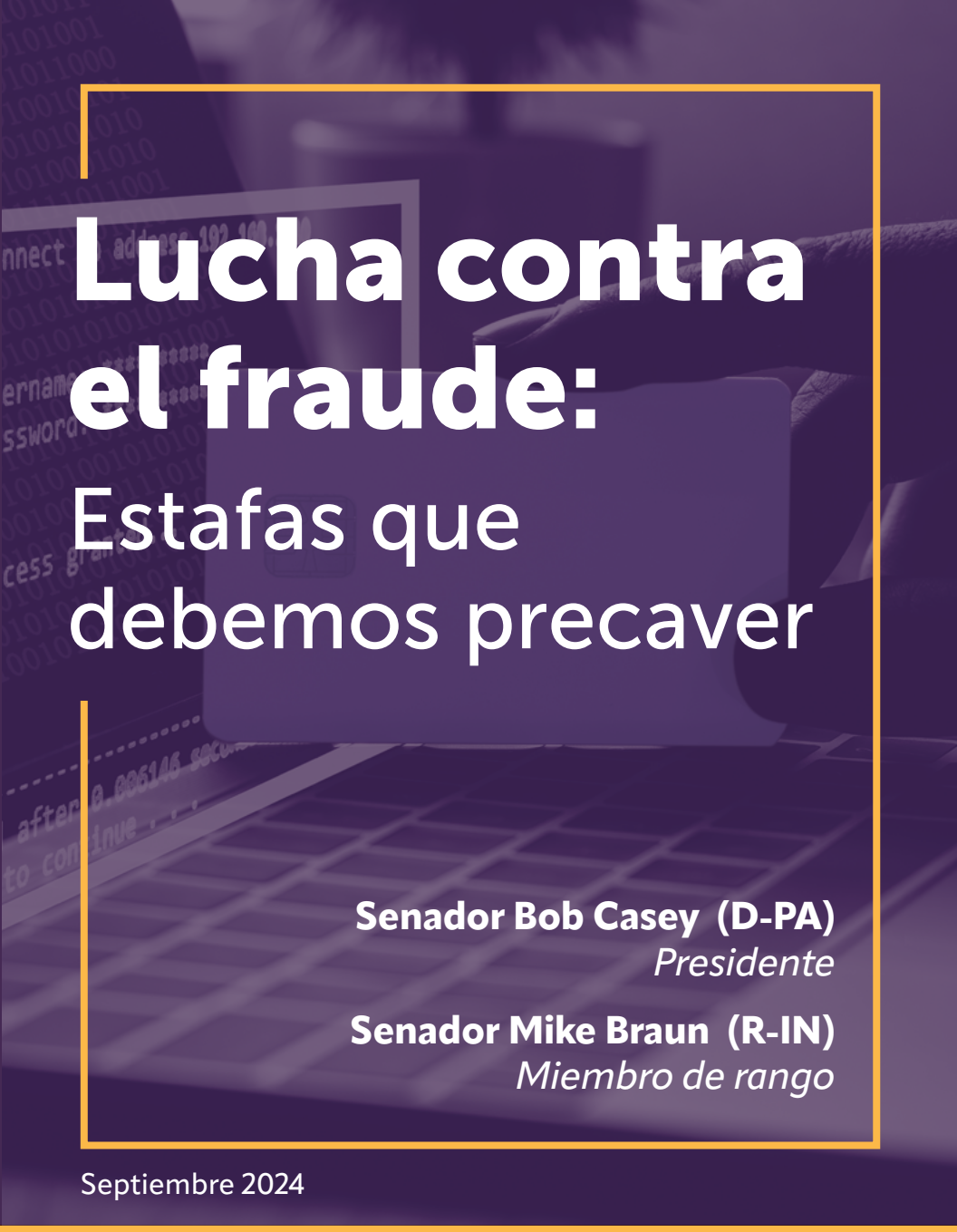


Lucha contra el fraude:

Estafas que debemos precaver

Senador Bob Casey (D-PA)
Presidente

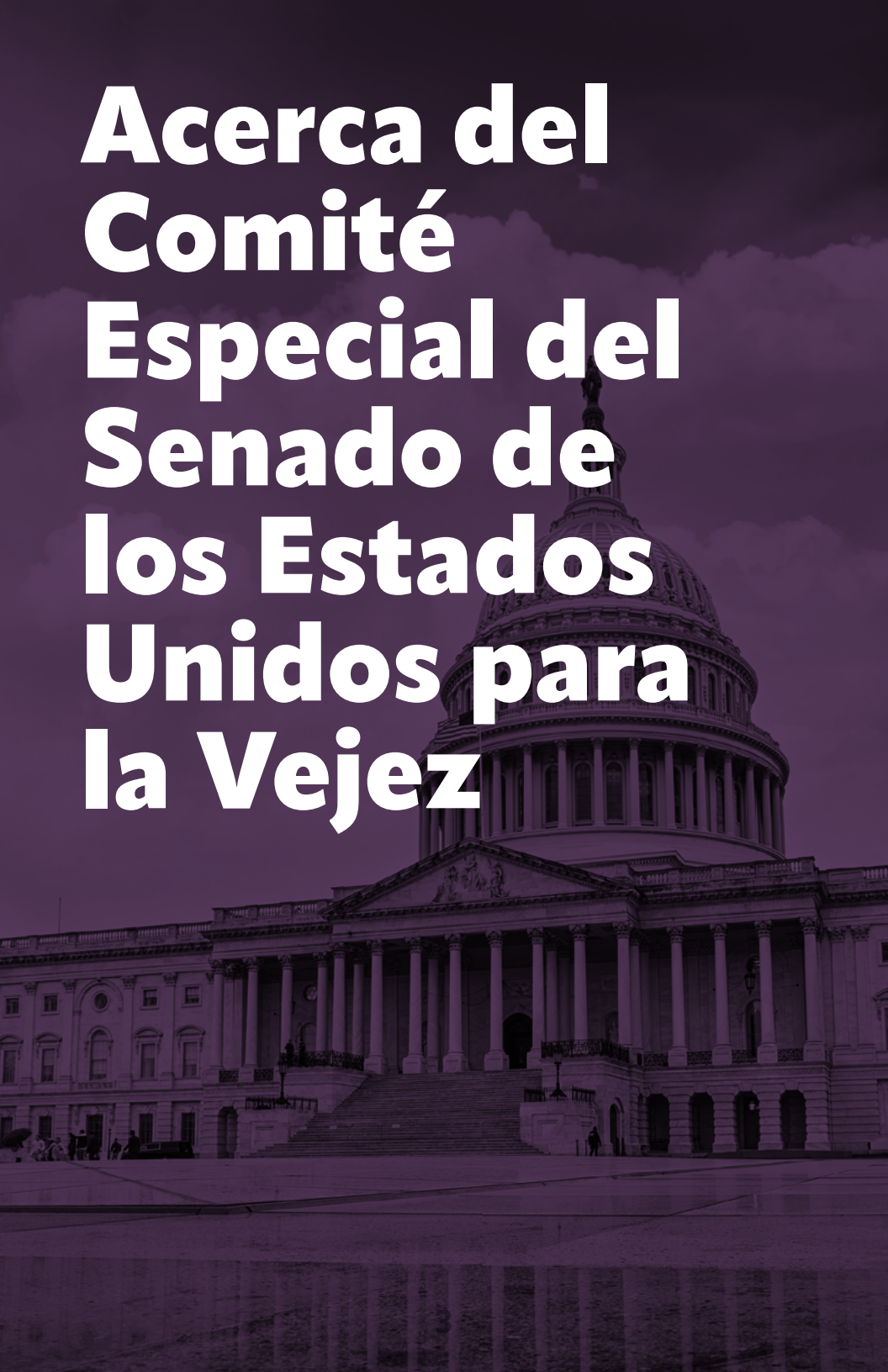
Senador Mike Braun (R-IN)
Miembro de rango

Septiembre 2024

Comité Especial del Senado de los Estados Unidos para la Vejez

TABLA DE CONTENIDO

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 la 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.

BOB CASEY, 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

Más información sobre nuestros miembros y su trabajo en 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.

El Comité mantiene una línea directa gratuita contra el fraude donde el personal del Comité proporciona a las personas que llaman recursos y orientación para ayudar a las personas que llaman a denunciar incidentes de fraude a los funcionarios adecuados, como las fuerzas del orden locales y las agencias federales como la Comisión Federal de Comercio (FTC), el Departamento de Justicia (DOJ) y la Oficina Federal de Investigaciones (FBI), entre otras.

Si usted o un ser querido necesita ayuda para conectarse a los recursos o desea denunciar actividades sospechosas que cree pueden ser fraudulentas, **comuníquese con la Línea directa gratuita contra fraude del Comité al 1-855-303-9470**. El personal del Comité está disponible de lunes a viernes, de 9 a.m. a 5 p.m., Hora del Este.

En 2023, muchas de las estafas denunciadas tanto a la Línea directa contra el fraude del Comité como a la FTC fueron similares a las denunciadas el año anterior: las estafas de impostores, sorteos y loterías fueron mencionadas como algunas de las principales categorías denunciadas en ambos años. Las estafas relacionadas

con la tecnología, incluidas las criptomonedas, la inteligencia artificial (IA) y las redes sociales, siguen desempeñando un papel importante. En 2023, los métodos de pago utilizados por los estafadores en los que los consumidores perdieron más dinero fueron las transferencias bancarias y las criptomonedas.[1]

Si bien los tipos de estafas se mantienen relativamente iguales año tras año, las pérdidas van en aumento. La FTC informa que en 2023, las pérdidas superaron los $10 mil millones, $1 mil millones más que las reportadas en 2022, y las pérdidas más cuantiosas que se hayan reportado a la FTC.[2]

El Comité continúa su trabajo para educar y crear conciencia sobre las estafas dirigidas a los adultos mayores, en particular las que están en aumento. En noviembre de 2023, el Comité celebró una audiencia titulada *Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back*.[3] Esta audiencia se enfocó en la amenaza que representan las estafas impulsadas por IA y las formas en que esta tecnología podría usarse para combatir el fraude. Un testigo, Gary Schildhorn, abogado de Filadelfia, contó su historia de cómo estuvo a punto de ser estafado por 9.000 dólares a través de un esquema de clonación de voz generado por IA. Puede leer más detalle sobre la historia de Gary en la página 25.

El Comité desea agradecer a las numerosas organizaciones de defensa del consumidor, centros comunitarios y funcionarios locales encargados del cumplimiento de la ley, que brindan una asistencia

invaluable a los estadounidenses en estos temas. Esperamos que esta guía pueda usarse como un recurso para ayudar a los adultos mayores y a otras personas a hacerles frente a las estafas más frecuentes de las que son víctimas los estadounidenses en la actualidad.

Sinceramente,

Bob Casey
Presidente

Mike Braun
Miembro de Rango

Explotación financiera

Cada año, millones de estadounidenses mayores son explotados financieramente por personas conocidas y desconocidas. Según la Asociación Nacional de Servicios de Protección para Adultos (NAPSA, por sus siglas en inglés), la explotación financiera de los adultos mayores es el uso indebido, el mal manejo o la explotación de la propiedad, las posesiones o los activos de los adultos mayores. Esto ocurre a menudo sin el consentimiento del adulto mayor, bajo falsos pretextos o mediante influencia, coerción o manipulación indebidas.[4] Los perpetradores de dicha explotación financiera de los adultos mayores van desde familiares y otras personas de confianza, hasta timadores y estafadores profesionales.

