COMITÉ ESPECIAL DEL SENADO DE EE. UU.

PARA ASUNTOS DE LA VEJEZ

SEN. RICK SCOTT (R-FL)
PRESIDENTE

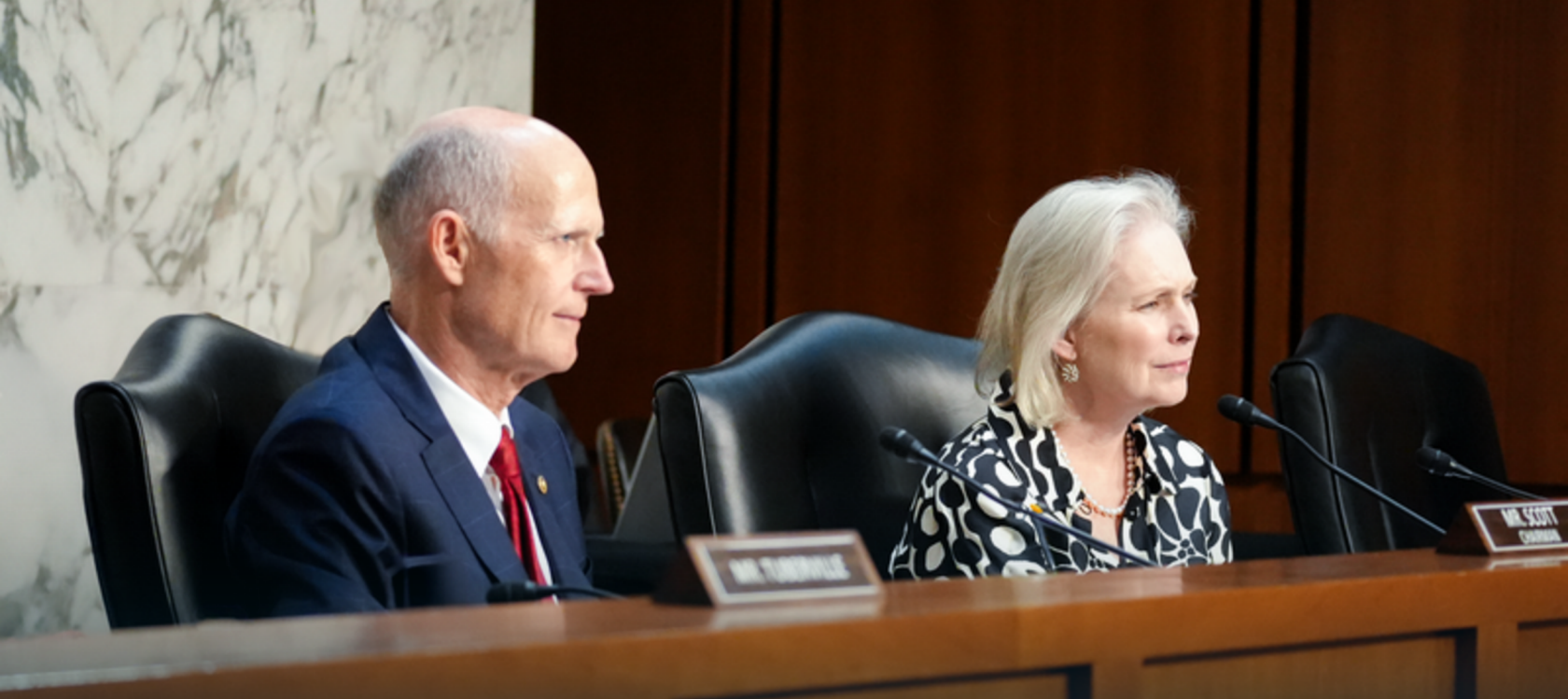
SEN. KIRSTEN GILLIBRAND (D-NY)
MIEMBRO DE ALTO RANGO

LA ERA DEL FRAUDE

ESTAFAS QUE ENFRENTAN LAS PERSONAS MAYORES DE NUESTRA NACIÓN

EDICIÓN 2025

TABLA DE CONTENIDO



ESTABLECIDO EN 1961, EL COMITÉ ESPECIAL PARA ASUNTOS DE LA VEJEZ DEL SENADO DE EE. UU. ES EL PUNTO FOCAL EN EL SENADO PARA LA DISCUSIÓN Y EL DEBATE SOBRE ASUNTOS RELACIONADOS CON LOS ESTADOUNIDENSES MAYORES. EL COMITÉ DE ENVEJECIMIENTO OPERA UNA LÍNEA DIRECTA GRATUITA DE FRAUDE (1-855-303-9470), QUE PROPORCIONA INFORMACIÓN PARA LOS ESTADOUNIDENSES MAYORES Y SUS FAMILIARES SOBRE CÓMO IDENTIFICAR Y DENUNCIAR FRAUDES Y ESTAFAS A LOS FUNCIONARIOS CORRESPONDIENTES, INCLUIDAS LAS FUERZAS DEL ORDEN.

RICK SCOTT, FLORIDA, PRESIDENTE
DAVE McCORMICK, PENNSYLVANIA
JIM JUSTICE, VIRGINIA OCCIDENTAL
TOMMY TUBERVILLE, ALABAMA
RON JOHNSON, WISCONSIN
ASHLEY MOODY, FLORIDA
JON HUSTED, OHIO

KIRSTEN GILLIBRAND, NUEVA YORK, MIEMBRO DE ALTO RANGO
ELIZABETH WARREN, MASSACHUSETTS
MARK KELLY, ARIZONA
RAPHAEL WARNOCK, GEORGIA
ANDY KIM, NUEVA JERSEY
ANGELA ALSOBROOKS, MARYLAND

OBTENGA MÁS INFORMACIÓN SOBRE NUESTROS MIEMBROS Y TRABAJO EN AGING.SENATE.GOV

MENSAJE DEL PRESIDENTE DEL COMITÉ SCOTT Y DE LA MIEMBRO DE ALTO RANGO GILLIBRAND

Queridos amigos,

El Comité Especial para Asuntos de la Vejez del del Senado de los Estados Unidos está comprometido con la protección de los estadounidenses mayores ante el fraude, las estafas y la explotación financiera en todos los niveles. A medida que estos planes se vuelven más sofisticados, el Comité trabaja para aumentar concientización, proporcionar recursos y abogar por protecciones más sólidas para garantizar Nuestros adultos mayores permanecen seguros, financieramente seguros y con tranquilidad en todo momento sus años dorados.

Una herramienta valiosa en este esfuerzo es la línea directa gratuita de fraude del Comité (1-855-303-9470) con personal capacitado y listo para ofrecer recursos y orientación y conectar a las personas con a las autoridades correspondientes para cualesquiera que sean sus necesidades. Este esfuerzo tiene como objetivo empoderar a las personas mayores y sus familias para que denuncien las estafas rápidamente y con confianza.

Cada año, el Comité recibe miles de informes de estafas y tendencias que son consistentes en el tiempo. En 2024, las personas mayores de 60 años perdieron una asombrosa cantidad 4.800 millones de dólares en estafas, mientras que las personas de 50 a 59 años perdieron 2.500 millones de dólares, según un reciente informe publicado por el FBI. En 2024, las estafas más comunes incluyeron esquemas de impostores, fraude de sorteos y estafas de lotería. Sin embargo, los estafadores recurren cada vez más a tecnologías emergentes, como las criptomonedas, la inteligencia artificial (IA) y las redes sociales, para crear productos más difíciles de detectar y más fraudes convincentes.

Los esquemas de fraude se presentan de muchas formas, incluidas las estafas de los abuelos, ayuda técnica de fraude, estafas de servicios financieros, estafas románticas o hacerse pasar por agentes gubernamentales. Estos esquemas a menudo se enfocan en vulnerabilidades emocionales, particularmente entre las personas mayores que enfrentan soledad, aislamiento o depresión.

Para ayudar a combatir estas amenazas en evolución, el Comité lideró un esfuerzo designando el 6 de marzo de 2025 como el Día Nacional de Slam the Scam, una iniciativa para crear conciencia sobre las estafas y educar al público sobre cómo evitarlos. Esta designación anual sirve como un poderoso recordatorio para las personas mayores y a sus seres queridos a mantenerse alerta e informados.

A través de la vigilancia continua, la educación pública y una supervisión sólida, esperamos para salvaguardar aún más el futuro financiero de nuestros estadounidenses que envejecen y restauran la confianza pública en los sistemas destinados a apoyarlos. Juntos, debemos permanecer enfocados en acabar con el fraude, proteger a las personas mayores y responsabilizar a las instituciones, por los adultos mayores de hoy y las generaciones venideras.

