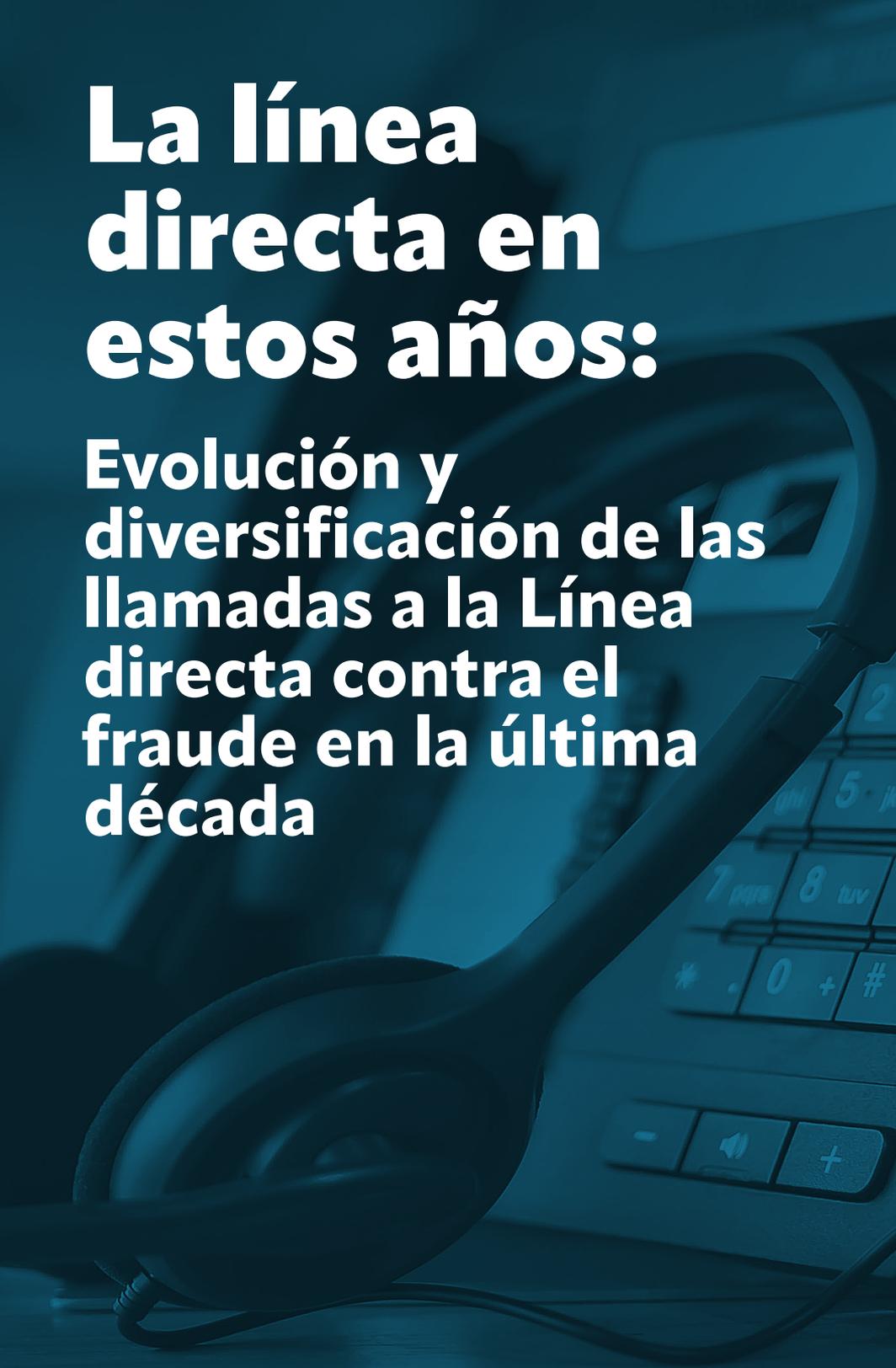
- Reporte todas las llamadas o mensajes sospechosos a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en <https://reportfraud.ftc.gov/>.