Un análisis reciente de la Red de Ejecución de Delitos Financieros (FinCEN) del Departamento del Tesoro de los Estados Unidos reveló que entre junio de 2022 y junio de 2023, se detectaron más de 155.400 declaraciones bancarias, por un valor total de $27 mil millones, donde se sospechaba de explotación financiera de adultos mayores.[5]

Si bien las personas de todas las edades pueden ser víctimas de explotación financiera, los adultos mayores son atacados con frecuencia, pues resulta más probable que hayan acumulado riquezas durante décadas de trabajo y ahorro. Mediante la práctica de este tipo de explotación financiera, a muchos adultos mayores les sustraen sus ahorros para la jubilación, o los fondos ahorrados para futuros gastos médicos y de cuidados. La explotación financiera de los adultos mayores también puede provocar un deterioro de la salud mental y física.[6]

La explotación financiera, que es una forma de abuso de adultos mayores, es más común entre quienes están socialmente aislados, confrontan dificultades para acceder a los servicios, o experimentan deterioro cognitivo. Un delito que no se denuncia con frecuencia debido al miedo, la vergüenza o la falta de recursos.[7]

LA EXPLOTACIÓN FINANCIERA DE LAS ADULTOS MAYORES SE DIVIDE GENERALMENTE EN DOS CATEGORÍAS: ROBO Y ESTAFAS

Robo

El robo ocurre cuando alguien sustrae bienes, fondos o ingresos de un adulto mayor. El perpetrador suele ser una persona conocida y de confianza como un familiar, un cuidador, un amigo, un profesional financiero o un socio comercial.

Entre los ejemplos de robo están la falsificación de cheques, el cambio de nombres en cuentas bancarias o el uso de tarjetas de crédito sin autorización.

Estafas

Las estafas consisten en la transferencia de dinero a un desconocido o impostor a cambio de un beneficio prometido que la víctima nunca recibe. Los perpetradores de estas estafas son principalmente extraños, radicados con frecuencia en un estado o país diferente al de sus víctimas.

Algunos ejemplos de estafas son las de soporte técnico, las de abuelos o personas necesitadas, y las de impostores gubernamentales, que se explican más adelante en esta guía.

LA EXPLOTACIÓN FINANCIERA DE LOS ADULTOS MAYORES TAMBIÉN PUEDE PRESENTARSE EN OTRAS VARIANTES COMO:

- Coacción o engaño a un adulto mayor para que firme un contrato, testamento u otro documento.
- Uso indebido de una conservaduría, tutela o poder notarial.

Pasos para protegerse:

- Planifique con anticipación para proteger sus activos y asegurarse de que se cumplan sus deseos.
- Triture todo documento que tenga su información personal, como recibos, estados de cuenta bancarios, correspondencia e incluso ofertas de tarjetas de crédito no utilizadas antes de tirarlos a la basura.
- Guarde bajo llave información financiera importante y confidencial cuando haya otras personas en su casa.
- No permita que otras personas tengan acceso a su información financiera.
- Verifique a las personas que va a contratar revisando referencias y credenciales.
- Revise regularmente su informe de crédito.
- Nunca revele información personal por teléfono, a menos que usted haya iniciado la llamada y sepa

que la comunicación es legítima. Esta información incluye su número de Seguro Social, número de cuenta bancaria u otra información confidencial.

- No se apresure a tomar una decisión financiera. Considere una segunda opinión y solicite información adicional por escrito.
- Consulte con un profesional confiable, como su asesor financiero o abogado, antes de firmar algún documento que no entiende.
- **Confíe en su instinto:** si algo le parece raro, probablemente lo es.

Denuncia de explotación financiera de adultos mayores

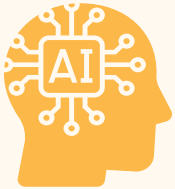
- Si usted, o alguien que conoce, corre un riesgo inmediato, llame al **9-1-1.**
- Denuncie el incidente a su banco y a la policía local.
- Reporte el incidente a los Servicios de Protección para Adultos (APS). Use la lista de NAPSA para encontrar el número de teléfono del APS en su localidad en **www.napsa-now.org/aps-program-list/** o llame al **2-1-1.**
- Presente una denuncia ante la FTC en **reportfraud.ftc.gov** o ante el FBI en **ic3.gov.**
- Repórtelo a la Línea directa contra el fraude de adultos mayores del DOJ al **833-FRAUD-11** (833-372-8311).

- Si el abuso ocurre en un centro de atención a largo plazo, como un hogar de adultos mayores o un centro de vida asistida, APS y los defensores de personas en centros de atención a largo plazo puede ayudar. Estos funcionarios son defensores de los consumidores que garantizan los derechos y la dignidad de los residentes en centros de cuidados a largo plazo.
- Utilice el mapa interactivo del Centro Nacional de Recursos del Defensor de personas en centros de cuidados a largo plazo de Consumer Voice para encontrar un programa en su localidad: **theconsumervoice.org/get_help**.

Cómo los estafadores roban dinero ajeno

Para robarles a sus víctimas, los estafadores utilizan tecnología que les permite llegar a miles de personas de manera fácil y económica, así como métodos de pago y monedas que les ayudan a acceder al dinero rápidamente y no dejar rastro.

ENFOQUE EN LA TECNOLOGÍA: INTELIGENCIA ARTIFICIAL



La Inteligencia Artificial (IA) es una tecnología que permite a las computadoras imitar cierto comportamiento similar al humano, 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 usar para hacer el bien, estas poderosas herramientas también pueden ser explotadas por delincuentes para hacer que las estafas sean más sofisticadas y convincentes. En esta sección se describe la tecnología de IA, cómo se puede utilizar en el fraude y en las estafas, y qué señales de advertencia debe tener en cuenta.

¿Cómo se utiliza la IA?

***Chatbots*:** Un *chatbot* es un programa informático que puede utilizar la IA para simular una conversación humana y podría utilizarse de forma maliciosa para obtener, almacenar o manipular sus datos personales.

Tecnología de clonación de voz: La clonación de voz utiliza la IA para crear modelos que aparentan la voz real de alguien conocido.

***Deepfakes*:** Un *deepfake* (ultrafalso) es un vídeo o una imagen generada por la IA que se hace para que parezca auténtica.

LA IA ACELERA LA EFICACIA DE LAS ESTAFAS PREEXISTENTES

Estas son las principales estafas basadas en IA a las que hay que prestar atención:

Ataques de phishing generados por IA: Los ataques de *phishing*, donde los estafadores engañan a sus víctimas para que revelen información confidencial, se han vuelto cada vez más sofisticados con el uso de la IA. Auxiliados por esta tecnología, los estafadores pueden personalizar rápidamente los mensajes de correos electrónicos de *phishing*, imitar diálogos sofisticados y eludir los filtros de correo basura (*spam*) tradicionales, lo que dificulta a las víctimas la distinción entre comunicaciones genuinas y fraudulentas.

Estafas de emergencia familiar: En estas estafas, los delincuentes convencen a las víctimas de que su familiar está en apuros para obtener dinero en efectivo o información privada. 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.

Estafas "románticas": Los estafadores emplean la IA para crear y operar perfiles falsos en sitios web de citas y plataformas de redes sociales. Luego, los *chatbots* generados por IA simulan una conversación realista para infundir confianza, con el objetivo de engañar a la víctima para que les envíe dinero.

Determinar si alguien está utilizando la tecnología de IA en una estafa no es fácil. **Pero lo cierto es: la IA hace que los fraudes y estafas tradicionales sean más convincentes y fáciles de implementar a mayor escala.**

Consejos para protegerse:

No revele información confidencial por teléfono, correo electrónico, mensaje de texto o redes sociales.

No transfiera ni envíe dinero a lugares desconocidos.

Considere designar una "palabra de seguridad" para uso de la familia, que solo se comparta con familiares y los contactos cercanos.

No proporcione ninguna información personal o confidencial a un *chatbot*.

Denuncie las posibles estafas a las autoridades y a las empresas involucradas.

ENFOQUE EN LOS MÉTODOS DE PAGO: CRIPTOMONEDAS, PAGOS PEER-TO-PEER (P2P) Y TARJETAS DE REGALO

Criptomonedas: La criptomoneda es un tipo de moneda digital que solo existe electrónicamente. Como las transacciones de criptomonedas no tienen que contar necesariamente con la supervisión una tercera persona de confianza, y son seudónimas y difíciles de rastrear, este método de pago podría ser un mecanismo útil para los estafadores. También es el preferido por los delincuentes porque obtienen el dinero al instante y los pagos no suelen ser reversibles.

Los pagos con criptomonedas se pueden utilizar en una gran variedad de operaciones fraudulentas, incluidas las estafas de inversión falsa y las de falsa amistad o "románticas." Estas estafas también se pueden producir unidas: las estafas de inversión en criptomonedas pueden comenzar con delincuentes que inicialmente "enganchan" a las víctimas por medio de una falsa amistad o romance, y luego progresar a solicitudes de dinero para una supuesta inversión.

Una técnica común que utilizan los estafadores es crear una relación con sus víctimas a lo largo del tiempo, ganándose su confianza para luego convencerlas de que inviertan en una operación fraudulenta, lo que resulta en pérdidas financieras significativas. Este proceder, conocido como "estafa de inversión de confianza", se analiza más adelante en esta guía. Una vez que el estafador se ha ganado la

confianza de la víctima, la presiona para que "invierta" en una plataforma de criptomoneda específica prometiendo altos rendimientos, y utilizando tácticas sofisticadas para crear un sentido de legitimidad. En realidad, la plataforma es falsa y está controlada por los estafadores, que desaparecen con los fondos "invertidos" una vez que han acumulado suficiente dinero de inversores desprevenidos.

La Oficina Federal de Investigaciones (FBI) reveló que los adultos mayores de 60 años perdieron casi $1.7 mil millones por estafas relacionadas con criptomonedas en 2023, un aumento reportado de casi el 52 por ciento con respecto a 2022.[8] El FBI también descubrió que las principales pérdidas relacionadas con las criptomonedas en los adultos mayores fueron estafas de inversión relacionadas con criptomonedas, con más de $716 millones en pérdidas reportadas.[9]

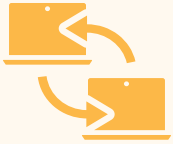
Consejos para protegerse:

- Ignore las sugerencias y ofertas para ayudarle a invertir en criptomonedas: lo más probable es que se trate de una estafa.
- Si conoce a alguien en un sitio o aplicación de citas, y quiere que le envíe criptomonedas o le muestre cómo invertir en criptomonedas, es casi seguro que se trata de una estafa.
- Ignore las afirmaciones de retorno de la inversión (ROI) que parecen demasiado buenas para ser verídicas.