Sen. Rick Scott (R-FL)
Presidente

Sen. Kirsten Gillibrand (D-NY)
Miembro de Alto Rango

UN VISTAZO AL FRAUDE:

- El FBI dice que 2024 fue un año récord para las pérdidas reportadas al Centro de Quejas de Delitos en Internet (IC3), por un total de $ 16.6 mil millones
- En 2024 se registraron 859.532 denuncias y 4,2 millones en los últimos cinco años
- Las pérdidas totales aumentaron 33% de 2023 a 2024, y se descubrió que la mayor parte de ellas eran fraudes
- La cantidad promedio robada a adultos de 60+ años aumentó a $83,000 en 2024, y las denuncias para ese grupo de edad aumentaron 43%
- Las pérdidas relacionadas con las criptomonedas aumentaron 66% y las quejas de los quioscos de criptomonedas aumentaron un 99%

EXPLOTACIÓN FINANCIERA

Cada año, millones de estadounidenses mayores son explotados financieramente por personas conocidas y desconocidas para ellos. Según la Asociación Nacional de Servicios de Protección para Adultos (NAPSA, por sus siglas en inglés), la explotación financiera de las personas mayores es el uso indebido, el mal manejo o la explotación de la propiedad, las posesiones o los activos de los adultos mayores. Con frecuencia, esto se lleva a cabo sin el consentimiento del adulto mayor , bajo falsos pretextos o mediante influencia, coerción o manipulación indebidas. Los perpetradores de la explotación financiera de las personas mayores van desde miembros de la familia y otras personas de confianza hasta ciberdelincuentes y estafadores profesionales.

Un análisis de la Red de Ejecución de Delitos Financieros (FinCEN) del Departamento del Tesoro de EE. UU. encontró que entre junio de 2022 y junio de 2023, hubo más de 155,400 presentaciones bancarias, por un valor total de $ 27 mil millones, donde se sospechaba de explotación financiera de personas mayores. Además, FinCEN declaró que estas pérdidas anuales habían aumentado a 28.300 millones de dólares en un comunicado con varias agencias federales de regulación financiera el 18 de abril de 2024.

Si bien las personas de todas las edades pueden ser víctimas de la explotación financiera, los adultos mayores a menudo son atacados porque tienden a ser confiados y es más probable que hayan acumulado activos de décadas de trabajo y ahorro. Muchos adultos mayores son robados de sus ahorros para la jubilación o fondos médicos a través de la explotación financiera de los ancianos. La explotación financiera de las personas mayores también puede provocar un deterioro considerable de la salud mental y física.

La explotación financiera, que se etiqueta como una forma de abuso de personas mayores, es más común entre los adultos mayores socialmente aislados que encuentran barreras para acceder a los servicios o experimentan deterioro cognitivo. A menudo no se denuncia debido al miedo, la vergüenza o la falta de recursos.

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

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

Ejemplos de robo incluyen la falsificación de cheques, el cambio de nombres en cuentas bancarias o el uso de tarjetas de crédito sin permiso explícito.

Estafas
Las estafas implican la transferencia de dinero de una persona mayor a un extraño o impostor por un beneficio prometido que nunca se recibe. Los perpetradores de estafas son principalmente extraños, a menudo ubicados en un estado o país diferente al de sus víctimas.

Algunos ejemplos de estafas son las estafas de soporte técnico, las estafas de abuelos o de necesidades personales y las estafas de impostores del gobierno, que se destacan más adelante en este libro.

LA EXPLOTACIÓN FINANCIERA DE LAS PERSONAS MAYORES TAMBIÉN PUEDE PRESENTARSE DE OTRAS FORMAS. INCLUYE:

- Coaccionar o engañar a un adulto mayor para que firme un contrato, testamento o documento.
- El uso indebido de la curatela, la tutela o el poder notarial.

Pasos para protegerse:
- Planifique para proteger sus activos y asegúrese de que se cumplan sus deseos.
- Rompa todo lo que tenga su información personal, incluidos recibos, estados de cuenta bancarios, correo e incluso ofertas de tarjetas de crédito sin usar antes de tirarlas.
- Guarde bajo llave información financiera y confidencial importante cuando haya otras personas en su hogar.
- No permita que otras personas tengan acceso a su información financiera.
- Verifique a las personas que planea contratar verificando las referencias y credenciales.
- Revise regularmente su informe de crédito.
- Nunca comparta información personal con nadie 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 en el que confíe, como su asesor financiero o abogado, antes de firmar algo que no comprenda.
- Confía en tu instinto: si algo no se siente bien, puede que no esté bien.

Denuncia de la explotación financiera de los ancianos

- Si usted, o alguien que conoce, está en 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 área https://www.napsa-now.org/help-in-your-area/ o llame al 2-1-1.
- Presenta una denuncia ante la FTC en reportfraud.ftc.gov o ante el FBI en ic3.gov.
- Repórtelo a la Línea Directa de Fraude para Personas Mayores del DOJ al 833-FRAUD-11 (833-372-8311).
- Si el abuso está ocurriendo en un centro de atención a largo plazo, como un hogar de ancianos o un centro de vida asistida, APS y los defensores del pueblo de atención a largo plazo pueden ayudar. Los defensores del pueblo de cuidados a largo plazo son defensores de los consumidores que garantizan los derechos y la dignidad de los residentes que viven en centros de cuidados a largo plazo. Utilice el mapa interactivo del Centro Nacional de Recursos para el Cuidado a Largo Plazo de Consumer Voice para encontrar un Programa del Defensor del Pueblo para el Cuidado a Largo Plazo en su área: theconsumervoice.org/get_help

CÓMO LOS ESTAFADORES ESTÁN ROBANDO EL DINERO DE LAS PERSONAS

PARA ROBAR EL DINERO DE LAS PERSONAS, LOS ESTAFADORES UTILIZAN TECNOLOGÍA QUE LES PERMITE LLEGAR A MILES DE PERSONAS DE MANERA FÁCIL Y ECONÓMICA, ASÍ COMO MÉTODOS DE PAGO Y MONEDA QUE LES AYUDAN A ACCEDER AL DINERO RÁPIDAMENTE Y NO DEJAN RASTRO.

ENFOQUE EN LA TECNOLOGÍA: INTELIGENCIA ARTIFICIAL:

La Inteligencia Artificial (IA) es una tecnología que permite a las máquinas imitar a ciertos como conductas similares, como el habla o la escritura. Por ejemplo, nuevos chatbots y lenguaje. Las herramientas de procesamiento pueden responder preguntas detalladas, escribir ensayos convincentes y desarrollar código informático. Si bien esta tecnología se puede utilizar para el bien, estas poderosas herramientas también pueden ser explotados por los malos actores para hacer que las estafas sean más sofisticadas y convincentes. Éste describe la tecnología de IA, cómo se puede utilizar en fraudes y estafas, y qué señales de advertencia a las que hay que prestar atención.

¿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 de voz que suenan como la voz real de alguien que puede conocer.

Deepfakes: Un deepfake es un vídeo o una imagen generada por una IA que se hace parecer 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 impulsados por AAI: Ataques de phishing, en los que los estafadores engañan a las personas
revelar información confidencial, se han vuelto cada vez más sofisticados con la uso de la IA. Con el uso de la IA, los estafadores pueden crear fácilmente correos electrónicos para ataques de phishing, que personalizan los correos electrónicos de phishing imitando diálogos sofisticados y omitiendo los filtros de spam tradicionales, lo que dificulta que las personas distingan entre comunicaciones genuinas y fraudulentas.

Estafas románticas: Los estafadores emplean la IA para crear y operar perfiles falsos en las citas sitios web y plataformas de redes sociales. A continuación, los chatbots impulsados por IA simulan de forma realista una conversación para generar confianza, con el objetivo de engañar a la víctima para que les envíe dinero. Puede ser difícil saber si alguien está utilizando tecnología de IA en una estafa. Lo cierto es que la IA hace que los fraudes y estafas tradicionales sean más convincentes y fáciles de desplegar a mayor escala.