## MÁS INFORMACIÓN

- La FTC tiene consejos útiles con respecto a estas llamadas en <https://www.consumer.ftc.gov/articles/0204-family-emergency-scams>.
- La FCC proporciona más información para evitar estas estafas <https://www.fcc.gov/grandparent-scams-get-more-sophisticated>.
- Para más detalles acerca del uso de la IA en este tipo de estafas, la FTC tiene información útil en <https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes>.

# **La línea directa en estos años:**

**Evolución y  
diversificación de las  
llamadas a la Línea  
directa contra el  
fraude en la última  
década**



**11,800**  
**LLAMADAS**

**22**  
**AUDIENCIAS**

**7** GUÍAS  
**CONTRA**  
**EL FRAUDE**

**4**  
**LEYES**

In en los últimos 10 años, el Comité ha recibido casi 11,800 llamadas a la Línea directa contra el fraude, ha celebrado 22 audiencias para examinar fraudes y estafas, ha publicado 7 guías contra el fraude, y ha aprobado 4 leyes para abordar los fraudes y las estafas dirigidas a los adultos mayores, incluida Stop Senior Scams, y Senior Safe Act.

Si bien las estafas evolucionan constantemente, utilizan nuevas tecnologías y desarrollan nuevas formas de privarle de su dinero; muchas de las principales estafas reportadas a la Línea directa contra el fraude continúan presentándose año tras año.

Esto se refleja mejor en los informes que la Línea directa contra el fraude ha recibido en los últimos 10 años, algunos de los cuales se muestran a continuación. Para muchas de estas llamadas, el método de pago o contacto ha cambiado, pero la estafa

se ha mantenido en gran medida igual.

En 2013 y 2014, por ejemplo, los estafadores utilizaron métodos como una tarjeta de débito prepagada para obtener fondos de las víctimas. Ahora, los estafadores también utilizan aplicaciones de pago P2P, tarjetas de regalo y criptomonedas. Los estafadores también utilizan cada vez más la tecnología de IA para atacar y obligar a las víctimas potenciales. A menudo a las víctimas se les hace difícil saber si fueron estafadas con la ayuda de la IA, pero en general, la tecnología ha hecho que las estafas tradicionales, como las de abuelos y las de impostores, sean más convincentes y más fáciles y económicas de implementar para el estafador.

## Estafa del impostor del gobierno antes y ahora:



*En 2014, una mujer residente en Missouri denunció que su madre fue*

*contactada por un vendedor de puerta en puerta. A la madre de la persona que llamó le dijeron que podía inscribirse para que un médico fuera a su casa y le informara sobre los servicios que ofrece Medicare. La señora firmó algunos formularios y proporcionó su Número de Seguro Social y su Identificador de Beneficiario de Medicare al estafador.*



*En 2021, un hombre residente en Massachusetts recibió un mensaje grabado*

*en el que se afirmaba que su Número de Seguro Social se había visto comprometido. Cuando habló con la persona que decía ser de la SSA, la persona que llamó solicitó los últimos cuatro dígitos de su Número de Seguro Social. El hombre pidió varias veces el número de identificación de empleado de la SSA de la persona que llamaba, y el estafador finalmente colgó.*

## Estafas "románticas" antes y ahora:



*En 2014, una persona que llamó informó que un hombre que conoció*

*en eHarmony [sitio de citas en línea] le estafó \$1,500. El estafador también le pidió a la persona que llamaba que abriera una cuenta bancaria y le proporcionara la información de la misma para poder convertirla en beneficiaria de cierta cantidad de oro que supuestamente encontró.*



*En 2022, una persona que llamó desde Mississippi informó que su madre conoció*

*a un hombre en Facebook y comenzó a comunicarse con él a través de Facebook Messenger. El estafador afirmó que estaba realizando una misión en el extranjero y no podía acceder a su dinero. La madre de la persona que llamaba le había estado enviando tarjetas de regalo.*