- No se relacione con “gestores de inversiones” que se pongan en contacto con usted y le hagan promesas sobre un retorno de la inversión.
- Ninguna celebridad se pondrá en contacto directamente con nadie para vender criptomonedas. No responda a ningún mensaje que pretenda ser de una personalidad famosa.
- No acepte criptomonedas “gratuitas” que le ofrezcan desconocidos.
- Si ha sido víctima de una estafa con criptomonedas, desconfíe de cualquier persona que afirme que puede recuperar sus fondos, ya que podría tratarse de otra estafa recurrente. Con mucha frecuencia, los estafadores se dirigen a la misma persona más de una vez porque la consideran vulnerable, confiada y potencialmente menos propensa a denunciar el fraude o buscar recursos jurídicos después de la victimización inicial.
- **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 mismas, la FTC tiene información útil en **consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams**.

El FBI también ha publicado una guía para las víctimas de estafas de criptomonedas, que se puede encontrar aquí: **www.ic3.gov/Media/Y2023/PSA230824**.



Pagos peer-to-peer (P2P): Los pagos P2P (red entre pares) son transacciones entre dos partes con cuentas bancarias separadas, mediadas a través de un sitio web o aplicación móvil de terceros. Los estafadores pueden utilizar estas plataformas porque, al igual que las criptomonedas, reciben el dinero instantáneamente después de que se inicia una transferencia. Si bien muchas empresas de pagos P2P emplean sistemas avanzados para detectar e interrumpir transacciones sospechosas, a menudo no pueden revertir una transacción una vez que se envía el dinero. Estas aplicaciones también pueden carecer de las mismas protecciones contra el fraude que emplean los bancos tradicionales y las tarjetas de crédito.

En 2023, la FTC recibió más de 65.300 denuncias de consumidores que enviaron dinero a estafadores a través de aplicaciones de pago P2P como CashApp, Venmo o Zelle, con pérdidas declaradas por un total de casi $210 millones.[10] Estos reportes representan un aumento del 5 por ciento con respecto al año anterior, pero las pérdidas informadas son un 28 por ciento más altas que en 2022.[11]

Consejos para protegerse:

- Nunca envíe pagos a alguien que no conozca. Tómese su tiempo para asegurarse de que está enviando dinero a la persona adecuada.
- Configure alertas de fraude en su aplicación de pago P2P o con la cuenta bancaria o de tarjeta

de crédito que haya vinculado a la aplicación. Las alertas de fraude pueden informarle si se cambia la información personal o cuándo se realizan transacciones.

- Las aplicaciones de pago P2P tienen elementos de redes sociales, como "listas de amigos". Evite compartir información como su dirección, número de teléfono y otros datos personales. Al igual que en las redes sociales, ignore las solicitudes de "amistad" de personas que no conoce.
- Debe evitarse cualquier negocio que acepte exclusivamente aplicaciones de pago P2P o pagos con tarjeta de débito prepagada.
- Al igual que 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 siguen siendo los métodos principales utilizados por los estafadores, para solicitar y sustraer dinero a adultos mayores que denunciaron estafas a la Línea directa contra el fraude del Comité. Cuando la víctima envía al estafador el número de la tarjeta de regalo, el delincuente utiliza inmediatamente el saldo, lo que hace imposible recuperar el dinero.

En 2023, la FTC recibió más de 41.600 denuncias de estafas con tarjetas de regalo, lo que resultó en casi $217 millones por concepto de pérdidas reportadas.[12]

Consejos para protegerse:

- Si le pagó a un estafador con una tarjeta de regalo, infórmelo de inmediato a la compañía que emitió la tarjeta.
- Si compra tarjetas de regalo para regalar o donar a familiares y amigos, hágalo en tiendas conocidas y confiables. Revise las pegatinas protectoras de la tarjeta para asegurarse de que no hayan sido manipuladas.
- Guarde siempre su recibo y una copia de la tarjeta de regalo. El número de la tarjeta de regalo y el recibo de la tienda le ayudarán a presentar una denuncia si pierde la tarjeta o necesita denunciar una estafa.
- Tenga cuidado con las señales de estafas como las solicitudes para comprar tarjetas de regalo en varias tiendas, o un tipo específico de tarjeta de regalo.

- **Tenga en cuenta**: Ninguna empresa o agencia gubernamental le dirá que compre una tarjeta de regalo para pagar. Esto siempre es una estafa.

Para obtener más información sobre las estafas con tarjetas de regalo y cómo protegerse, visite la FTC en **consumer.ftc.gov/articles/avoiding-and-reporting-gift-card-scams**.

Estafas a las que debe prestar atención

En 2023, la Línea directa contra el fraude del Comité recibió 536 nuevas quejas de personas de todo el país. Estas quejas elevan a casi 12.300 la cifra total de denuncias registradas en la Línea directa contra el fraude desde 2013.

Muchos de estos fraudes también se denuncian a la FTC. Mediante la recopilación de informes, investigaciones y otras acciones administrativas, la Oficina de Protección al Consumidor de la FTC combate las prácticas injustas, engañosas y fraudulentas empleadas tanto por empresas como por estafadores individuales.

Los fraudes denunciados representan casi 2.6 millones de los 5.4 millones de quejas presentadas a la FTC en 2023.[13] Entre las categorías de fraude más comunes están las estafas de impostores, compras en línea y críticas negativas, estafas de premios y lotería, y fraude relacionado con inversiones. Otras estafas menos comunes, pero aún frecuentes, son las de cobro de deudas, estafas hipotecarias y de falsa reparación de viviendas.[14]

ESTAFAS DE IMPOSTORES

Las estafas de impostores son las más generalizadas de todas las denunciadas a la FTC, con más de 850.000 en 2023.[15] Estas estafas pueden manifestarse de muchas formas diferentes en la medida que los estafadores encuentran nuevas formas de atacar a las víctimas. En las cinco secciones siguientes se analizan algunas de las estafas de impostores más frecuentes que se usan comúnmente contra los adultos mayores.

SCAM SURVIVOR

Gary Schildhorn

Víctima de estafa a persona necesitada

FILADELFIA, PENSILVANIA

En febrero de 2020, me dirigía a la oficina cuando sonó mi teléfono. Era mi hijo, Brett. Estaba molesto y lloraba. Me dijo que necesitaba mi ayuda porque tuvo un accidente automovilístico y fue arrestado. Dijo que [él] podría tener la nariz rota y que se había lastimado el brazo. El automóvil contra el que chocó era conducido supuestamente por una embarazada que resultó herida. Me informó además que se le asignó un defensor público llamado Barry Goldstein... Le respondí que me pondría en contacto con Goldstein y le devolvería la llamada, pero me dijo: 'No puedes, me quitaron el teléfono, sácame de aquí, por favor'.

Soy padre y abogado. Mi hijo estaba lesionado, confrontaba problemas y una embarazada resultó herida. Esta llamada instigó y requería una acción inmediata de mi parte. Primero intenté buscar al señor Goldstein. Antes de que llegaran los resultados de la búsqueda, sonó mi teléfono. Era el señor Goldstein. Me dijo que se había reunido con mi hijo, que estaba herido, pero que todo iba a salir bien.

Añadió que el juez había ordenado una fianza considerable de $150.000 y que necesitaría el 10 por ciento de esa cantidad en efectivo para sacarlo... Luego me preguntó si estaba en condiciones de ayudar a mi hijo. Le aseguré que sí. Él entonces... me dijo que llamara al tribunal y arreglara la fianza ... Llamé al número que me proporcionó. Respondieron: 'Juzgado del Condado de Montgomery'... [y] confirmaron que tenían detenido a mi hijo... [Ellos] también informaron que... el juez ... había rebajado la fianza a $90.000.

Los del [Juzgado del Condado de Montgomery] me dijeron entonces que para pagar la fianza [de mi hijo] tendría que recurrir al fiador del condado, pero que había un problema: el único disponible tenía una emergencia familiar y no estaba en la ciudad... [Ellos] sugirieron que llamara al Sr. Goldstein porque él podría ayudar. Hice la llamada.

El Sr. Goldstein accedió a pagar la fianza y me informó que tendría que transferirle $9.000. Dijo que era miembro de una cooperativa de ahorro y crédito y que tendría que ir a ciertos quioscos para transferir el dinero. Más tarde me enteré de que se trataba de

quioscos de bitcoin [un tipo de criptomoneda]. Luego me dijo que como iba a asistir a una conferencia fuera de la ciudad y que se iría al aeropuerto en dos horas, por lo que tenía que apurarme.

Esta serie de llamadas se produjeron en pocos minutos. No fue hasta que cesaron y me dirigía al banco que tuve oportunidad de pensar. Llamé a mi nuera, Kim, le conté lo que había pasado y le pedí que avisara a la oficina de mi hijo de que había tenido un accidente.

Unos minutos después, recibí una llamada por Facetime. Era Brett. 'Papá, Kim llamó al trabajo y me pusieron al teléfono'. 'Te están estafando; mira, estoy bien'. Conmoción, alivio y rabia: una emoción seguía a la otra. Le dije a Brett que no me cabía duda de que era su voz en el teléfono, era la cadencia exacta con la que habla... **¿Cómo consiguieron la voz de mi hijo? La única conclusión que puedo sacar es que utilizaron inteligencia artificial, o IA, para clonar su voz.**

Extractos tomados del testimonio del Sr. Schildhorn proporcionado al Comité para la Vejez en noviembre de 2023.

Estafas a "personas necesitadas" y "abuelos"

Como testificó Gary en noviembre de 2023, los timadores pueden hacerse pasar por familiares o amigos en estafas a "personas necesitadas" o "abuelos." Los impostores pueden hacerse pasar por un nieto o un agente de la policía que ha detenido al nieto de la víctima. También pueden usar la IA para clonar la voz de alguien que la víctima conoce, quien afirma que está en problemas y necesita dinero para hacerle frente a una emergencia como salir de la cárcel, pagar una factura del hospital o salir de un país extranjero. Los estafadores juegan con las emociones y engañan a los familiares preocupados para que les envíen dinero. Otras estafas similares pueden usar las voces de sobrinas, sobrinos, hijos u otras personas. Entre enero y septiembre de 2023, el IC3 del FBI recibió más de 195 informes sobre estafas de abuelos, lo que resultó al menos en $1.9 millones en pérdidas reportadas.[16]

SEÑALES DE ALERTA

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

- La persona que llama le pide que envíe dinero de inmediato y le ofrece detalles específicos sobre cómo hacerlo. Puede sugerirle que envíe el dinero a través de una tarjeta de regalo, una transferencia bancaria o una criptomoneda.
- 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 informa que se encuentra en una situación o lugar que no se corresponde con el comportamiento típico de la persona que dice ser.