Consejos para protegerse:

- No comparta información confidencial por teléfono, correo electrónico, mensaje de texto o redes sociales.
- No transfieras ni envíes dinero a lugares desconocidos.
- Considere designar una "palabra de seguridad" para su familia que solo se comparta con los miembros de la familia y los contactos cercanos.
- No proporcione ninguna información personal o confidencial a un chatbot en línea.
- 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

La criptomoneda es un tipo de moneda digital que solo existe electrónicamente. Es posible que las transacciones de criptomonedas no estén mediadas por un tercero de confianza, sean seudónimas y difíciles de rastrear, lo que puede hacer que este método de pago sea un mecanismo útil para los estafadores. También es el preferido por los estafadores porque obtienen el dinero al instante y los pagos no suelen ser reversibles.

Los pagos con criptomonedas se pueden utilizar en una variedad de estafas, incluidas las estafas de inversión falsa y las estafas de amistad o romance falsos. Estas estafas también se pueden usar juntas: las estafas de inversión en criptomonedas pueden comenzar con estafadores que inicialmente enganchan a las víctimas a través de un falso romance y luego progresar a solicitudes de dinero para una supuesta inversión.

Una técnica común que utilizan los estafadores es construir una relación con sus víctimas con el tiempo, ganándose su confianza y luego convenciéndolas de invertir en un esquema fraudulento, lo que resulta en pérdidas financieras significativas; Esto se conoce como una "estafa de inversión de confianza", que se analiza más adelante en este libro. Una vez que el estafador se ha ganado la confianza de la víctima, los estafadores presionan a las víctimas para que "inviertan" en una plataforma de criptomonedas específica prometiendo altos rendimientos y utilizando tácticas sofisticadas para crear un sentido de legitimidad. En realidad, la plataforma es falsa y está controlada por estafadores, que desaparecen con los fondos "invertidos" una vez que han acumulado suficiente dinero de inversores desprevenidos.

La Oficina Federal de Investigaciones (FBI) descubrió que los adultos de 60+ años perdieron más de $2,839,333,197 por estafas relacionadas con criptomonedas en 2024, un aumento reportado de casi el 52 por ciento con respecto a 2022. En un comunicado del 15 de junio de 2024, el FBI determinó que ya se habían producido pérdidas por valor de 1.600 millones de dólares entre enero y mayo de 2024, casi 300 millones de dólares más que en el mismo periodo de 2023. El FBI también descubrió que las mayores pérdidas entre los adultos mayores relacionadas con las criptomonedas fueron estafas de inversión relacionadas con las criptomonedas, con más de USD 1,600,353,509 en pérdidas reportadas en 2024.

Consejos para protegerse:

- Ignore los consejos y las ofertas que lo ayuden a invertir en criptomonedas: lo más probable es que sea una estafa.
- Si conoces a alguien en un sitio o aplicación de citas, y quiere que le envíes criptomonedas o te 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 verdad.
- No se relacione con "gestores de inversiones" que se ponen en contacto con usted y le hacen promesas sobre el retorno de la inversión.
- Una celebridad no se pondrá en contacto con las personas directamente para vender criptomonedas. No respondas a ningún mensaje que pretenda ser de una celebridad.
- No acepte criptomonedas "gratuitas" de extraños.
- Si ha sido víctima de una estafa de criptomonedas, desconfíe de cualquier persona que afirme que puede recuperar sus fondos, ya que podría tratarse de otra estafa. Los estafadores a menudo se dirigen a la misma persona más de una vez porque la perciben como vulnerable, confiada y potencialmente menos propensa a denunciar el fraude o buscar recursos legales 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 criptomonedas, 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: https://www.ic3.gov/PSA/2023/PSA230824.

PAGOS PEER-TO-PEER (P2P):

Los pagos P2P son transacciones entre dos partes con cuentas bancarias separadas, mediadas a través de un sitio web o una aplicación móvil de terceros. Los estafadores pueden abusar de estas plataformas porque, al igual que las criptomonedas, los estafadores reciben el dinero inmediatamente después de que se inicia una transferencia. Si bien muchas empresas de pago P2P emplean sistemas avanzados para marcar y congelar transacciones sospechosas, estas plataformas a menudo no pueden revertir una transacción una vez que se envía el dinero. Estas aplicaciones también pueden carecer de la misma protección contra el fraude que ahora emplean los bancos tradicionales y las tarjetas de crédito.

En 2024, la FTC recibió alrededor de 90,531 informes de consumidores que enviaron dinero a estafadores a través de aplicaciones de pago P2P, como CashApp, Venmo o Zelle, con pérdidas reportadas por un total de más de $391 millones.

Consejos para protegerse:

- Nunca envíes pagos a alguien que no conozcas. Tómate tu tiempo para asegurarte de que estás enviando dinero a la persona adecuada.
- Configura alertas de fraude en tu aplicación de pago P2P o con la cuenta bancaria o de tarjeta de crédito que hayas 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. Y en las redes sociales, ignora las solicitudes de amistad de personas que no conoces.
- Debe evitarse cualquier negocio que acepte exclusivamente aplicaciones de pago P2P o pagos con tarjeta de débito prepaga.
- 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 uno de los principales métodos utilizados por los estafadores para solicitar y robar dinero a los adultos mayores. [JH1] [MW2] [MS3] Cuando la víctima envía al estafador el número de la tarjeta de regalo, el estafador utiliza inmediatamente el saldo, lo que hace imposible recuperar el dinero.

En 2024, la FTC recibió más de 41,100 denuncias de estafas con tarjetas de regalo, lo que resultó en aproximadamente $212 millones en pérdidas reportadas.

Consejos para protegerse:

- Si le paga a un estafador con una tarjeta de regalo, dígaselo de inmediato a la compañía que emitió la tarjeta
- Si compras tarjetas de regalo para regalar o donar a familiares y amigos, compra las tarjetas de regalo en tiendas que conozcas y en las que confíes. Revise las pegatinas protectoras de la tarjeta para asegurarse de que no parezcan haber sido manipuladas.
- Guarde siempre su recibo y una copia de la tarjeta de regalo. El número que aparece en la tarjeta de regalo y el recibo de la tienda te ayudarán a presentar una denuncia si pierdes la tarjeta de regalo o necesitas denunciar una estafa.
- Tenga cuidado con las señales de estafas, como las solicitudes para comprar tarjetas de regalo en varias tiendas o para comprar un tipo específico de tarjeta de regalo.
- Tenga en cuenta: Ninguna empresa o agencia gubernamental le dirá que compre una tarjeta de regalo para pagarles. Esto siempre es una estafa.
- Para obtener más información sobre las estafas con tarjetas de regalo y cómo protegerse, visite la FTC en https://consumer.ftc.gov/articles/avoiding-and-reporting-gift-card-scams.

ESTAFAS A LAS QUE HAY QUE PRESTAR ATENCIÓN

En 2024, la Línea Directa de Fraude del Comité recibió casi 500 nuevas quejas de personas de todo el país. Estas quejas elevan el número total de quejas registradas en la Línea Directa de Fraude desde 2013 a casi 12,400.

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

Los fraudes denunciados representan casi 2.6 millones[1] de las 6.5 millones de quejas denunciadas ante la FTC en 2024. Las categorías de fraude comunes incluyen 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, incluyen estafas de cobro de deudas, estafas hipotecarias y estafas de reparación de viviendas.

ESTAFAS DE IMPOSTORES

Las estafas de impostores son las más generalizadas de todas las estafas reportadas a la FTC, con casi 846,000 reportes en 2024. Estas estafas pueden aparecer de muchas formas diferentes a medida que los estafadores encuentran nuevas formas de dirigirse a las víctimas. Las siguientes cinco secciones discutirán algunas de las estafas de impostores más frecuentes que se usan comúnmente para dirigirse a los adultos mayores.

VÍCTIMAS DE ESTAFAS

Víctimas del Huracán Helene

Funcionarios federales, estatales y locales emitieron avisos esta semana advirtiendo a las víctimas de huracanes, especialmente a las más necesitadas, que tengan cuidado con las personas que se presentan en su puerta o las llaman diciendo que quieren ayudar. Defraudar a las víctimas de los huracanes y a la propia Agencia Federal para el Manejo de Emergencias (FEMA, por sus siglas en inglés) es una industria multimillonaria para los delincuentes, según expertos, autoridades federales y advertencias gubernamentales.

"Los estafadores y delincuentes pueden intentar obtener dinero o robar información personal a través de fraude o robo de identidad después del huracán Helene", advirtieron los funcionarios de FEMA. "En algunos casos, los ladrones intentan solicitar asistencia de FEMA usando nombres, direcciones y números de Seguro Social que han robado de personas afectadas por el desastre".