## Estafas de suplantación de identidad comercial antes y ahora:



*En 2013, una persona que llamó informó que un estafador que se hacía*

*pasar por UPS se había puesto en contacto con él por teléfono. El estafador le dijo a la persona que llamó que UPS estaba tratando de entregar un paquete del IRS, pero que había franqueo adeudado. La persona que llamó colgó. El estafador volvió a llamar y dejó un mensaje diciéndole a la persona que llamaba que comprara una tarjeta de dinero prepagada para pagar el franqueo y enviar el paquete por correo a la Florida.*



*En 2022, un hombre residente en Minnesota dijo que un estafador*

*se puso en contacto con él a través de un mensaje de texto. El estafador afirmó ser un empleado de Amazon y dijo que la persona que llamaba tenía que actualizar su membresía de Amazon Prime o perdería el acceso. La persona que llamó pagó \$159.99 por PayPal [aplicación de pago P2P]. Por suerte, la persona que llamó se dio cuenta de que era una estafa y pudo cancelar el pago.*

**El Comité ha demostrado un firme compromiso de educar a los consumidores sobre los métodos siempre cambiantes que utilizan los estafadores y continuará buscando oportunidades para adelantarse a la nueva tecnología de los estafadores.**

# Número de quejas reportadas a la Línea directa contra el fraude por estado





<b>Estado</b>	<b>2015 - 2021</b>	<b>2022</b>	<b>Total</b>
Illinois	143	20	163
Indiana	58	5	63
Iowa	135	3	138
Kansas	32	10	42
Kentucky	45	3	48
Luisiana	33	6	39
Maine	2,596	56	2,652
Maryland	483	16	499
Massachusetts	114	73	187
Michigan	134	3	137
Minnesota	59	7	66
Mississippi	18	2	20
Missouri	59	5	64
Montana	22	0	22
Nebraska	27	3	30
Nevada	38	8	46
Nueva Hampshire	32	4	36
Nueva Jersey	118	7	125
Nuevo México	32	4	36
Nueva York	468	26	494
Carolina del Norte	97	13	110
Dakota del Norte	10	2	12
Ohio	136	8	144
Oklahoma	38	7	45
Oregón	61	8	69
Pensilvania	655	46	701
Rhode Island	79	0	79
Carolina del Sur	73	14	87
Dakota del Sur	16	0	16

<b>Estado</b>	<b>2015 - 2021</b>	<b>2022</b>	<b>Total</b>
Tennessee	77	11	88
Tejas	573	16	589
Utah	74	3	77
Vermont	6	0	6
Virginia	175	11	186
Washington	141	13	154
Virginia Occidental	36	1	37
Wisconsin	55	7	62
Wyoming	12	0	12
Puerto Rico	1	0	1
Fuera de los EE.UU.	1	0	1
Desconocidos	403	79	482
<b>Todas las áreas</b>	<b>9,069</b>	<b>659</b>	<b>9,728*</b>

**Nota:** Si bien la Línea directa contra el fraude se creó en 2013, los datos recopilados en 2013 y 2014 están incompletos e incompatibles con los recopilados desde 2015 hasta 2022. Por esa razón, el Comité optó por no incorporarlos a este análisis. El número de llamadas no es una medida estadísticamente representativa de la incidencia de estafas o explotación financiera de los adultos mayores en cada estado. Es probable que las llamadas a la Línea directa contra el fraude reflejen el conocimiento del consumidor sobre la Línea directa contra el fraude en cada estado/jurisdicción.

*\*En 2013 y 2014 se presentaron 2,057 quejas adicionales a la Línea directa contra el fraude.*

# Recursos



# CONSEJOS ADICIONALES SOBRE CÓMO PROTEGERSE DE LOS DIFERENTES MÉTODOS DE CONTACTO UTILIZADOS POR LOS ESTAFADORES:

**Mensajes de texto:** Los estafadores suelen utilizar estafas por mensajes de texto para hacerse pasar por empresas conocidas, como un banco o un servicio de entrega de paquetes. Podrían prometer un regalo, un premio o un empleo. Una cosa es cierta: estos estafadores están tratando de apoderarse de su dinero e información personal.