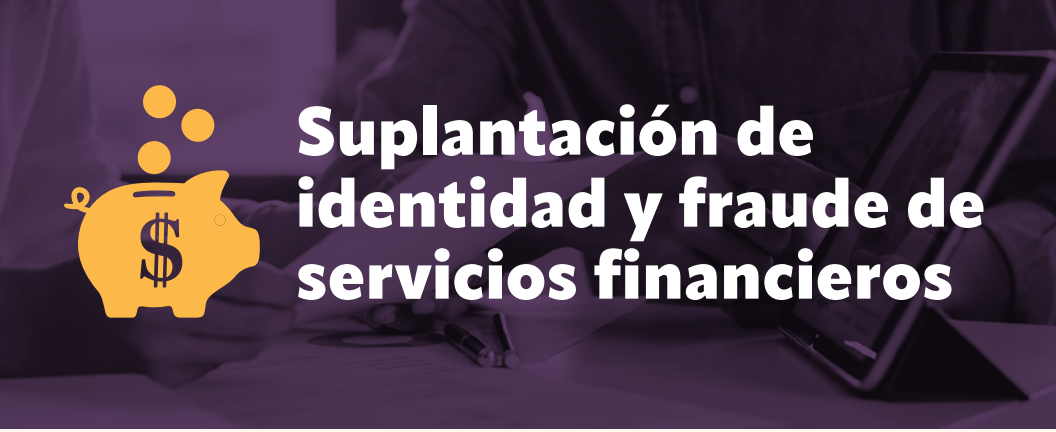
PASOS PARA PREVENIR Y RESPONDER

- Cuelgue y llame al número de su familiar o de un amigo genuino para asegurarse de que está a salvo.
- Si la persona dice ser un oficial de la policía, cuelgue y llame a la agencia de orden público correspondiente para verificar su identidad y cualquier información compartida. **Tenga en cuenta:** la policía nunca se pondrá en contacto con un miembro de la familia para cobrar el dinero de una fianza en representación de otra persona.
- Verifique la historia con familiares y amigos de confianza, incluso si le han dicho que la mantenga en secreto.

- Verifique la configuración de privacidad de sus redes sociales y limite la información que comparte en línea. Los delincuentes pueden utilizar los datos personales para orientar mejor su estafa y hacerla aún más convincente.
- 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 **reportfraud.ftc.gov**.
- **Consejo útil:** Si envió dinero a un estafador a través de una transferencia bancaria, repórtelo al IC3 del FBI dentro de las 72 horas posteriores a la transferencia en **ic3.gov**. Es posible que puedan ayudarlo a recuperar parte de sus fondos perdidos.

MÁS INFORMACIÓN

- Para hacer frente a estas llamadas, la FTC tiene consejos útiles en **www.consumer.ftc.gov/articles/0204-family-emergency-scams**.
- La FCC proporciona más información sobre cómo evitar estas estafas en **www.fcc.gov/grandparent-scams-get-more-sophisticated**.
- El FBI publicó un anuncio de servicio público sobre estas estafas, que se puede ver en **www.ic3.gov/Media/Y2023/PSA231117**.
- Para obtener más información sobre cómo se usa la IA en este tipo de estafas, la FTC tiene información útil en **consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes**.



Suplantación de identidad y fraude de servicios financieros

Los estafadores pueden hacerse pasar por funcionarios de empresas de servicios financieros como bancos, cobradores de deudas o administradores hipotecarios. Por ejemplo, los estafadores pueden hacerse pasar por cobradores e intentar engañar a sus víctimas para que paguen deudas que no existen. También pueden acosar o amenazar con penalidades o cárcel si se niegan a pagar. Por su parte, las estafas de alivio hipotecario consisten en promesas relacionadas con el refinanciamiento, y mentiras sobre los términos de un préstamo.

Según la FTC, en 2023 se reportaron más de 124.400 casos de fraude de cobro de deudas y casi 26.200 casos de fraude hipotecario.[17] En 2022, las advertencias falsas de fraude bancario fueron la estafa por mensaje de texto más denunciada,[18] con una pérdida promedio declarada de $3.000.[19]

Informes de la Línea directa contra el fraude

Una residente de la Florida informó que recibió la llamada de un estafador que se hacía pasar por su banco. Como el estafador había falsificado el identificador de llamadas de la víctima, parecía que Bank of America se estaba comunicando con ella. Luego, el estafador le indicó a la víctima que enviara $950 por Zelle y CashApp.

CUIDADO: ESTAFAS DE *PHISHING*

Las estafas de *phishing* engañan a las víctimas para que revelen información confidencial haciéndose pasar por organizaciones o empresas legítimas. Los estafadores utilizan mensajes de correo electrónico, de texto o sitios web falsos que imitan a los verdaderos, instando a una acción rápida a través de enlaces o archivos adjuntos. Los datos obtenidos a través del *phishing* se utilizan a menudo para el robo de identidad o el fraude financiero. Para protegerse, verifique la autenticidad de los mensajes inesperados, evite presionar sobre enlaces sospechosos y use contraseñas seguras y únicas.

SEÑALES DE ALERTA

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

Fraude de suplantación de identidad bancaria

- Usted recibe un mensaje de texto, una llamada telefónica o un mensaje de correo electrónico indicando que la información de su cuenta se ha visto comprometida. Es posible que le soliciten 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 revele información personal confidencial por teléfono, mensaje de texto o de correo electrónico. Tampoco le pedirán que transfiera dinero a nadie, incluido usted mismo, ni que proporcione información personal para obtener un reembolso o emitir una corrección.

Fraude de cobro de deudas

- La persona que llama dice que usted irá a la cárcel si no paga la deuda que describe. Es ilegal que los cobradores amenacen con arrestar a alguien por no pagar sus deudas.
- La persona que llama no le dirá a quién le debe dinero. Los cobradores legítimos siempre le dirán

quién es el acreedor, incluso si usted no se lo pregunta.

- Los cobradores legítimos brindan suficiente tiempo para pagar su deuda y colaborarán con usted. Los estafadores lo presionarán para que pague mientras usted está al teléfono.

Fraude de alivio hipotecario

- La persona que llama y le presenta la oportunidad de una hipoteca no ha sido referida a usted por amigos ni 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 le piden 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 para ocultar su identidad o permitirles hacerse pasar por una persona o empresa.

- No haga clic en enlaces inesperados ni responda a mensajes de texto que no conoce.
- Si recibe una llamada, mensaje de texto o de correo electrónico sospechoso, cuelgue y no responda al mensaje de texto o de correo electrónico. Llame a su banco o institución financiera directamente utilizando información de contacto verificada, como el número de teléfono en el sitio web del banco o al reverso de su tarjeta bancaria.

Fraude de cobro de deudas

- Pida una carta de validación de deuda por escrito. Los cobradores 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

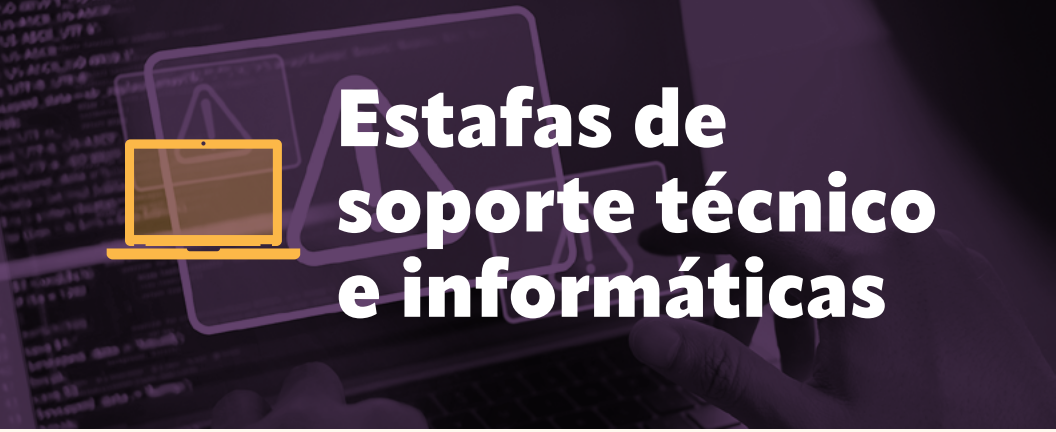
- Antes de firmar cualquier documento, consulte con un abogado para asegurarse de que se trata de una hipoteca legítima. Si la persona que intenta que usted firme se opone agresivamente a que consulte a un abogado, podría ser un estafador.

- Asegúrese de leer detenidamente todos los documentos antes de firmar. Si tiene preguntas, pídale explicación a la persona que intenta que usted firme. Si ignora sus preocupaciones, podría 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 **reportfraud.ftc.gov**.

MÁS INFORMACIÓN

- La Asociación Estadounidense de Banqueros (ABA) tiene más información sobre las estafas de suplantación de identidad bancaria en **www.banksneveraskthat.com**.
- La FTC proporciona más información sobre préstamos y estafas relacionadas con deudas en **consumer.ftc.gov/credit-loans-debt**.
- La Oficina del Contralor de la Moneda (OCC, por sus siglas en inglés) tiene más información sobre estafas en **www.occ.treas.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/index-fraud-resources.html**.



Estafas de soporte técnico e informáticas

Las estafas informáticas son obra de estafadores que fingen estar asociados con una empresa de tecnología conocida como Microsoft, Apple, Dell o Geek Squad de Best Buy. Pueden usar tácticas como afirmar falsamente que su computadora ha sido infectada con un virus, o solicitar que se les proporcione información personal y/o acceso remoto a esa computadora. También pueden solicitar el número de su tarjeta de crédito o cuenta bancaria para "facturar" sus servicios.

En una estafa similar, la víctima puede ver una ventana emergente en la pantalla de su computadora que advierte sobre una violación de la seguridad, y le indica que llame al número de un agente de soporte técnico que es en realidad un estafador. El FBI informa que en 2023, al igual que en 2022, las estafas de soporte técnico fueron las que más afectaron a las víctimas adultas mayores. Según los informes, los adultos mayores perdieron casi $590 millones por estafas de soporte técnico en 2023.[20]

Informes de la Línea directa contra el fraude

Una residente de Georgia llamó a la Línea directa contra el fraude del Comité para informar que perdió $25.000 en una estafa de soporte técnico. La víctima informó que su computadora se había congelado y apareció una ventana emergente, lo que la llevó a llamar a lo que creyó que era el número de soporte técnico de Microsoft. Luego marcó el número para pedir ayuda y los estafadores pudieron robarle miles de dólares.

SEÑALES DE ALERTA

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

- Usted recibe una alerta de hay un virus en su teléfono o computadora y que debe llamar a un número específico para resolver el problema.
- El estafador asegura que la única solución para proteger su dinero o datos personales del "pirata cibernético" es transferirles los fondos de su cuenta mientras eliminan el supuesto virus.
- Si usted responde que preferiría solucionar el problema yendo a un establecimiento convencional o llamar a una empresa diferente, la persona que llama intenta convencerle de que la eliminación del virus es urgente y que solo ellos pueden ayudarle.

PASOS PARA PREVENIR Y RESPONDER

- Si recibe una alerta advirtiendo que su teléfono o computadora tiene un virus, no llame al número proporcionado. En su lugar, llame al número 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 comprometido por un virus, cuelgue y bloquee ese número de teléfono.
- Nunca proporcione información personal o financiera a una persona que llame sin previo aviso.
- No proporcione acceso remoto a un dispositivo o cuenta, a menos que usted se haya puesto primero en contacto con esa empresa y sepa que es legítima.
- 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 **reportfraud.ftc.gov**.