En Carolina del Norte, que incluye algunas de las regiones más afectadas por las inundaciones de Helene, el principal fiscal federal del estado dijo esta semana que los delincuentes se están sumando a un desastre ya histórico. Al menos 144 personas murieron durante Helene y cientos de casas han sido destruidas.

"El impacto de los desastres que afectan a nuestros ciudadanos no es solo de los eventos en sí, sino también de los estafadores que se aprovechan de las víctimas de desastres y de las personas de buen corazón que quieren ayudar a los afectados", dijo Sandra J. Hairston, fiscal federal para el Distrito Medio de Carolina del Norte. "Estos delincuentes se aprovechan de las víctimas antes, durante y después de que ocurra un desastre natural, apuntando a las personas cuando son más vulnerables".

"Los esquemas incluyen organizaciones benéficas falsas que solicitan donaciones para las víctimas de desastres, estafadores que se hacen pasar por funcionarios del gobierno que reparten asistencia y empresas falsas que ofrecen ayudar con la recuperación", dijo Hairston.

ESTAFAS A PERSONAS NECESITADAS Y ABUELOS

Los malos actores pueden hacerse pasar por familiares o amigos en "persona necesitada" o Estafas de "abuelos". Los impostores pueden hacerse pasar por un nieto o por una agente de la ley oficial que ha detenido al nieto del objetivo. También pueden usar la IA para clonar la voz de alguien que la persona sabe que afirma que está en problemas y necesita dinero para ayudar con 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 ellos envíen dinero. Esquemas similares pueden usar las voces de sobrinas, sobrinos, hijos u otras personas.

BANDERAS ROJAS

Las señales comunes de que puede estar enfrentando este tipo de estafas incluyen:

- La persona al otro lado de la línea le pide que envíe dinero de inmediato y comparte detalles específicos sobre cómo hacerlo. Pueden sugerirle que envíe dinero a través de una tarjeta de regalo, una transferencia bancaria o criptomonedas.
- El "nieto" o el "agente de la ley" al otro lado de la línea 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 alinea con el comportamiento típico de la persona que dice ser.

MEDIDAS PARA PREVENIR Y RESPONDER

- Cuelgue y llame al número de su familiar o amigo que sepa que es genuino para asegurarse de que estén a salvo.
- Si la persona dice ser un oficial de la ley, cuelgue y llame a la agencia de aplicación de la ley correspondiente para verificar la identidad de la persona y cualquier información compartida. Tenga en cuenta: las fuerzas del orden nunca se pondrán en contacto con un miembro de la familia para cobrar el dinero de la fianza en nombre de otra persona.
- Verifica la historia con familiares y amigos de confianza, incluso si te han dicho que la mantengas en secreto.
- Verifique la configuración de privacidad de sus redes sociales y limite la información que comparte en línea. Los delincuentes pueden intentar 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 enviaste dinero a un estafador a través de una transferencia bancaria, repórtalo al IC3 del FBI dentro de las 72 horas posteriores a la transferencia en ic3.gov. Es posible que puedan ayudarlo a recuperar algunos de sus fondos perdidos.

MÁS INFORMACIÓN

- Para manejar 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
- Un anuncio de servicio público sobre estas estafas se puede ver en https://www.napsa-now.org/wp-content/uploads/2024/03/NAPSA-March-2024-Scam-Forum-Resources.pdf
- Para obtener más información sobre cómo se usa 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

USURPACIÓN DE IDENTIDAD Y FRAUDE DE SERVICIOS FINANCIEROS

Los estafadores pueden hacerse pasar por empresas de servicios financieros, como bancos, cobradores de deudas o servicios hipotecarios. Por ejemplo, los estafadores pueden hacerse pasar por cobradores de deudas e intentar engañar a sus víctimas para que paguen deudas que no existen. Pueden acosar o amenazar a sus víctimas con sanciones o penas de cárcel si se niegan a pagar. Las estafas de alivio hipotecario involucran promesas relacionadas con el refinanciamiento y mentiras sobre los términos de un préstamo. Según la FTC, en 2024, se reportaron más de 218,700 casos de fraude de cobro de deudas y más de 34,100 casos de fraude hipotecario.

VÍCTIMA DE ESTAFA

Milan Jackson
Sobreviviente de la estafa de suplantación de identidad de servicios financieros
Chicago, Illinois.
Luchando por contar lo que le sucedió, Milan Jackson ha optado por hablar, con la esperanza de advertir a otros sobre el malvado plan. La estilista de North Side dijo que todo comenzó hace unos meses, cuando su teléfono comenzó a sonar mientras trabajaba con un cliente.

Contesto el teléfono, y era un hombre que me decía: 'Este es el Bank of America', y que había actividad sospechosa", recordó Jackson. Jackson dijo que miró el reverso de su tarjeta de Bank of America y verificó que el número de teléfono de la tarjeta coincidía con el número de la persona que llamó. Dijo que el hombre al teléfono le informó que un pirata informático estaba tratando de robar $ 20,000 de su cuenta, y que necesitaban actuar rápido para evitar que sucediera.

"Muy molesto. Solo estoy tratando de darme prisa y asegurarme de que no puedan obtener ese dinero, porque había reservado dinero para abrir un negocio", dijo Jackson. "Luego me transfieren y me explican cómo detener potencialmente el fraude".

Le dijeron que iniciara sesión en su cuenta y transfiriera $20,000 a una cuenta diferente donde su dinero estaría protegido. Jackson procedió con el cable.

CUIDADO: ESTAFAS DE PHISHING

Las estafas de phishing engañan a las personas para que revelen información confidencial haciéndose pasar por organizaciones o empresas legítimas. Los estafadores utilizan correos electrónicos, mensajes de texto o sitios web falsos para imitar los reales, instando a tomar medidas inmediatas a través de enlaces o archivos adjuntos. Los datos robados 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 o desconocidos, evite los enlaces sospechosos y utilice contraseñas seguras y únicas.

BANDERAS ROJAS

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

Fraude de robo de identidad bancaria

- Recibe un mensaje de texto, una llamada telefónica o un correo electrónico que indica que la información de su cuenta se ha visto comprometida. Es posible que le pidan información personal como nombres de usuario, contraseñas, PIN y números de Seguro Social para "proteger" su cuenta. También pueden pedirte que transfieras fondos utilizando una aplicación de pago P2P, como Cash App, PayPal, Venmo o Zelle.
- Los bancos nunca se comunicarán con usted y le pedirán que comparta 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 de cobro de deudas

- La persona que lo llama le 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 suficiente tiempo para pagar su deuda y trabajarán con usted. 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 llenadas por el estafador después de que usted haya firmado.
- Se le presiona a pagar por adelantado antes de obtener cualquier servicio.

MEDIDAS PARA PREVENIR Y RESPONDER

Fraude de suplantación de identidad bancaria

- Los estafadores pueden "falsificar" su identificador de llamadas o falsificar la información transmitida a su identificador de llamadas, para que oculte su identidad o les permita hacerse pasar por una persona o empresa.
- No haga clic en enlaces inesperados ni responda a textos inesperados.
- Si recibe una llamada, un mensaje de texto o un correo electrónico sospechosos, cuelgue la llamada y no responda al mensaje de texto o 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 en el reverso de su tarjeta bancaria.

Fraude de deudas

- Pida una carta de validación de deuda por escrito. Los cobradores de deudas están obligados por ley a enviarle información detallada sobre la deuda que debe. Los estafadores se opondrán a esta solicitud.
- Pregúntele a la persona que lo llama el nombre del cobrador y el nombre de la agencia de cobranza de deudas para la que trabaja. Si dicen que están con la policía o con un abogado, entonces 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 hacer que firme se opone agresivamente a que consulte a un abogado, puede ser un estafador.
- Asegúrese de leer detenidamente todos los documentos antes de firmar. Si tiene preguntas, pídale a la persona que intenta que firme. Si hacen a un lado sus preocupaciones, pueden 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 Americana de Banqueros 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 https://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

SOPORTE TÉCNICO Y ESTAFAS INFORMÁTICAS

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

En una estafa similar, la víctima prevista puede ver una ventana emergente en la pantalla de su computadora que describe una amenaza de seguridad e instruye que llame a un número de un agente de soporte técnico que es un estafador. Los estafadores de este tipo pueden utilizar una variedad de métodos para ganarse la confianza de la víctima, en algunos casos incluso ofreciendo descuentos para personas mayores en su software antivirus. El objetivo de esto es obtener acceso a cuentas bancarias e información confidencial.