## Consejos para protegerse:

- Si recibe un mensaje de texto inesperado de un remitente desconocido, no haga clic en ningún enlace ni responda al mensaje. Si cree que el mensaje de texto es legítimo, comuníquese directamente con la empresa. No utilice la información de contacto proporcionada en el mensaje de texto.
- No pague para que le vuelvan a entregar un paquete. Las empresas de entrega de paquetes nunca solicitarán un pago para volver a entregar un paquete.
- Puede denunciar estas estafas por mensaje de texto reenviándolas al 7726 (SPAM). Esto puede ayudar a su proveedor de telefonía celular a identificar y bloquear mensajes de spam similares.

**Ventanas emergentes y anuncios en línea:** Las ventanas emergentes son una estrategia común utilizada por los estafadores de “soporte técnico,” que se analizan más adelante en esta guía.

Los anuncios en línea se utilizan para hacerse pasar por empresas y minoristas legítimos. A menudo, estos anuncios anuncian ofertas que son “demasiado buenas para ser ciertas”. Los estafadores roban la información de la víctima, como un número de tarjeta de crédito, una vez que se realiza la compra.

## **Consejos para protegerse de anuncios y ventanas emergentes fraudulentas en línea:**

- No haga clic en ningún enlace de ventanas emergentes y anuncios en línea de un sitio web. Para visitar un sitio web, escriba la dirección del mismo directamente en el navegador.
- Haga una copia de seguridad de sus datos con regularidad. Las copias de seguridad pueden ser la mejor manera de recuperar su información y archivos si su computadora está infectada con un virus o ransomware (programa de secuestro de datos).
- No descargue software de sitios que no conoce.
- Autorice su software antivirus y antimalware para que se actualice automáticamente, y analice regularmente su computadora en busca de virus y malware.

**Redes sociales:** Las redes sociales son uno de los métodos de contacto más comunes utilizados por los estafadores que tienen como objetivo a los adultos mayores en línea, y les ofrecen la oportunidad de acceder a datos personales y ganarse la confianza de la víctima.

## **Consejos para protegerse de estafadores en las redes sociales:**

- Use una contraseña sólida y configuración de seguridad que oculte información como su ciudad de residencia, número telefónico y fecha de nacimiento.
- No acepte una nueva solicitud de amistad de desconocidos, de alguien a quien ya tiene como "amigo" en las redes sociales, o de alguien que usted sabe que no usa las redes sociales.
- No haga clic en enlaces enviados por amigos con los que normalmente no se comunica. Estos enlaces suelen invitarle a visitar un sitio web para reclamar un premio, ganar una tarjeta de regalo, responder un cuestionario, completar una encuesta o ver un video.
- Confirme con un amigo o contacto, o reúnanse con los mismos en persona, si recibe una solicitud urgente en línea de ellos para obtener dinero o una inversión. Tenga en cuenta: Su cuenta puede haber sido pirateada, especialmente si le piden que envíe criptomonedas, tarjetas de regalo o una transferencia bancaria.

## RECURSOS ADICIONALES DE AGENCIAS Y OTRAS ORGANIZACIONES

Estas organizaciones y sitios web proporcionan información sobre una amplia gama de estafas, incluidos otros engaños comunes dirigidos a adultos mayores que no se reseñan en esta guía.

<b>Entidad</b>	<b>Sitio web</b>
Better Business Bureau (BBB)	<a href="https://www.bbb.org/scamtracker">https://www.bbb.org/scamtracker</a>
AARP Fraud Watch Network	<a href="https://www.aarp.org/fraudwatchnetwork">https://www.aarp.org/fraudwatchnetwork</a>
Comisión Federal de Comercio (FTC)	<a href="https://www.consumer.ftc.gov/scams">https://www.consumer.ftc.gov/scams</a>
FBI	<a href="https://www.fbi.gov/scams-and-safety/common-scams-and-crimes">https://www.fbi.gov/scams-and-safety/common-scams-and-crimes</a>
USA.gov	<a href="https://www.usa.gov/common-scams-frauds">https://www.usa.gov/common-scams-frauds</a>

## CÓMO DENUNCIAR ABUSOS FINANCIEROS A ADULTOS MAYORES

Los perpetradores de las estafas analizadas en esta guía son principalmente desconocidos, que operan a menudo desde un estado o país diferente al de su víctima. Sin embargo, cada año millones de adultos mayores estadounidenses son explotados por personas a quienes conocen, ya sea un miembro de la familia, cuidador, amigo, profesional financiero u otra persona de confianza. Muchos adultos mayores que son abusados financieramente también sufren abusos de otras maneras.