MÁS INFORMACIÓN

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

Estafas de impostores del gobierno

En las estafas de impostores del gobierno, los timadores se hacen pasar por representantes de una agencia federal como la Administración del Seguro Social (SSA) o el Servicio de Impuestos Internos (IRS). Pueden amenazar con la cancelación de beneficios, exigir el pago de "impuestos" o "tarifas", o alegar algún problema para robar su dinero o información personal. También pueden usar documentos o imágenes como un logotipo federal cuando se comunican con la víctima prevista, para hacer que su reclamo parezca legítimo. Entre los diferentes tipos de estafas de impostores gubernamentales, las relacionadas con el Seguro Social fueron las más comunes de este tipo reportadas tanto a la Línea directa contra el fraude del Comité como a la FTC en 2023. Según la FTC, las víctimas perdieron más de $126 millones debido a estafas de impostores del Seguro Social el año pasado.[21]

Informes de la Línea directa contra el fraude

Una persona que llamó desde Virginia Occidental informó que recibió una llamada de un estafador que decía ser empleado del gobierno federal. La víctima informó que el mismo le pidió que enviara $900 al estafador para saldar su deuda con el IRS.

SEÑALES DE ALERTA

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

- Usted recibe una llamada telefónica, un mensaje de texto o de correo electrónico pidiéndole que confirme información que la agencia gubernamental ya debería tener, como una dirección o un número de Seguro Social.
- La persona que se comunica con usted amenaza cancelar sus beneficios, le pide que transfiera dinero, que deposite dinero en una tarjeta de débito prepagada o una tarjeta de regalo, o que envíe efectivo o cheque utilizando un servicio de entrega al día siguiente. También puede pedirle que pague con criptomonedas o a través de una aplicación de pago P2P.
- Se le presiona para que decida rápida y urgentemente, a veces en un día o una semana.

PASOS PARA PREVENIR Y RESPONDER

- Cuelgue o no responda al mensaje de correo electrónico o de texto.
- Nunca dé ni confirme información financiera u otra información confidencial en respuesta a llamadas inesperadas, o si tiene alguna sospecha.
- No confíes inherentemente en un nombre o número. Los estafadores pueden usar nombres aparentemente oficiales para que confíe en ellos. Para hacer que su llamada parezca legítima, también pueden usar la tecnología para disfrazar su número de teléfono real.
- Una agencia gubernamental nunca le pedirá que transfiera dinero, proporcione su número de Seguro Social ni envíe fondos a través de una tarjeta de regalo.
- Llame directamente a 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.
- 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 **reportfraud.ftc.gov**.

MÁS INFORMACIÓN

- La FTC ofrece consejos sobre cómo detectar y evitar estafas de impostores en **consumer.ftc.gov/features/imposter-scams**.
- La SSA tiene más información sobre cómo protegerse de las estafas del Seguro Social en **www.ssa.gov/scam**.

Estafas “románticas”

Los estafadores “románticos” explotan el deseo de compañía y amor de una persona creando identidades falsas y formando conexiones emocionales en línea. Estos estafadores se hacen pasar a menudo por posibles parejas románticas, ganándose la confianza de las víctimas con el tiempo a través de la comunicación frecuente y las declaraciones de afecto. Una vez que se crea confianza, el estafador inventa generalmente una crisis o una necesidad urgente de dinero, como gastos médicos, costos de viaje o inversiones, persuadiendo a la víctima para que le envíe fondos. Las víctimas pueden ser manipuladas para mantener la relación en secreto o apresurarse a realizar transacciones financieras antes de verificar completamente la autenticidad de su supuesta pareja.

Las estafas “románticas” son muy comunes en los sitios web de citas, las plataformas de redes sociales, las aplicaciones de mensajería y los foros en línea. El sentido común y la precaución son cruciales para reconocer las señales de engaño y protegerse de daños emocionales y financiero. La FTC informa que más de 64.000 consumidores informaron que fueron víctimas de estafas “románticas” en 2023, con pérdidas reportadas por un total de más de $1.1 mil millones.[22]

Informes de la Línea directa contra el fraude

Una residente de Ohio llamó a la Línea directa contra el fraude para informar que, durante los últimos dos años, ha sido víctima de una estafa "romántica" en la que perdió $40.000.

SEÑALES DE ALERTA

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

- La persona nunca le hace videollamadas ni le conoce en persona.
- No tienen amistades en común con ellos en las redes sociales y su identidad es difícil de rastrear en línea.
- Afirman estar enamorados de usted antes de conocerse personalmente.
- Planean visitarle, pero siempre tienen una excusa de último minuto para explicar por qué no pueden hacerlo.
- Solicitan que el dinero se envíe a través de criptomonedas, transferencia bancaria, aplicación de pago P2P o tarjeta de regalo.

PASOS PARA PREVENIR Y RESPONDER

- Si la persona siempre se niega a hacer una videollamada o reunirse en persona, bloquéela.
- Nunca envíe dinero o regalos a alguien que no haya conocido en persona.
- Hable con tu familia y amigos, o con alguien en quien confíe, para que le aconseje.
- Comuníquese con su banco de inmediato si cree que envió dinero a 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 **reportfraud.ftc.gov**.

MÁS INFORMACIÓN

- El Servicio Secreto de los Estados Unidos brinda consejos sobre cómo evitar las estafas "románticas" en **www.secretservice.gov/investigation/romancescams**.
- La FTC proporciona información y recursos de presentación de informes en **www.consumer.ftc.gov/articles/what-know-about-romance-scams**.

Otras estafas comunes

Estafas de sorteos y loterías

Las estafas de sorteos y loterías explotan las esperanzas de ganar un gran premio en efectivo, engañando a las víctimas para hacerles creer que han ganado un concurso en el que nunca participaron. Los estafadores se comunican frecuentemente con las víctimas por mensaje de texto, teléfono, correo electrónico o correo postal, alegando que han ganado una suma sustancial, pero que deben pagar "impuestos" o "tarifas" por adelantado para reclamar el premio.

Estas operaciones fraudulentas manipulan la emoción y el deseo de obtener ganancias financieras, instando a las víctimas a proporcionar información personal o enviar dinero, para desaparecer una vez que se realiza el pago. El sentido común y la precaución son cruciales para evitar ser objeto de estas prácticas engañosas, ya que una vez enviado el dinero, generalmente es irrecuperable, dejando a las víctimas devastadas financiera y emocionalmente. En 2023, la FTC descubrió que las víctimas reportaron $338 millones en pérdidas por estafas relacionadas con premios, sorteos y loterías.[23]

Informes de la Línea directa contra el fraude

Una residente de Pensilvania informó que fue contactada por un estafador que le aseguró era ganadora en la lotería. El estafador le dijo que para reclamar el premio, tenía que pagar $800.

SEÑALES DE ALERTA

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

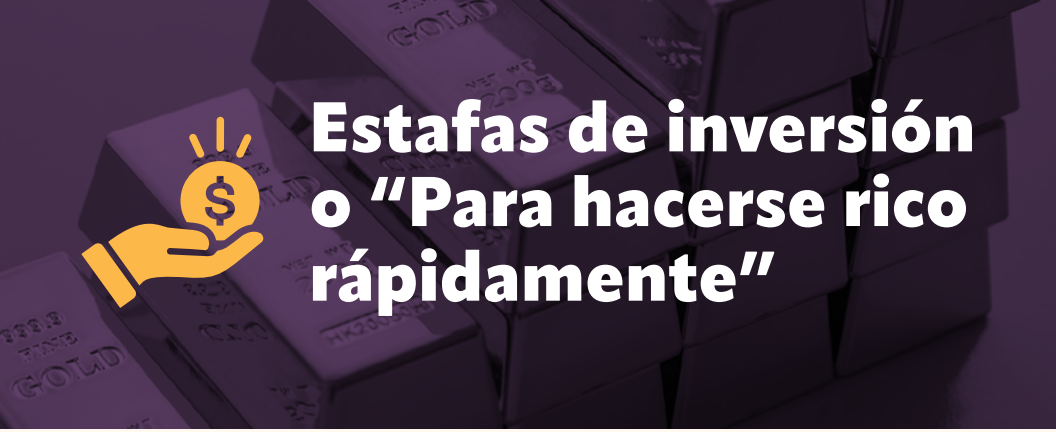
- Usted recibe una llamada o un mensaje diciendo que ha ganado un premio, pero para reclamar el premio debe pagar un "impuesto" o una "tarifa de procesamiento."
- La persona que dice que ha ganado un premio trata de convencerle de que sus familiares y amigos preocupados están celosos o equivocados.
- Se le pide que pague el "impuesto" o la "tarifa de procesamiento" mediante una transferencia o enviando dinero por correo o mediante tarjeta de regalo, aplicaciones de pago P2P o criptomonedas.
- Le dicen que 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 de alguien que le asegura que usted ha ganado un premio y menciona el abono de un "impuesto" o una "tarifa," anote el número, cuelgue y bloquéelo.
- No responda a cartas, mensajes de texto o de correo electrónico comunicándole que ha ganado un premio, especialmente si mencionan el pago de un "impuesto" o "tarifa" para reclamarlo.
- Denuncie cualquier llamada, mensaje o correo sospechoso a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en **reportfraud.ftc.gov**.

MÁS INFORMACIÓN

- Better Business Bureau ofrece consejos sobre cómo identificar y evitar estas estafas en **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 loterías en **consumer.ftc.gov/articles/fake-prize-sweepstakes-lottery-scams**.



Estafas de inversión o "Para hacerse rico rápidamente"

Con las estafas de inversión, los delincuentes se jactan de la posibilidad de obtener altos rendimientos con poco esfuerzo y poco riesgo por su parte, si invierte en una nueva oportunidad como criptomonedas, bienes raíces o metales preciosos. Estas estafas pueden originarse en las redes sociales, aplicaciones de citas en línea o por contacto no solicitado a través de un mensaje de texto, una llamada telefónica o un correo electrónico. A menudo comienzan con la creación de una relación entre el estafador y su víctima. Una vez que el estafador se gana la confianza de la víctima, la alentará a invertir, al tiempo que garantiza altos rendimientos sin riesgos.

Según el IC3 del FBI, en 2023 las estafas de inversión fueran las más costosas para los adultos mayores, con pérdidas reportadas que superaron los $1.2 mil millones.[24] Las pérdidas sufridas por los adultos mayores por estafas de inversión han aumentado en más del 400 por ciento desde 2021.[25]

Informes de la Línea directa contra el fraude

Una persona que llamó desde Pensilvania informó que cobró su 401K y depositó todos sus fondos en lo que pensó era una cuenta de ahorros de alto rendimiento. La víctima informó que el sitio web de la compañía de inversión falsa ha desaparecido desde entonces, y no ha podido extraer su dinero, quedándose sin fondos de jubilación.

CUIDADO: ESTAFAS PIRAMIDALES

Las estafas piramidales también son un tipo de estafa de inversión. Se presentan como oportunidades de empleo reales, pero funcionan con un modelo engañoso en el que los participantes son atraídos con la promesa de altos rendimientos por reclutar a otros, en lugar de vender productos o servicios genuinos. Con frecuencia, se requiere que los participantes inviertan por adelantado, con la certidumbre de que obtendrán ganancias sustanciales. Las estafas piramidales se basan en el reclutamiento continuo por parte de los participantes, invitando a amigos y conocidos a que se les unan. Si bien los primeros participantes pueden recibir pagos de las tarifas pagadas por los nuevos reclutados, este tipo de estafa es insostenible y colapsa inevitablemente, dejando a la mayoría de los participantes con pérdidas

financieras.