Si sospechas que esto te está pasando, DEJA DE HACER LO QUE ESTÁS HACIENDO. DESCONÉCTATE CON EL PRESUNTO ESTAFADOR Y APAGA TU COMPUTADORA DE INMEDIATO.

INFORMES DE LA LÍNEA DIRECTA DE FRAUDE

Una mujer de Georgia llamó a la línea directa de fraude del Comité para informar que perdió $25,000 en una estafa de soporte técnico. La persona que llamó informó que su computadora se había congelado y apareció una ventana emergente, lo que la llevó a llamar, lo que creía que era el número de soporte técnico de Microsoft. La persona que llamó marcó el número para pedir ayuda y los estafadores pudieron robarle miles de dólares.

BANDERAS ROJAS

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

- Recibe una alerta que dice que hay un virus en su teléfono o computadora y que debe llamar al número proporcionado para resolver el problema.
- Un estafador dice que la única solución para proteger su dinero o datos personales del "hacker" es transferirles los fondos de su cuenta mientras se deshacen del supuesto virus.
- Si dice que preferiría solucionar el problema yendo a una tienda física o llamando a una empresa diferente, la persona que llama intenta convencerlo de que el virus es urgente y que solo ellos pueden ayudarlo.

MEDIDAS PARA PREVENIR Y RESPONDER

- Si recibe una alerta que dice que su teléfono o computadora tiene un virus, no llame al número proporcionado en la alerta. En su lugar, llame al número oficial de soporte técnico de su dispositivo (por ejemplo, Apple o Microsoft).
- Si una persona te llama diciendo que tu dispositivo ha sido hackeado o comprometido por un virus, cuelga y bloquea su número de teléfono.
- Nunca proporcione información personal o financiera a una persona que llame inesperadamente.
- No concedas acceso remoto a un dispositivo o cuenta a menos que primero te pongas en contacto con esa empresa y sepas que es legítimo.
- 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 las estafas de soporte técnico en https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams.

ESTAFAS DE IMPOSTORES DEL GOBIERNO

En las estafas de impostores gubernamentales, los malos actores 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 los beneficios de una persona, 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 estafas más comunes de este tipo reportadas tanto a la Línea Directa de Fraude del Comité como a la FTC en 2024 . Según la FTC, las víctimas perdieron $789 millones debido a estafas de impostores del gobierno el año pasado.

INFORMES DE LA LÍNEA DIRECTA DE FRAUDE

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

BANDERAS ROJAS

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

- Recibe una llamada telefónica, un mensaje de texto o un 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 sus beneficios, le pide que transfiera dinero, que deposite dinero en una tarjeta de débito prepagada o una tarjeta de regalo, o le dice que envíe efectivo o cheque utilizando un servicio de entrega al día siguiente. También pueden pedirle que pague con criptomonedas o a través de una aplicación de pago P2P. Se le presiona para que decida de forma rápida y urgente.

MEDIDAS PARA PREVENIR Y RESPONDER

- Cuelgue el teléfono o no responda al correo electrónico o mensaje de texto recibido.
- Nunca dé ni confirme información financiera u otra información confidencial en respuesta a llamadas inesperadas, o si es sospechoso.
- No confíes inherentemente en un nombre o número. Los estafadores pueden usar nombres que suenan oficiales para que confíes en ellos. Para hacer que su llamada parezca legítima, los estafadores 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 o 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 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 https://consumer.ftc.gov/consumer-alerts/2020/10/how-spot-avoid-and-report-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 a menudo se hacen pasar por posibles parejas románticas, ganándose la confianza de las víctimas con el tiempo a través de comunicaciones frecuentes y declaraciones de afecto. Una vez que se establece la confianza, el estafador generalmente inventa una crisis o una necesidad urgente de dinero, como gastos médicos, costos de viaje o inversiones, persuadiendo a la víctima para que 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 están muy extendidas en los sitios web de citas, las plataformas de redes sociales, las aplicaciones de mensajería y los foros en línea. La conciencia y la precaución son cruciales para reconocer las señales de engaño y protegerse de los daños emocionales y financieros. La FTC informa que más de 59,000 [GC(S1] consumidores informaron que fueron víctimas de estafas románticas en 2024, con pérdidas reportadas por un total de más de $1.17 mil millones.

INFORMES DE LA LÍNEA DIRECTA DE FRAUDE

Una mujer de Ohio llamó a la Línea Directa de Fraude para informar que, durante los últimos dos años, ha sido víctima de una estafa romántica que le ha costado $40,000.

BANDERAS ROJAS

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

- La persona nunca te llama por videollamada ni te conoce en persona.
- No compartes amigos en común con ellos en las redes sociales y su identidad es difícil de rastrear en línea.
- Afirman estar enamorados de ti antes de conocerse en persona.
- Planean visitarte, pero siempre tienen una excusa de por qué no pueden que surge en el último minuto.
- Solicitan que el dinero se envíe a través de criptomonedas, transferencia bancaria, aplicación de pago P2P o tarjeta de regalo.

MEDIDAS PARA PREVENIR Y RESPONDER

- Si la persona siempre se niega a hacer una videollamada o reunirse en persona, bloquéela.
- Nunca envíes dinero o regalos a alguien que no hayas conocido en persona.
- Habla con tu familia y amigos, o con alguien en quien confíes, para que te aconsejen.
- Comunícate con tu banco de inmediato si crees que puedes haber enviado 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 EE. UU. brinda consejos sobre cómo evitar las estafas románticas en https://www.secretservice.gov/investigations/romancescams
- La FTC proporciona información y recursos de presentación de informes en https://consumer.ftc.gov/articles/what-know-about-romance-scams

OTRAS ESTAFAS COMUNES

SORTEOS Y ESTAFAS DE LOTERÍA

Las estafas de sorteos y loterías explotan las esperanzas de las personas de ganar un gran premio en efectivo engañándolas haciéndoles creer que han ganado un concurso en el que nunca participaron. Los estafadores a menudo se comunican 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. Estos esquemas fraudulentos manipulan la emoción y el deseo de obtener ganancias financieras, instando a las víctimas a proporcionar información personal o enviar dinero, solo para desaparecer una vez que se realiza el pago. La concienciación y la precaución son cruciales para evitar ser víctima de estas prácticas engañosas, ya que las transacciones financieras realizadas suelen ser irrecuperables y dejan a las víctimas devastadas financiera y emocionalmente. En 2024, la FTC descubrió que las víctimas reportaron más de $350 millones en pérdidas por estafas relacionadas con premios, sorteos y loterías.

INFORMES DE LA LÍNEA DIRECTA DE FRAUDE

Una mujer de Pensilvania informó que fue contactada por un estafador que afirmó que había ganado la lotería. El estafador le dijo a la mujer que para reclamar el premio, tenía que pagar 800 dólares.

BANDERAS ROJAS

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

- 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 has ganado un premio trata de convencerte de que la familia y los amigos preocupados están celosos o equivocados.
- Se le pide que pague el "impuesto" o la "tarifa de procesamiento" mediante una transferencia de dinero 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").

MEDIDAS PARA PREVENIR Y RESPONDER

- Si recibe una llamada que dice que ha ganado un premio y la persona que llama menciona un "impuesto" o una "tarifa", anote el número, cuelgue y bloquee el número.•No responda a cartas, mensajes de texto o correos electrónicos que digan que ha ganado un premio, especialmente si mencionan un "impuesto" o una "tarifa" para reclamar.
- 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

- La Oficina de Buenas Prácticas Comerciales (BBB, por sus siglas en inglés) ofrece 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 loterías en https://consumer.ftc.gov/articles/fake-prize-sweepstakes-and-lottery-scams

ESTAFAS DE INVERSIÓN Y OTRAS OFERTAS FALSAS DE "HÁGASE RICO RÁPIDAMENTE"

A través de las estafas de inversión, los estafadores se jactarán de la posibilidad de obtener altos rendimientos con poco esfuerzo y poco riesgo de su parte, si invierte en una nueva oportunidad, como criptomonedas, bienes raíces o metales preciosos. Las estafas de inversión pueden comenzar 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 el estafador construyendo una relación con su víctima. Una vez que el estafador tiene la confianza de la víctima, la alentará a invertir, al tiempo que garantiza altos rendimientos sin riesgos. Según la FTC, en 2024, las estafas de inversión fueron las estafas más costosas para los adultos mayores, con pérdidas reportadas que superaron los $5.6 mil millones. El principal método de contacto fueron las plataformas de redes sociales, y el principal método de pago fue la criptomoneda.