- Si conoce a alguien que está en riesgo inmediato, llame al **9-1-1**.
- Reporte el incidente a los Servicios de Protección para Adultos (APS, por sus siglas en inglés). Use la lista de National Adult Protective Services Association (NAPSA) para encontrar el número de teléfono del APS en su área <https://www.napsa-now.org/aps-program-list/> o llame al **2-1-1**.
- Si el abuso está teniendo lugar en un centro de atención a largo plazo, como un hogar de ancianos o un centro de vida asistida, un defensor de atención a largo plazo puede ayudar. Use el mapa interactivo del Consumer Voice National Long-Term Care Ombudsman Resource Center para encontrar un Programa de defensores de cuidados a largo plazo en su área: [https://theconsumervoice.org/get\\_help](https://theconsumervoice.org/get_help).
- Póngase en contacto con su congresista o senador. Puede denunciar el fraude en sus oficinas, y ellos le proporcionarán ayuda. Para localizar a su congresista usando su código postal, visite <https://www.house.gov>. Para ubicar a su senador, visite <https://www.senate.gov/senators/senators-contact.htm>. También puede llamar al número telefónico **(202) 224-3121**. La operadora le conectará directamente con la oficina que solicite.

## **CÓMO BUSCAR AYUDA DESPUÉS DE UNA ESTAFA**

Las estafas afectan nuestra salud financiera, emocional y física. Hay recursos para ayudarle a responder y recuperarse del fraude.

### **Apoyo y asesoramiento a las víctimas**

**Recurso:** Centro de recursos de VictimConnect

**Sitio web:** <https://victimconnect.org/>

**Teléfono:** 1-855-484-2846

### **Ayuda jurídica**

**Recurso:** Legal Services Corporation

**Sitio web:** <https://www.lsc.gov/about-lsc/what-legal-aid/get-legal-help>

**Teléfono:** Use la herramienta de búsqueda para encontrar el número telefónico de la oficina de ayuda jurídica local

### **Para otros servicios**

**Recurso:** Eldercare Locator

**Sitio web:** <https://eldercare.acl.gov/>

**Teléfono:** 1-800-677-1116

## PROCURADORES GENERALES ESTATALES

Puede llamar a la oficina de su Procurador General, según su estado de residencia:

<b>ESTADO/TERRITORIO</b>	<b>NÚMERO TELEFÓNICO</b>
Alabama	(334) 242-7300
Alaska	(907) 269-5100
Samoa Americana	(684) 633-4163
Arizona	(602) 542-5025
Arkansas	(800) 482-8982
California	(916) 445-9555
Colorado	(720) 508-6000
Connecticut	(860) 808-5400
Delaware	(302) 577-8600
Distrito de Columbia	(202) 442-9828
Florida	(850) 414-3300
Georgia	(404) 651-8600
Guam	(671) 475-2720
Hawái	(808) 586-1500
Idaho	(208) 334-2400
Illinois	(312) 814-3000
Indiana	(317) 232-6330
Iowa	(515) 281-5926
Kansas	(785) 296-3751

<b>ESTADO/TERRITORIO</b>	<b>NÚMERO TELEFÓNICO</b>
Kentucky	(502) 696-5300
Luisiana	(225) 326-6465
Maine	(207) 626-8800
Maryland	(410) 576-6300
Massachusetts	(617) 727-2200
Michigan	(517) 335-7622
Minnesota	(651) 296-3353
Mississippi	(601) 359-3680
Missouri	(573) 751-3321
Montana	(406) 444-2026
Nebraska	(402) 471-2682
Nevada	(702) 486-3132
Nueva Hampshire	(603) 271-3658
Nueva Jersey	(609) 292-8740
Nuevo México	(505) 490-4060
Nueva York	(518) 776-2000
Carolina del Norte	(919) 716-6400
Dakota del Norte	(701) 328-2210
Islas Marianas del Norte	(670) 237-7600
Ohio	(614) 466-4986
Oklahoma	(405) 521-3921