Su enfoque se basa en explotar el deseo de obtener una riqueza rápida, ofreciendo falsas esperanzas de éxito financiero sin oportunidades legítimas de ingresos. Las autoridades de todo el mundo clasifican las operaciones piramidales como fraudulentas y advierten contra la participación para evitar dificultades financieras y consecuencias de índole jurídica.

CUIDADO: ESTAFAS DE INVERSIÓN DE CONFIANZA

Las estafas de inversión de confianza, también conocidas como “matanza de cerdos” (o "Pig Butchering" en inglés) son obra de estafadores que cultivan una relación falsa en línea con sus víctimas con el propósito de ganarse su confianza y convencerlas para que inviertan en lo que consideran una oportunidad segura de inversión, pero que es en realidad una operación fraudulenta. El término “matanza de cerdos” ha sido acuñado por los propios estafadores, y hace referencia a la práctica de “engordar” a la víctima con afecto y atención antes de “descuartizarla” económicamente.

Los estafadores se hacen pasar con frecuencia por posibles parejas románticas o nuevos amigos, y convencen a sus objetivos de que inviertan en plataformas falsas de criptomonedas u otras oportunidades financieras engañosas. Una vez que la víctima invierte dinero, el estafador desaparece con los fondos, dejando a la víctima no solo devastada

financieramente, sino también traicionada en el aspecto emocional. Esta estafa ha sido cada vez más frecuente en los últimos años, aprovechando la creciente popularidad de las plataformas de citas en línea y redes sociales.

SEÑALES DE ALERTA

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

- El estafador promete grandes ganancias o rendimientos a corto plazo con poco esfuerzo.
- Se le presiona para que actúe rápidamente diciendo que podría perder la oportunidad de ganar "a lo grande."
- El estafador afirma que hay poco riesgo para la inversión y rendimientos garantizados. Es una estafa. Todas las inversiones implican riesgo de perder dinero.
- Se le dan pocos detalles sobre la inversión. Por lo general, los estafadores no proporcionan un folleto u otra información escrita que detalle el alcance o los riesgos de la inversión.
- Prometen un sistema secreto y probado que le permitirá ganar mucho dinero rápidamente y con poco esfuerzo.
- Requieren que pague una tarifa por adelantado, compre kits de inicio o invierta en productos o servicios antes de que pueda comenzar a ganar

dinero. Por lo general, los empleos legítimos no requieren que usted pague para trabajar.

- Las estafas piramidales enfatizan en el reclutamiento de otros participantes, en lugar de vender productos o servicios genuinos. Si el objetivo principal es reclutar nuevos miembros y ganar comisiones de sus inversiones o membresías, es probable que se trate de una operación piramidal.

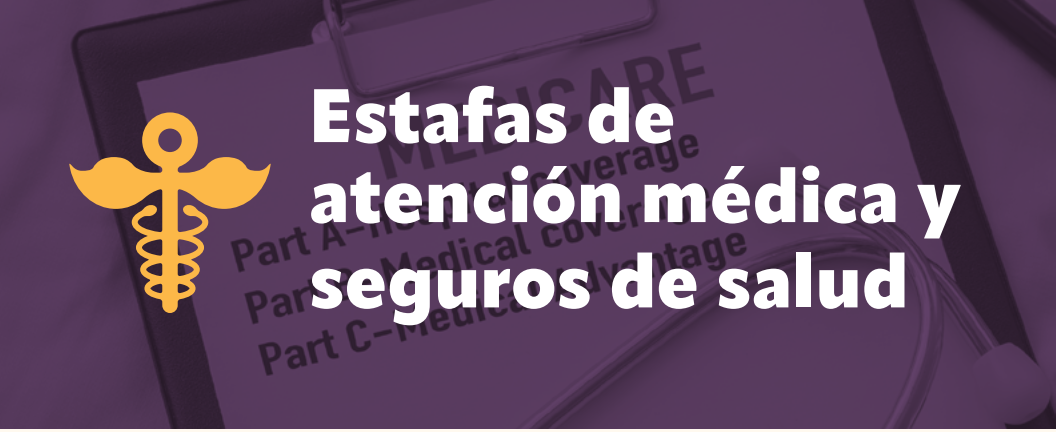
PASOS PARA PREVENIR Y RESPONDER

- No invierta dinero basándose en los consejos de alguien que solo ha conocido en línea o a través de una aplicación.
- Tenga cuidado con las ofertas no solicitadas. Desconfíe de las llamadas, mensajes de texto, de correo electrónico o de redes sociales no solicitados.
- No se apresure a invertir. Si se trata de una inversión legítima, seguirá estando disponible.
- Verifique las credenciales y compruebe de forma independiente cualquier información que se le proporcione, o estados de cuenta que le muestren. La mayoría de las estafas de inversión involucran a participantes no certificados.
- Conozca sus finanzas. Si no puede permitirse perder parte o la totalidad de su inversión, debe pensarlo dos veces antes de invertir.

- Consulte con un asesor financiero o un familiar o amigo de confianza si tiene dudas.
- 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 **reportfraud.ftc.gov**.
- Presente una queja ante la Comisión de Bolsa y Valores de los Estados Unidos (SEC) en **sec.gov/tcr**.

MÁS INFORMACIÓN

- Consulte la base de datos EDGAR de la SEC para verificar la veracidad de las afirmaciones en **www.sec.gov/edgar/search-and-access.**
- Si tiene un problema o pregunta sobre inversiones, el regulador estatal de valores puede ayudarlo. Para encontrar un regulador en su estado, visite **www.nasaa.org/contact-your-regulator** o llame al 202-737-0900.
- La FTC tiene más información sobre las estafas que consisten en oportunidades para ganar dinero e inversiones en **consumer.ftc.gov/jobs-and-making-money/money-making-opportunities-and-investments**.



Estafas de atención médica y seguros de salud

Las decisiones sobre la atención médica y la cobertura de seguros pueden ser complejas. Los estafadores se aprovechan de esta complejidad haciéndose pasar por representantes del programa Medicare, los planes de seguro médico comerciales 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. En 2023 se confirmaron 17 millones de dólares en pérdidas debidas a estafas de seguros médicos, pero se estima que la cifra real es mucho mayor, ya que es muy probable que estas pérdidas no se denuncien.[26]

Informes de la Línea directa contra el fraude

Una persona que llamó desde Massachusetts fue contactada por un estafador que se hizo pasar por funcionario de Medicare. El estafador dijo que la tarjeta de Medicare de la víctima estaba a punto de vencer y solicitó su número de Medicare y el nombre de su médico.

SEÑALES DE ALERTA

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

- Una persona que llama haciéndose pasar por empleado del gobierno le dice que se le cobrará una tarifa para obtener una tarjeta de Medicare. El gobierno nunca le cobrará por una tarjeta de Medicare nueva o de reemplazo.
- Recibe una llamada de alguien que dice que su tarjeta de Medicare está por vencer. Es una estafa. Mientras permanezca inscrito en Medicare y pague su prima mensual, su tarjeta de Medicare no perderá validez.
- Se le solicita por llamada, mensaje de correo electrónico o de texto información personal o financiera para "verificar" su seguro médico.
- Se le ofrece ayuda para transitar por el Mercado de Seguros Médicos, a cambio de una tarifa.

- Se le ofrece un plan médico con “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 detalles específicos relacionados con la cobertura de seguro que 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 aclarar la situación.
- Visite fuentes confiables como **Healthcare.gov** o **Medicare.gov**, para comparar planes, coberturas 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 médica, 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, llamados también

"navegadores" o "asistentes", no le cobrarán. Visite **www.healthcare.gov/find-assistance/** directamente para obtener ayuda. Las personas elegibles para Medicare pueden encontrar asistencia con sus Programas Estatales de Asistencia de Seguro de Salud (SHIP, por sus siglas en inglés) en **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 **reportfraud.ftc.gov**.

MÁS INFORMACIÓN

- La FTC proporciona información y consejos adicionales en **consumer.ftc.gov/articles/spot-health-insurance-scams**.
- La FCC tiene más información sobre las estafas de Medicare en **fcc.gov/older-americans-and-medicare-scams**.
- Los Centros de Servicios de Medicare y Medicaid (CMS, por sus siglas en inglés) tienen recursos para denunciar estafas o intentos de estafa en **www.medicare.gov/basics/reporting-medicare-fraud-and-abuse**.
- El Departamento de Salud y Servicios Humanos de los Estados Unidos mantiene una extensa lista de información sobre prevención de estafas en **oig.hhs.gov/fraud/consumer-alerts**.

Estafas de viajes, vacaciones y propiedades de tiempo compartido

Las estafas de viajes, vacaciones y propiedades de tiempo compartido explotan el deseo de lujo y relajación asequibles. Estas estafas comienzan generalmente con tentadoras ofertas de viajes gratis, paquetes de vacaciones con grandes descuentos u ofertas exclusivas de tiempo compartido, ofrecidas usualmente a través de llamadas telefónicas no solicitadas, correos electrónicos o atractivos anuncios en línea. Los estafadores persuaden a las víctimas a pagar tarifas por adelantado por la reserva, los impuestos o la membresía, prometiendo un valor increíble que nunca se materializa.

En el caso de los planes de tiempo compartido, el engaño puede ser aún más insidioso. Los estafadores utilizan tácticas de venta de alta presión para obligar a sus víctimas a comprar propiedades vacacionales, con frecuencia con falsos pretextos o términos engañosos. A menudo, una vez atrapadas en un contrato de tiempo compartido, las víctimas descubren que es casi imposible escapar del acuerdo, enfrentándose a tarifas de mantenimiento continuas, evaluaciones especiales y falta de mercado de reventa.

Los supuestos beneficios de la propiedad de tiempo compartido, como la flexibilidad y el ahorro de costos se evaporan, dejando a los propietarios con una carga financiera significativa y sin una salida fácil. Esta situación puede convertir lo que estaba destinado a ser unas vacaciones de ensueño en una pesadilla financiera a largo plazo. La FTC reportó más de $122 millones en pérdidas debido a estafas de vacaciones y propiedades de tiempo compartido.[27]

Informes de la Línea directa contra el fraude

Una residente de la Florida llamó a la Línea directa y explicó que le habían prometido un plan de tiempo compartido con cero por ciento de financiamiento. Sin embargo, no ha podido usar su plan y se ha quedado con extensas tarifas ocultas a pagar. Tampoco ha podido cancelar su plan.

SEÑALES DE ALERTA

Los estafadores de vacaciones y propiedades de tiempo compartido emplean estas tácticas con frecuencia:

- Tenga cuidado con las ofertas inesperadas o las tácticas de venta agresivas que le obligan a tomar decisiones rápidas sin una investigación adecuada.
- Evite las ofertas que requieran pagos por adelantado de impuestos, reservas o membresías para reclamar vacaciones “gratis” o con grandes

descuentos. Por lo general, las ofertas legítimas no solicitan dichas tarifas por adelantado.

- Tenga cuidado con los contratos vagos, poco claros o demasiado complejos que ocultan los verdaderos costos y condiciones de los acuerdos de tiempo compartido. Siempre revise los contratos cuidadosamente y busque asesoramiento profesional si es necesario.