INFORMES DE LA LÍNEA DIRECTA DE FRAUDE

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

CUIDADO: ESQUEMAS PIRAMIDALES

Los esquemas piramidales también son un tipo de estafa de inversión. Los esquemas piramidales se presentan como oportunidades de trabajo 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. A menudo, se requiere que los participantes inviertan por adelantado, creyendo que obtendrán ganancias sustanciales. Los esquemas piramidales se basan en el reclutamiento continuo por parte de los participantes, donde los participantes persuaden a amigos y conocidos para que se unan. Si bien los primeros participantes pueden recibir pagos de las tarifas pagadas por los nuevos reclutas, los esquemas piramidales son insostenibles e inevitablemente colapsan, dejando a la mayoría de los participantes con pérdidas financieras. Estos esquemas explotan el deseo de las personas de obtener una riqueza rápida, ofreciendo falsas esperanzas de éxito financiero sin oportunidades de ingresos legítimas. Las autoridades de todo el mundo clasifican los esquemas piramidales como fraudulentos y advierten contra la participación para evitar dificultades financieras y consecuencias legales.

CUIDADO: ESTAFAS DE INVERSIÓN EN CONFIANZA

Las estafas de inversión en confianza, también conocidas como "estafas de carnicería de cerdos", involucran a estafadores que cultivan una relación falsa en línea con sus víctimas para ganarse la confianza y convencerlas de que inviertan en lo que creen que es una buena oportunidad de inversión, pero en realidad es un esquema fraudulento. El término "matanza de cerdos" fue acuñado por los propios estafadores y se refiere a la práctica de "engordar" a la víctima con atención y cariño antes de "masacrarla" económicamente. Los estafadores a menudo se hacen pasar por posibles parejas románticas o nuevos amigos y convencen a sus objetivos de invertir en plataformas de criptomonedas falsas u otras oportunidades financieras falsas. Una vez que la víctima invierte dinero, el estafador desaparece con los fondos, dejando a la víctima financieramente devastada y emocionalmente traicionada. 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.

BANDERAS ROJAS

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

- El estafador promete grandes ganancias a corto plazo o rendimientos financieros con poco esfuerzo.
- Te presionan para que actúes rápidamente diciéndote que podrías perder la oportunidad de ganar a lo grande.
- El estafador afirma que hay poco riesgo para la inversión y rendimientos garantizados. Esto es una estafa. Todas las inversiones conllevan el riesgo de que pierdas dinero.
- Dan algunos detalles sobre la inversión que están anunciando. 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 trabajos legítimos no requieren que pagues para trabajar.
- Los esquemas piramidales enfatizan el reclutamiento de otros en el esquema en lugar de vender productos o servicios genuinos a los clientes. Si el objetivo principal es reclutar nuevos miembros y ganar comisiones de sus inversiones o membresías, es probable que se trate de un esquema piramidal.

MEDIDAS PARA PREVENIR Y RESPONDER

- No inviertas dinero basándote en los consejos de alguien que solo has conocido en línea o a través de una aplicación.
- Tenga cuidado con las ofertas no solicitadas. Siempre sea escéptico con las llamadas, mensajes de texto, correos electrónicos o mensajes de redes sociales no solicitados de contactos no reconocidos.
- No te apresures a invertir. Si se trata de una inversión legítima, seguirá estando disponible.
- Verifique las credenciales y verifique de forma independiente cualquier información que se le proporcione o estados de cuenta que se le muestren. La mayoría de las estafas de inversión involucran a actores no registrados.
- Conoce tus 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, amigo o colega 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 https://reportfraud.ftc.gov/
- Presentar una queja ante la Comisión de Bolsa y Valores de EE. UU. (SEC) en https://www.sec.gov/submit-tip-or-complaint/tips-complaints-resources/report-suspected-securities-fraud-or-wrongdoing

MÁS INFORMACIÓN

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

ESTAFAS DE CUIDADO DE SALUD Y SEGUROS DE SALUD

Las decisiones sobre la cobertura de atención médica y seguro pueden ser complejas. Los estafadores se aprovechan de esta complejidad haciéndose pasar por el programa Medicare, los planes de seguro médico comerciales y los proveedores de atención médica, o vendiendo "planes de salud con descuento" que no brindan suficiente cobertura. También pueden solicitar información personal o financiera "a cambio" de beneficios. La Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) encuentra 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 anualmente de octubre a diciembre. En 2024 se confirmaron 79,9 millones de dólares en pérdidas debidas a estafas sanitarias, pero se estima que la cifra real es mucho mayor, ya que es más probable que estas pérdidas no se denuncien.

INFORMES DE LA LÍNEA DIRECTA DE FRAUDE:

Una persona que llamó desde Maryland fue contactada por un estafador que se hizo pasar por Capital One. Afirmaron que tenía un saldo de $5,600 de hace un año.

BANDERAS ROJAS

Estas son señales comunes de que puede estar enfrentando 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. 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. Esto es una estafa. Mientras permanezca inscrito en Medicare y pague su prima mensual, su tarjeta de Medicare no vencerá.
- Se le solicita por llamada, 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 "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 pregunta sobre detalles específicos relacionados con la cobertura de seguro que la persona está vendiendo.

MEDIDAS PARA PREVENIR Y RESPONDER

- Nunca dé información personal por teléfono.
- Revise detenidamente todas las facturas médicas para detectar cualquier servicio que no haya recibido. Comunícate con tu proveedor de seguros para hablar sobre ello.
- Visita 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 de salud y si el vendedor afirma que el plan se proporciona a través de una aseguradora importante, confirme directamente con esa aseguradora.
- Los servicios que ofrecen ayuda legítima con el Mercado de Seguros Médicos, a veces llamados "navegadores" o "asistentes", no le cobrarán. Ve a www.healthcare.gov/find-assistance/directly 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 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 adicional y consejos en consumer.ftc.gov/articles/spot-health-insurance-scams
- La FCC tiene más información sobre las estafas de Medicare en https://www.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 EE. UU. (HHS, por sus siglas en inglés) mantiene una extensa lista de información sobre prevención de estafas en https://oig.hhs.gov/fraud/consumer-alerts/

ESTAFAS DE VIAJES, VACACIONES Y TIEMPO COMPARTIDO

Las estafas de viajes, vacaciones y tiempo compartido explotan el deseo de las personas por el lujo asequible y la relajación. Estas estafas generalmente comienzan con ofertas tentadoras de viajes gratis, paquetes de vacaciones con grandes descuentos u ofertas exclusivas de tiempo compartido, a menudo entregadas a través de llamadas telefónicas no solicitadas, correos electrónicos o anuncios llamativos en línea. Los estafadores persuaden a las víctimas para que paguen tarifas por adelantado por la reserva, los impuestos o la membresía, prometiendo un valor increíble que no 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 presionar a las personas a comprar propiedades vacacionales, a menudo bajo falsos pretextos o con términos engañosos. Una vez atrapadas en un contrato de tiempo compartido, las víctimas a menudo descubren que escapar del acuerdo es casi imposible, enfrentando tarifas de mantenimiento continuas, evaluaciones especiales y la falta de mercado de reventa. Los supuestos beneficios de la propiedad de tiempo compartido, como la flexibilidad y el ahorro de costos, a menudo se evaporan, dejando a los propietarios con una carga financiera significativa y sin una salida fácil. Esto puede convertir lo que estaba destinado a ser unas vacaciones de ensueño en una pesadilla financiera a largo plazo.

INFORMES DE LA LÍNEA DIRECTA DE FRAUDE

Una mujer en Florida llamó a la línea directa y explicó que le habían prometido un plan de tiempo compartido con cero por ciento de financiamiento. Ella no ha podido usar su plan y se ha quedado con extensas tarifas ocultas. No ha podido cancelar su plan de tiempo compartido.

BANDERAS ROJAS

Los estafadores de vacaciones y tiempo compartido a menudo emplean estas tácticas:

- Tenga cuidado con las ofertas inesperadas o las tácticas de venta agresivas que lo empujan a tomar decisiones rápidas sin una investigación o consulta adecuadas.
- 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 oscurecen los verdaderos costos y condiciones de los acuerdos de tiempo compartido. Siempre revise los contratos cuidadosamente y busque asesoramiento profesional si es necesario.