<b>ESTADO/TERRITORIO</b>	<b>NÚMERO TELEFÓNICO</b>
Oregón	(503) 378-4400
Pensilvania	(717) 787-3391
Puerto Rico	(787) 721-2900
Rhode Island	(401) 274-4400
Carolina del Sur	(803) 734-3970
Dakota del Sur	(605) 773-3215
Tennessee	(615) 741-3491
Tejas	(512) 463-2100
Islas Vírgenes Estadounidenses	(340) 774-5666
Utah	(800) 244-4636
Vermont	(800) 649-2424
Virginia	(804) 786-2071
Washington	(360) 753-6200
Virginia Occidental	(304) 558-2021
Wisconsin	(608) 266-1221
Wyoming	(307) 777-7841

También puede contactarlos en línea. La Asociación Nacional de Secretarios de Justicia (National Association of Attorneys General) proporciona una lista actualizada de todos los sitios web de cada Secretario Estatal de Justicia en: <https://www.naag.org/find-my-ag/>.

# TRES PASOS PARA AYUDARSE USTED MISMO Y A LOS DEMÁS



## Correr la voz

- Hable con familiares, amigos y vecinos.
- Comparta este libro sobre fraudes y lo que ha aprendido con otras personas.



## Denunciar la estafa

- A las autoridades: su información puede ayudar a identificar y localizar a los estafadores.
- A las empresas involucradas: a menudo también son víctimas y pueden ayudar a combatir a los estafadores junto con usted.



## Estar alerta y ser proactivo

- Considere inscribirse para recibir alertas de su banco y compañía de tarjeta de crédito, o de un servicio de monitoreo de crédito.
- Proteja su información en línea mediante el uso de contraseñas diferentes y seguras para sus cuentas. Utilice la autenticación de dos factores cuando esté disponible.
- Utilice las herramientas y consejos que le proporciona esta guía.

# **COMITÉ ESPECIAL DEL SENADO DE LOS ESTADOS UNIDOS PARA LA VEJEZ**

## **Línea directa contra el fraude**

La Línea directa contra el fraude es un recurso para que los adultos mayores estadounidenses mayores y sus familiares informen actividades sospechosas y proporcionen información sobre cómo denunciar fraudes y estafas a los funcionarios adecuados, incluida la policía.

**1-855-303-9470**

**LUN – VIE**

**9 AM a 5 PM Hora del Este (ET)**



## LISTA DE VERIFICACIÓN DE INFORMES Y NOTAS

Esta lista puede ayudarlo a reportar el incidente a las agencias y compañías.

Actuar pronto es importante. No espere a tener toda esta información antes de informar.

<input checked="" type="checkbox"/> Información importante que debe incluir en su queja	Sus notas
<input type="checkbox"/> ¿Cuándo sucedió?	
<input type="checkbox"/> ¿Cómo lo contactaron?	
<input type="checkbox"/> ¿Qué se le pidió que hiciera?	
<input type="checkbox"/> ¿Cuánto dinero se le pidió que proporcionara?	

<input type="checkbox"/>	¿Cómo se le pidió que proporcionara el dinero?	
<input type="checkbox"/>	¿Dónde dijo la persona que estaba ubicada?	
<input type="checkbox"/>	¿Reportó el incidente a la empresa implicada o a la institución financiera?	
<input type="checkbox"/>	¿Reportó este incidente a alguien más?	
<input type="checkbox"/>	¿Se le reembolsó algo del dinero que envió?	
<input type="checkbox"/>	¿Hubo algún otro efecto (cuenta cerrada, robo de identidad)?	

---

---

---

---

---

**Advertencia:** La Guía proporciona información general al consumidor sobre fraudes y estafas. Esta información puede incluir enlaces a recursos o contenido de terceros. El Comité no respalda a esos terceros. Puede haber otros recursos que también satisfagan sus necesidades.