PASOS PARA PREVENIR Y RESPONDER

- Verifique la legitimidad de la empresa y la oferta comprobando las reseñas, las calificaciones y el estado regulatorio.
- Evite las ofertas que requieran cargos por adelantado por concepto de impuestos, reservas o membresías, especialmente para ofertas "gratuitas" o con grandes descuentos.
- Revise todos los términos y condiciones en detalle, y considere consultar a un asesor jurídico o financiero antes de firmar cualquier contrato.
- Si se siente apurado o presionado para tomar una decisión, de un paso atrás y reconsidere. Las ofertas legítimas le proporcionarán tiempo suficiente para pensar.
- Denuncie cualquier llamada, correo electrónico o correo sospechoso a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en **reportfraud.ftc.gov**.

MÁS INFORMACIÓN

- La FTC tiene más información sobre estafas de viajes, vacaciones y propiedades de tiempo compartido en **consumer.ftc.gov/articles/timeshares-vacation-clubs-and-related-scams**.

Robo de identidad

Las estafas de robo de identidad se producen cuando un delincuente obtiene y utiliza indebidamente los datos personales de otra persona. Un objetivo común para el robo de identidad es el acceso no autorizado a una cuenta bancaria ajena. También puede consistir en el robo de números de Seguro Social, la dirección personal o incluso información de atención médica. Los estafadores pueden retirar dinero, presentar solicitudes falsas de préstamos o intentar reclamar beneficios como el de Seguro Social o de desempleo a nombre del adulto mayor. En 2023, la FTC reportó más de un millón de casos de robo de identidad,[28] y un informe de AARP reveló que los estadounidenses perdieron $43 mil millones por tal razón ese mismo año.[29]

Informes de la Línea directa contra el fraude

Un residente de Delaware recibió una llamada de alguien que intentaba robar su información de identificación personal haciéndose pasar por un empleado de la compañía estatal de electricidad.

SEÑALES DE ALERTA

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

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

PASOS PARA PREVENIR Y RESPONDER

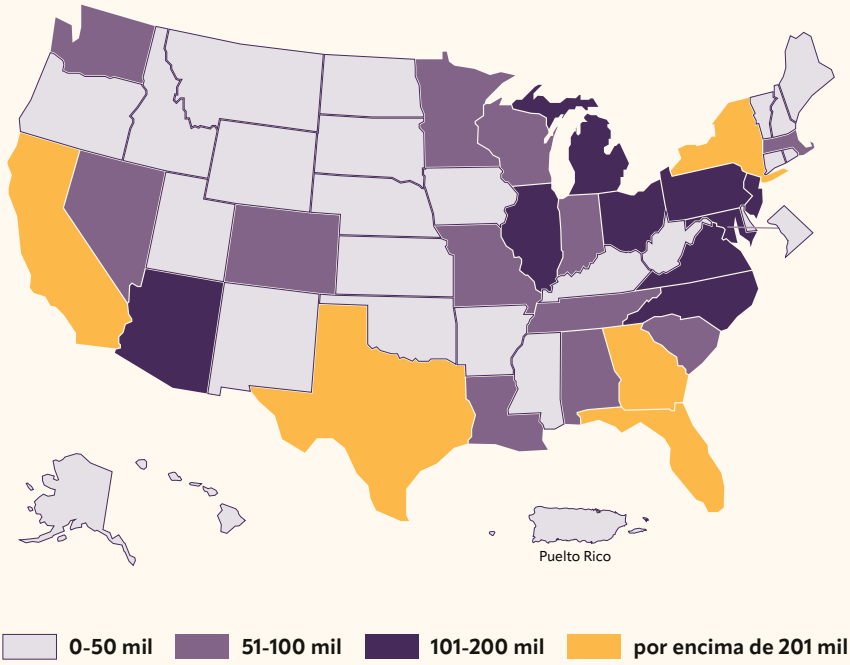
- Si alguien le pide su número de Seguro Social o información personal por teléfono, cuelgue. Si afirma ser de una empresa o agencia legítima, vaya al sitio web oficial de esa organización y llame a su línea oficial para verificar.
- No haga clic en enlaces de correo electrónico ni abra archivos adjuntos, incluso si el mensaje parece ser de una empresa conocida. Si lo hace, puede poner en riesgo su información personal. Si desea visitar la dirección del sitio web que aparece en el correo electrónico, hágalo manualmente en una ventana de búsqueda separada.

- Actualice sus contraseñas, especialmente si sospecha o se entera de que su banco o compañía de tarjeta de crédito fue pirateada. No utilice la misma contraseña en todas sus cuentas.
- Suscríbase a alertas de texto y por correo electrónico, especialmente aquellas que le informan sobre actividades inusuales.
- Denuncie todas las llamadas, mensajes o correos sospechosos a la FTC (1-877-382-4357) o a la policía local. También puede presentar una queja en línea en **reportfraud.ftc.gov**.

MÁS INFORMACIÓN

- Puede encontrar más información sobre el robo de identidad en el sitio web del Departamento de Justicia (DOJ, por sus siglas en inglés) en **www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud**.
- Denuncie las denuncias de robo de identidad y encuentre recursos de recuperación en **www.identitytheft.gov**.

QUEJAS REPORTADAS A LA FTC EN 2023, POR ESTADO:



Estado	2023
Alabama	68,818
Alaska	7,502
Arizona	107,477
Arkansas	30,171
California	537,766
Colorado	76,736
Connecticut	48,949
Delaware	18,673
Distrito de Columbia	16,687

Estado	2023
Florida	435,579
Georgia	219,245
Hawái	14,101
Idaho	17,198
Illinois	185,133
Indiana	71,890
Iowa	25,126
Kansas	27,452
Kentucky	40,221
Luisiana	63,121
Maine	13,317
Maryland	105,309
Massachusetts	89,545
Michigan	121,894
Minnesota	54,493
Misisipi	34,168
Misuri	73,176
Montana	10,120
Nebraska	18,252
Nevada	60,535
Nuevo Hampshire	15,022
Nueva Jersey	131,480
Nuevo México	21,541
Nueva York	267,377
Carolina del Norte	145,904
Dakota del Norte	5,764

Estado	2023
Ohio	146,405
Oklahoma	38,046
Oregón	50,988
Pensilvania	194,291
Rhode Island	11,906
Carolina del Sur	76,116
Dakota del Sur	6,274
Tennessee	88,131
Tejas	437,790
Utah	32,499
Vermont	6,188
Virginia	120,307
Washington	92,478
Virginia Occidental	16,233
Wisconsin	56,339
Wyoming	5,286
Puerto Rico	7,533
Desconocido*	957,971
Total	**5,524,523**

Nota: La cifra representa el total de denuncias de fraude, robo de identidad y otras estafas a la Consumer Sentinel Network de la FTC, en lugar de una medida estadísticamente representativa de la incidencia de estafas o explotación financiera de adultos mayores en cada estado. Es probable que las llamadas reflejen el conocimiento de los consumidores sobre la FTC y sus socios. *Desconocido representa los informes que no están definidos en los 50 estados, el Distrito de Columbia o Puerto Rico.

Recursos

CONSEJOS ADICIONALES SOBRE CÓMO PROTEGERSE DE LOS ESTAFADORES QUE TRATAN DE COMUNICARSE CON USTED A TRAVÉS DE LOS SIGUIENTES MECANISMOS:

Mensajes de texto: Los timadores suelen utilizar las estafas de 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. También pueden fingir que se comunican con usted accidentalmente a través de una estafa de mensajes de texto falsos con un número incorrecto. En esta estafa, es posible que reciba un mensaje de texto destinado supuestamente a otra persona o de alguien que dice conocerlo. Los destinatarios de mensajes de texto con "número incorrecto" responden a menudo por cortesía o curiosidad. Luego, el estafador usa esa respuesta inicial para crear una conexión, lo que le hace más susceptible a engaños como una estafa "romántica" o una estafa de inversión en criptomonedas.

Consejos para protegerse:

- Si recibe un mensaje de texto inesperado de un remitente desconocido, no haga clic en ningún enlace ni responda. Si cree que el mensaje de texto es legítimo, comuníquese directamente con la compañía. No utilice la información de contacto proporcionada en el mensaje de texto.

- Si recibe un mensaje de texto que cree podría ser una estafa, bloquee el número para que no vuelvan a comunicarse con usted. No responda, porque si lo hace, podría recibir más mensajes de los estafadores.
- No pague para que le vuelvan a entregar un paquete. Las empresas de entrega de paquetes nunca solicitarán un pago para hacerlo.
- Puede denunciar estas estafas de texto copiando el mensaje y reenviándolo al 7726 (SPAM). Esto puede ayudar a su proveedor de telefonía celular a identificar y bloquear mensajes de *spam* similares.

Anuncios en línea y ventanas emergentes: los anuncios en línea se utilizan para hacerse pasar por empresas y minoristas legítimos. Estos anuncios anuncian frecuentemente ofertas que son "demasiado buenas para ser ciertas." Los estafadores roban la información de la víctima como el número de tarjeta de crédito, una vez que la misma realiza la "compra."

Las ventanas emergentes son una estrategia común utilizada por los estafadores de "soporte técnico," analizadas anteriormente en esta guía.

Consejos para protegerse de anuncios y ventanas emergentes fraudulentos en línea:

- No haga clic en ningún enlace de ventanas emergentes de un sitio web ni de anuncios en línea.

Para visitar un sitio web, escriba la dirección de este directamente en el navegador.

- Tenga cuidado con los anuncios que vea en las redes sociales, ya que podrían tratarse de una estafa.
- 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 conozca.
- Autorice a su software contra virus y programas malignos a actualizarse automáticamente y analice regularmente su computadora en busca este tipo de amenazas.

Redes sociales: Las plataformas de redes sociales son uno de los métodos de contacto más comunes utilizados por los estafadores que atacan a los adultos mayores en línea y ofrecen la oportunidad de acceder a datos personales y ganarse la confianza de las víctimas.

Según la FTC, por tercer año consecutivo, las víctimas perdieron más dinero por estafas originadas en las redes sociales en comparación con cualquier otro método de contacto. En 2023, se reportaron pérdidas de $1.4 mil millones por estafas que comenzaron a través de plataformas de redes sociales,

principalmente Facebook e Instagram. Las mayores pérdidas reportadas por estafas perpetradas a través de las redes sociales fueron las de inversión.[30]

Consejos para protegerse de los estafadores en las redes sociales:

- Asegúrese de usar una contraseña segura y una configuración de privacidad que oculte información como su ciudad, número de teléfono y fecha de nacimiento.
- No acepte solicitudes de amistad de extraños, de alguien que 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 redirigirle a un sitio web para reclamar un premio, llenar un cuestionario, completar una encuesta o ver un video.
- Si recibe una solicitud urgente de dinero o una inversión en línea de un amigo o contacto en las redes sociales, lo más probable es que se trate de una estafa. Si cree que podría ser genuino, confirme con ellos en otra plataforma o véalos en persona para verificarlo. **Tenga en cuenta:** su cuenta podría haber sido pirateada, especialmente si le piden que envíe criptomonedas, tarjetas de regalo o una transferencia bancaria.

- Tenga cuidado con los anuncios falsos en las redes sociales. Antes de comprar algo a través de un anuncio en las redes sociales, verifique la empresa. Busque en línea su nombre añadiendo las palabras "estafa" o "queja."