MEDIDAS 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 tarifas iniciales para 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 legal o financiero antes de firmar cualquier contrato.
- Si se siente apurado o presionado a tomar una decisión financiera costosa, dé un paso atrás y reconsidere. Las ofertas legítimas le proporcionarán tiempo suficiente para pensar las cosas.
- Denuncie cualquier llamada, correo electrónico o correspondencia sospechosa 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 tiempo compartido en https://consumer.ftc.gov/articles/timeshares-vacation-clubs-and-related-scams

ROBO DE IDENTIDAD

Las estafas de robo de identidad se producen cuando un mal actor obtiene y utiliza indebidamente los datos personales de otra persona para su propio beneficio. Un objetivo común para el robo de identidad incluye el acceso no autorizado a la cuenta bancaria de una persona. También puede incluir el robo de números de Seguro Social, la dirección personal de una persona o incluso información de atención médica. Los estafadores pueden retirar dinero, ingresar solicitudes falsas de préstamos o intentar reclamar beneficios como el Seguro Social o el desempleo en nombre del adulto mayor. En el 2024, AARP descubrió que los estadounidenses perdieron $47 mil millones debido al robo de identidad.

INFORMES DE LA LÍNEA DIRECTA DE FRAUDE

Un hombre 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 energía.

BANDERAS ROJAS

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

- Recibe una llamada o un mensaje no solicitado solicitando información personal.
- Nota actividad inusual y desconocida 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 recibió o tiene condiciones de salud inexactas enumeradas en sus expedientes médicos.
- No recibes beneficios, como el Seguro Social o un reembolso de impuestos, a pesar de que tu cuenta diga que los fondos fueron enviados.

MEDIDAS PARA PREVENIR Y RESPONDER

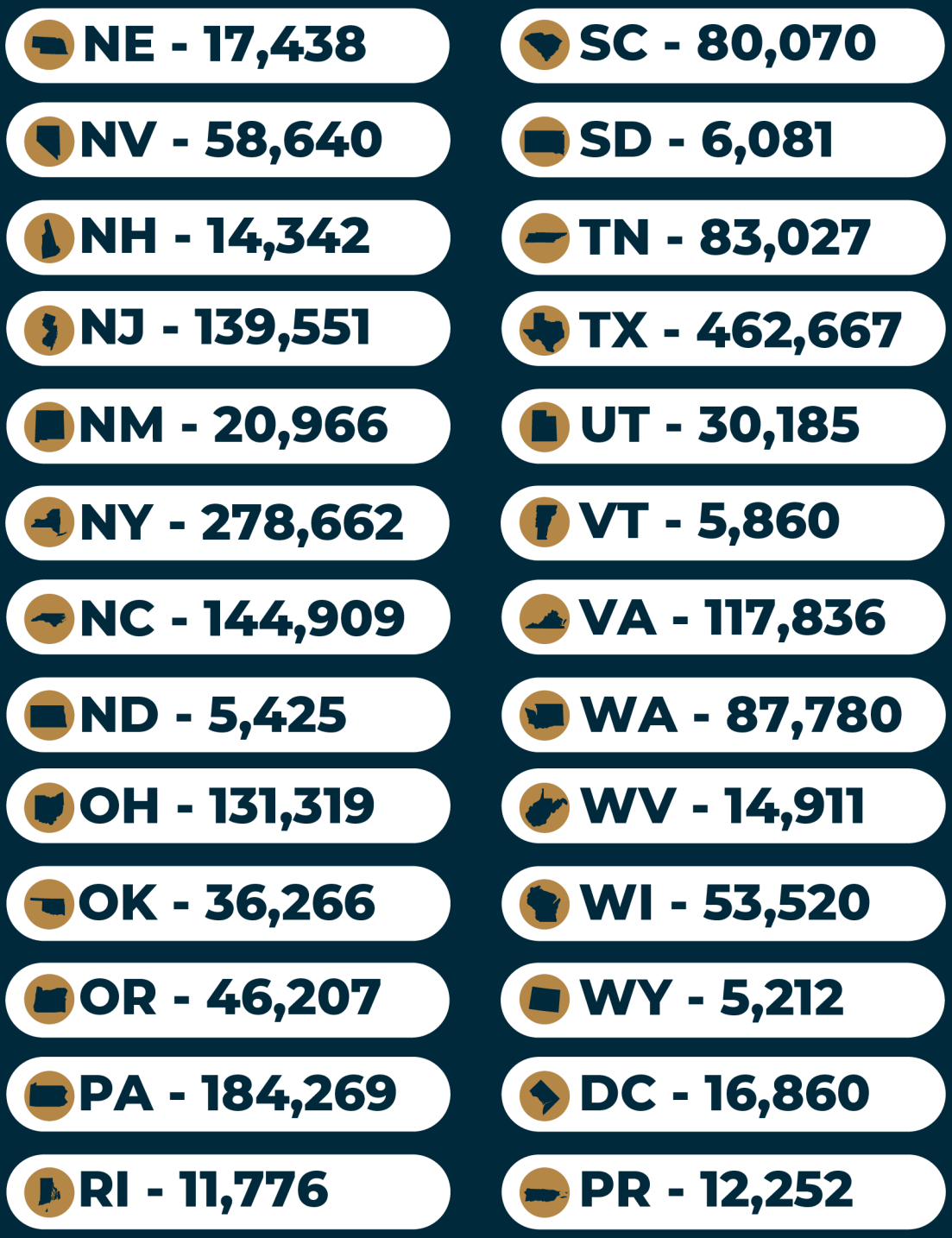
- Si alguien le pide su número de Seguro Social o información personal por teléfono, cuelgue. Si afirman ser de una empresa o agencia legítima, vaya al sitio web oficial de esa organización y llame a su línea oficial para verificar.
- No haga clic en enlaces de correo electrónico ni abra archivos adjuntos, incluso si el mensaje parece ser de una empresa que conoce. Si lo hace, puede poner en riesgo su información personal. Si desea visitar el sitio web oficial en el correo electrónico, hágalo manualmente en una pestaña de búsqueda separada.
- Actualice sus contraseñas, especialmente si sospecha o se entera de que su banco o compañía de tarjetas de crédito fue violada. No use la misma contraseña en todas las cuentas y use identificadores únicos al crear nuevas contraseñas.
- Suscríbase a las alertas de texto y 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

NÚMERO DE QUEJAS REPORTADAS A LA FTC EN 2024, POR ESTADO:

- AL - 70,132
- AK - 7,279
- AZ - 106,023
- AR - 29,453
- CA - 506,727
- CO - 73,231
- CT - 43,890
- DE - 18,870
- FL - 474,314
- GA - 228,132
- HI - 14,163
- ID - 16,080
- IL - 186,426
- IN - 72,938
- IA - 22,855
- KS - 24,924
- KY - 38,739
- LA - 68,025
- ME - 12,106
- MD - 111,041
- MA - 81,434
- MI - 117,326
- MN - 51,773
- MS - 36,023
- MO - 72,120
- MT - 9,651



Nota: El número representa el total de denuncias de fraude, robo de identidad y otras denuncias a la Red Centinela del Consumidor 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 etiquetados en los 50 estados, el Distrito de Columbia o Puerto Rico.

RECURSOS

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

MENSAJES DE TEXTO

Los estafadores suelen utilizar las 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 trabajo. Los estafadores 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 supuestamente destinado a otra persona o de alguien que dice conocerlo. Los destinatarios de los mensajes de texto con un "número equivocado" a menudo responden por cortesía o curiosidad. Luego, el estafador usa esa respuesta inicial para construir una conexión, lo que lo hace más susceptible a estafas como estafas románticas o estafas 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 al mensaje. Si crees que el mensaje de texto es legítimo, comunícate directamente con la empresa; No utilice la información de contacto proporcionada en el mensaje de texto.
- Si recibes un mensaje de texto que crees que podría ser una estafa, bloquea el número para que no puedan volver a comunicarse contigo. No responda porque, si lo hace, podría recibir más mensajes de texto de los estafadores.
- No pague para que le vuelvan a entregar un paquete. Las empresas de entrega de paquetes nunca solicitarán el pago para volver a entregar un paquete.
- 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 a menudo anuncian ofertas que son "demasiado buenas para ser verdad". Los estafadores roban la información de la víctima, como un número de tarjeta de crédito, una vez que realizan la compra.

Las ventanas emergentes son una estrategia común utilizada por los estafadores de "soporte técnico", que se analiza anteriormente en este libro.