## NOTAS FINALES

- 1 Federal Trade Commission (FTC), "FTC crunches the 2022 numbers. See where scammers continue to crunch consumers," <https://www.ftc.gov/business-guidance/blog/2023/02/ftc-crunches-2022-numbers-see-where-scammers-continue-crunch-consumers> (visita más reciente, 22 de octubre, 2023)
- 2 FTC, "Scammers use AI to enhance their family emergency schemes," <https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes> (visita más reciente, 22 de octubre, 2023)
- 3 Federal Bureau of Investigations (FBI), Elder Fraud Report 2022, pg 9, [https://www.ic3.gov/Media/PDF/AnnualReport/2022\\_IC3ElderFraudReport.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf) (visita más reciente, 3 de noviembre, 2023)
- 4 Análisis de datos de la FTC por el personal del Comité para la Vejez. El análisis incluye total de quejas de todas las edades en 2022. Los datos de la FTC están disponibles en: <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods> (visita más reciente, 22 de octubre, 2023)
- 5 Este análisis fue realizado por el personal del Comité para la Vejez e incluyó a las personas que no respondieron a preguntas referentes a pérdidas monetarias o de propiedad.
- 6 Este análisis fue realizado por el personal del Comité para la Vejez e incluyó a personas que no revelaron su relación con la víctima.

- 7 FTC, Explore Debt Collection Reports, <https://public.tableau.com/app/profile/federal.trade.commission/viz/DebtCollection/Infographic> (visita más reciente, 22 de octubre, 2023)
- 8 FTC, Consumer Sentinel Network Data Book 2022, pg 7, [https://www.ftc.gov/system/files/ftc\\_gov/pdf/CSN-Data-Book-2022.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf) (visita más reciente, 22 de octubre, 2023).
- 9 FTC, "New FTC Data Analysis Shows Bank Impersonation is Most-Reported Text Message Scam," <https://www.ftc.gov/news-events/news/press-releases/2023/06/new-ftc-data-analysis-shows-bank-impersonation-most-reported-text-message-scam> (last visited October 22, 2023)
- 10 FTC, "IYKYK: The top text scams of 2022," <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/06/iykyk-top-text-scams-2022> (visita más reciente, 22 de octubre, 2023)
- 11 Federal Communications Commission (FCC), "Health Care Scams Tend to Spike During Open Enrollment," <https://www.fcc.gov/health-care-scams-tend-spike-during-open-enrollment> (visita más reciente, 22 de octubre, 2023)
- 12 FCC, "Stop Unwanted Robocalls and Texts," <https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts> (visita más reciente, 22 de octubre, 2023)

- 13 FTC, "FTC Issues Annual Report to Congress on Agency's Actions to Protect Older Adults," <https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults> (visita más reciente, 22 de octubre, 2023)
- 14 FTC, "Romance scammers' favorite lies exposed," <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed> (visita más reciente, 22 de octubre, 2023)
- 15 FTC, Consumer Sentinel Network Data Book 2022, pg 8, [https://www.ftc.gov/system/files/ftc\\_gov/pdf/CSN-Data-Book-2022.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf) (visita más reciente, 22 de octubre, 2023)
- 16 FTC, Protecting Older Consumers 2022-2023, pg 25 [https://www.ftc.gov/system/files/ftc\\_gov/pdf/p144400olderadultsreportoct2023.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf) (visita más reciente, 27 de octubre, 2023)
- 17 FTC, "FTC Issues Annual Report to Congress on Agency's Actions to Protect Older Adults," <https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults> (visita más reciente, 22 de octubre, 2023)
- 18 FBI, "FBI Miami Warns of Grandparent Fraud Scam," <https://www.fbi.gov/contact-us/field-offices/miami/news/fbi-miami-warns-of-grandparent-fraud-scheme> (visita más reciente, 22 de octubre, 2023)











**Línea directa contra el fraude**

**1-855-303-9470**



**Comité Especial del Senado de  
los Estados Unidos para la Vejez**