Llamadas telefónicas: Las llamadas no solicitadas y las llamadas automáticas (*robocalls*) son las principales quejas que recibe la FCC.[31] Las llamadas automáticas se pueden realizar desde cualquier parte del mundo y, a menudo, contienen un mensaje de voz pregrabada, robótica o generada por IA. Las llamadas automáticas pueden intentar vender un producto o servicio, y pueden "falsificar" o imitar un número local o de una empresa con la que usted está familiarizado.

- Usted contesta el teléfono y la persona que llama (o una grabación) le pide que pulse una tecla para dejar de recibir las llamadas. Los estafadores suelen utilizar este truco para identificar posibles objetivos.
- Recibe una consulta de un supuesto representante de una empresa o agencia gubernamental. Cuando usted cuelga y llama al número de teléfono verificado de esa persona u organización, no tienen constancia de haberle llamado.
- Es posible que no pueda saber de inmediato si una llamada entrante es falsa. **Tenga en cuenta:** el identificador de llamadas que muestra un número "local" no significa necesariamente que sea una persona que llama localmente.

- No conteste llamadas de números desconocidos.
- No responda a ninguna pregunta no solicitada, especialmente aquellas que pueden responderse con un "Sí."
- Nunca proporcione información personal como números de cuenta, números de Seguro Social, apellido de soltera, contraseñas u otra información de identificación personal en respuesta a llamadas inesperadas, o si tiene sospechas.
- Si es víctima de fraude o pérdida monetaria por una llamada automática, comuníquese con la FCC al 1-888-225-5322 o con la FTC al 1-877-382-4357 lo antes posible. También puede presentar una queja en línea en **reportfraud.ftc.gov**.

Correo electrónico: Los estafadores usan frecuentemente mensajes de correo electrónico de *phishing* para engañar sus víctimas y hacerles que revelen su información personal. Estos son algunos ejemplos de mensajes de correo electrónico que podría recibir y que probablemente sean estafas:

- Un mensaje afirma que necesita verificar o actualizar la información de su cuenta, y lo dirige a una página de inicio de sesión falsa.
  - **No escriba** tu información en esta página. Los estafadores pueden capturar su nombre de usuario y contraseña e iniciar sesión en el sitio real usando su cuenta.

- Un mensaje le advierte de actividad sospechosa en su cuenta y le insta a hacer clic en un enlace para protegerla.
    - ◊ **No** haga clic en enlaces ni descargue archivos adjuntos de direcciones de correo electrónico desconocidas o sospechosas.
- Un mensaje le informa que ha ganado un premio o recompensa, pero debe proporcionar información personal o pagar una tarifa para reclamarlo.
- Un mensaje crea una sensación de urgencia, indicando que su cuenta se bloqueará a menos que proporcione de inmediato información confidencial.
- Un mensaje contiene una factura o recibo inesperado y le pide que abra un archivo adjunto o haga clic en un enlace para revisarlos.

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.

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

También puede ponerse en contacto con su representante o senador. Puede denunciar el fraude a su oficina, y es posible que puedan brindarle asistencia. Para localizar a su congresista usando su código postal, vaya a www.house.gov. Para localizar a su Senador, vaya a www.senate.gov/senators/senators-contact.htm. También puede llamar al (202) 224-3121. Un operador de centralita te conectará directamente con la oficina que solicites.

CÓMO OBTENER AYUDA DESPUÉS DE UNA ESTAFA

Las estafas afectan la salud financiera, emocional y física de las víctimas y sus familias. Existen recursos para ayudarle a responder y recuperarse del fraude.

Servicio	Recurso	Sitio web	Número telefónico
Apoyo y asesoría a víctimas	VictimConnect Resource Center	victimconnect.org/get-help/	1-855-484-2846
Ayuda jurídica	Legal Services Corporation	www.lsc.gov/about-lsc/what-legal-aid/get-legal-help	Use la herramienta de búsqueda para encontrar el número de teléfono de la oficina local de asistencia jurídica
Otros servicios	Localizador de atención a adultos mayores	eldercare.acl.gov/	1-800-677-1116

PROCURADORES GENERALES ESTATALES

Puede llamar a la oficina de su Procurador General a:

Estado/Territorio	Número telefónico
Alabama	(334) 242-7300
Alaska	(907) 269-5100
Samoa Estadounidense	(684) 633-4163
Arizona	(602) 542-5025
Arkansas	(800) 482-8982
California	(916) 445-9555
Colorado	(720) 508-6000
Connecticut	(860) 808-5318
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
Kentucky	(502) 696-5300
Luisiana	(225) 326-6465
Maine	(207) 626-8800
Maryland	(410) 576-6300
Massachusetts	(617) 727-2200
Michigan	(517) 335-7622

Estado/Territorio	Número telefónico
Minnesota	(651) 296-3353
Misisipi	(601) 359-3680
Misuri	(573) 751-3321
Montana	(406) 444-2026
Nebraska	(402) 471-2682
Nevada	(702) 486-3132
Nuevo 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
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
Texas	(512) 463-2100
Islas Vírgenes Estadounidenses	(340) 774-5666
Utah	(800) 244-4636
Vermont	(800) 649-2424
Virginia	(804) 786-2071

Estado/Territorio	Número telefónico
Washington	(360) 753-6200
Virginia Occidental	(304) 558-2021
Wisconsin	(608) 266-1221
Wyoming	(307) 777-7841

También puede comunicarse con su Procurador General en línea. La Asociación Nacional de Procuradores Generales proporciona una lista actualizada de todos los sitios web de los Procuradores Generales estatales en: **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 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 información puede ayudarlo a reportar el incidente a agencias y compañías. Actuar rápido es muy importante. No espere a tener toda esta información antes de reportar.

	Información importante que debe incluir en su queja	Escriba aquí sus notas
☐	¿Cuándo sucedió?	
☐	¿Cómo le contactaron?	
☐	¿Qué se le pidió que hiciera?	
☐	¿Cuánto dinero se le pidió que proporcionara?	

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

Advertencia: La Guía proporciona información general al consumidor sobre fraudes y estafas. La misma 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), Consumer Sentinel Network Data Book 2023, pg 11, **https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf** (visita más reciente, 13 de agosto de 2024)

2 FTC, "Think you know what the top scam of 2023 was? Take a guess," **https://consumer.ftc.gov/consumer-alerts/2024/02/think-you-know-what-top-scam-2023-was-take-guess** (visita más reciente, 13 de agosto de 2024)

3 Aging Committee Hearing, "Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back," **https://www.aging.senate.gov/hearings/modern-scams-how-scammers-are-using-artificial-intelligence-and-how-we-can-fight-back** (visita más reciente, 13 de agosto de 2024)

4 National Adult Protective Services Association (NAPSA), "Learning About Financial Exploitation," **https://www.napsa-now.org/financial-exploitation/** (visita más reciente, 13 de agosto de 2024)

5 U.S. Department of Treasury Financial Crimes Enforcement Network (FinCEN), "Financial Institutions Report $27 Billion in Elder Financial

Exploitation Suspicious Activity in One-Year Period," https://www.fincen.gov/news/news-releases/fincen-issues-analysis-elder-financial-exploitation (visita más reciente, 13 de agosto de 2024)

6 AARP, The Scope of Elder Financial Exploitation: What It Costs Victims, pg 1, https://www.aarp.org/content/dam/aarp/money/scams-and-fraud/2023/true-cost-elder-financial-exploitation.doi.10.26419-2Fppi.00194.001.pdf (visita más reciente, 13 de agosto de 2024)

7 FinCEN, Advisory on Elder Financial Exploitation, pg 2, https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf (visita más reciente, 13 de agosto de 2024)

8 Federal Bureau of Investigation (FBI), Elder Fraud Report 2023, pg 10, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf (visita más reciente, 13 de agosto de 2024)

9 FBI, Elder Fraud Report 2023, pg 16-17, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf (visita más reciente, 13 de agosto de 2024)

10 FTC, Consumer Sentinel Network, All Fraud Reports by Payment Method, **https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods** (visita más reciente, 13 de agosto de 2024)

11 Analysis of FTC data by Aging Committee staff. The analysis compares 2023 data to 2022 data. Datos de la FTC disponibles en línea: **https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods** (visita más reciente, 13 de agosto de 2024)

12 FTC, Consumer Sentinel Network, All Fraud Reports by Payment Method, **https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods** (visita más reciente, 13 de agosto de 2024)

13 FTC, Consumer Sentinel Network Data Book 2023, pg 5, **https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf** (visita más reciente, 13 de agosto de 2024)

14 FTC, Consumer Sentinel Network Data Book 2023, pg 7, **https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf** (visita más reciente, 15 de agosto de 2024)

15 FTC, Consumer Sentinel Network, Imposter Scams in 2023, **https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts** (visita más reciente, 16 de agosto de 2024)

16 FBI, "FBI Warns of Scammers Targeting Senior Citizens in Grandparent Scams and Demanding Funds by Wire, Mail, or Couriers," **https://www.ic3.gov/Media/Y2023/PSA231117** (visita más reciente, 15 de agosto de 2024)

17 FTC, Consumer Sentinel Network Data Book 2023, pg 7, **https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf** (visita más reciente, 15 de agosto de 2024)

18 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** (visita más reciente, 16 de agosto de 2024)

19 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, 16 de agosto de 2024)

20 FBI, Elder Fraud Report 2023, pg 7-8, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf (visita más reciente, 16 de agosto de 2024)

21 FTC, "Explore Government Imposter Scams," https://public.tableau.com/app/profile/federal.trade.commission/viz/GovernmentImposter/Infographic (visita más reciente, 16 de agosto de 2024)

22 FTC, "'Love Stinks' – when a scammer is involved," https://www.ftc.gov/business-guidance/blog/2024/02/love-stinks-when-scammer-involved (visita más reciente, 16 de agosto de 2024)

23 FTC, Consumer Sentinel Network Data Book 2023, pg 8, https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf (visita más reciente, 15 de agosto de 2024)

24 FBI, Elder Fraud Report 2023, pg 3, 15, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf (visita más reciente, 15 de agosto de 2024)

25 FBI, "FBI Highlights Growing Number of Reported Elder Fraud Cases Ahead of World Elder Abuse Awareness Day," https://www.fbi.gov/news/press-releases/fbi-highlights-growing-number-of-reported-elder-fraud-cases-ahead-of-world-elder-abuse-awareness-day (visita más reciente, 15 de agosto de 2024)

26 FTC, Consumer Sentinel Network Data Book 2023, pg 8, **https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf** (visita más reciente, 15 de agosto de 2024)

27 Id.

28 Id.

29 AARP, "Identity Fraud Cost Americans $43 Billion in 2023," **https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html** (visita más reciente, 15 de agosto de 2024)

30 FTC, "Who's who in scams: a spring roundup," **https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/05/whos-who-scams-spring-roundup (last visited August 15, 2024** visita más reciente, 15 de agosto de 2024)

31 Federal Communications Commission (FCC), "Stop Unwanted Robocalls and Texts," **https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts** (visita más reciente, 15 de agosto de 2024)

Notas

Notas

Notas

Notas

Línea Directa Contra el Fraude

1-855-303-9470

Comité Especial del Senado de los Estados Unidos para la Vejez