CONSEJOS PARA PROTEGERSE DE ANUNCIOS Y VENTANAS EMERGENTES FRAUDULENTOS EN LÍNEA:

- No haga clic en ningún enlace de ventanas emergentes del sitio web y anuncios en línea. Para visitar un sitio web, escriba la dirección del sitio web directamente en el navegador.
- Ten cuidado con los anuncios que veas en las redes sociales, ya que podría tratarse de una estafa.
- Haz una copia de seguridad de tus 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.
- No descargues software de sitios que no conozcas.
- 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 plataformas de redes sociales son uno de los métodos de contacto más comunes utilizados por los estafadores dirigidos a los adultos mayores en línea. Ofrecen a los estafadores la oportunidad de acceder a datos personales y ganarse la confianza de la víctima.

Según la FTC, entre 2020 y 2023, las víctimas perdieron más dinero por estafas que se originaron en las redes sociales que por cualquier otro método de contacto.

CONSEJOS PARA PROTEGERSE DE LOS MALOS ACTORES EN LAS REDES SOCIALES:

- Asegúrate de usar una contraseña segura y una configuración de privacidad que oculte información como tu ciudad, número de teléfono y fecha de nacimiento.
- No aceptes solicitudes de amistad de extraños, de alguien que ya tengas como "amigo" en las redes sociales o de alguien que conozcas que no use las redes sociales.
- No hagas clic en enlaces de amigos con los que normalmente no te comunicas. Estos enlaces suelen ser a un sitio web para reclamar un premio, realizar un cuestionario, completar una encuesta o ver un vídeo.
- Si recibes 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. Confirma con ellos en otra plataforma o reúnete con ellos en persona para verificar si crees que podría ser genuino. Tenga en cuenta: su cuenta puede haber sido pirateada, especialmente si le piden que envíe criptomonedas, tarjetas de regalo o

LLAMADAS

Las llamadas no deseadas y las llamadas automáticas son las principales quejas que recibe la FCC. Las llamadas automáticas se pueden realizar desde cualquier parte del mundo y, a menudo, contienen un mensaje de una 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 un número de una empresa con la que esté familiarizado.

- Contestas el teléfono y la persona que llama, o una grabación, te pide que pulses una tecla para dejar de recibir las llamadas. Los estafadores suelen utilizar este truco para identificar posibles objetivos.
- Recibes una consulta de alguien que dice representar a una empresa o agencia gubernamental. Cuando cuelga y llama al número de teléfono verificado de esa persona u organización, no tienen registro de haberlo llamado.
- Es posible que no pueda saber de inmediato si una llamada entrante es falsa. Tenga en cuenta: Si el identificador de llamadas 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 a aquellas que se pueden responder con un "sí".
- Nunca proporcione información personal, como números de cuenta, números de Seguro Social, nombres de soltera, contraseñas u otra información de identificación personal en respuesta a llamadas inesperadas, o si tiene alguna sospecha.
- Si sufres fraude o pérdidas monetarias por una llamada automática, comunícate 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 https://reportfraud.ftc.gov/

CORREO ELECTRÓNICO

Los estafadores suelen utilizar correos electrónicos de phishing para engañar a las personas para que revelen su información personal. Estos son algunos ejemplos de correos electrónicos que podrías recibir y que probablemente sean estafas:

- Un correo electrónico que afirma que necesita verificar o actualizar la información de su cuenta, dirigiéndolo a una página de inicio de sesión falsa.
  - No pongas tu información en esta página. Los estafadores pueden capturar su nombre de usuario y contraseña e iniciar sesión en el sitio real con su cuenta.
- Un correo electrónico que advierte de actividades sospechosas en tu cuenta y te insta a hacer clic en un enlace para protegerla.
  - No haga clic en enlaces ni descargue archivos adjuntos de correos electrónicos desconocidos o sospechosos.
- Un correo electrónico que le informa que ha ganado un premio o recompensa, pero debe proporcionar información personal o pagar una tarifa para reclamarlo.
- Un correo electrónico que crea una sensación de urgencia, indicando que su cuenta se bloqueará a menos que proporcione información confidencial de inmediato.
- Un correo electrónico contiene una factura o recibo inesperado y le pide que abra un archivo adjunto o haga clic en un enlace para revisarlo.

RECURSOS ADICIONALES DE AGENCIAS Y OTRAS ORGANIZACIONES

ESTAS ORGANIZACIONES Y SITIOS WEB PUEDEN SERVIR COMO UN RECURSO PARA LOS CONSUMIDORES Y PUEDEN INCLUIR INFORMACIÓN SOBRE OTRAS ESTAFAS COMUNES DIRIGIDAS A ADULTOS MAYORES QUE NO SE TRATAN EN ESTE LIBRO.

USA GOV
www.usa.gov/scams-and-fraud

BETTER BUSINESS BUREAU
www.bbb.org/scamtracker

AARP FRAUD WATCH NETWORK
www.aarp.org/fraudwatchnetwork

FEDERAL TRADE COMMISSION (FTC)
www.consumer.ftc.gov/scams

FEDERAL BUREAU OF INVESTIGATION (FBI)
www.fbi.gov/scams-and-safety/common-scams-and-crimes

También puede ponerse en contacto con su congresista o senador de EE. UU. Puede denunciar el fraude a su oficina, y es posible que ellos puedan ayudarlo. Para localizar a su miembro del Congreso usando su código postal, vaya a https://www.house.gov/representatives/find-your-representative. 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. HAY RECURSOS PARA AYUDARLO A RESPONDER Y RECUPERARSE DEL FRAUDE.

APOYO Y CONSEJERÍA A LAS VÍCTIMAS CENTRO DE RECURSOS VICTIM CONNECT

victimconnect.org

CORPORACIÓN DE SERVICIOS LEGALES DE AYUDA LEGAL

lsc.gov

OTROS SERVICIOS LOCALIZADOR DE CUIDADO DE ANCIANOS

https://www.usaging.org/eldercareloc

PROCURADURÍAS GENERALES DE JUSTICIA DEL ESTADO:

ALABAMA
(334) 242-7300

ALASKA
(907) 269-5602

SAMOA AMERICANA
(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) 577-8400

DISTRITO DE COLOMBIA
(202) 727-3400

FLORIDA
(850) 414-3300

GEORGIA
(404) 458-3600

GUAM
(671) 475-3324 EXT. 5020

HAWAII
(808) 586-1500

IDAHO
(208) 334-2400

ILLINOIS
(312) 814-3000

INDIANA
(317) 232-6201

IOWA
(515) 281-5164

KANSAS
(785) 296-2215

KENTUCKY
(502) 696-5300

LOUISIANA
(225) 326-6000

MAINE
(207) 626-8800

MARYLAND
(410) 576-6300

MASSACHUSETTS
(617) 727-2200

MÍCHIGAN
(517) 335-7622

MINNESOTA
(651) 296-3353

MISISIPI
(601) 359-3680

MISURI
(800) 392-8222

MONTANA
(406) 444-2026

NEBRASKA
(402) 471-2682

NEVADA
(775) 684-1100

NUEVO HAMPSHIRE
(603) 271-3658

NUEVA JERSEY
(609) 292-4925

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) 664-2341

OHIO
(614) 466-4320

OKLAHOMA
(405) 521-3921

OREGÓN
(503) 378-6002

PENNSYLVANIA
(717) 787-3391

PUERTO RICO
(787) 721-2900

RHODE ISLAND
(401) 274-4400

DAKOTA DEL SUR
(605) 773-3215

TENNESSEE
(615) 741-3491

TEXAS
(512) 463-2100

ISLAS VÍRGENES DE EE. UU.
(340) 774-5666 EXT.155

UTAH
(801) 538-9600

VERMONT
(802) 828-3171

VIRGINIA
(804) 786-2071

WASHINGTON
(360) 753-6200

VIRGINIA OCCIDENTAL
(304) 558-2021

WISCONSIN
(608) 266-1221

WYOMING
(307) 777-7841

TRES PASOS PARA AYUDARTE A TI MISMO Y AYUDAR A LOS DEMÁS

☑ Corre la voz:

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

☑ Denuncie la estafa:

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

☑ Mantente alerta y proactivo:

- Considere inscribirse para recibir alertas de su banco y/o compañía de tarjeta de crédito, o 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 se proporcionan en este libro.

COMITÉ ESPECIAL DEL SENADO DE EE. UU.

PARA ASUNTOS DE LA VEJEZ

LÍNEA DIRECTA DE FRAUDE

La Línea Directa de Fraude proporciona información para los estadounidenses mayores y sus familiares sobre cómo denunciar fraudes y estafas a los funcionarios correspondientes, incluidas las fuerzas del orden.

1-855-303-9470

LUN – VIE
DE 9 AM A 5 PM, HORA DEL ESTE

INFORMACIÓN IMPORTANTE QUE DEBE INCLUIR EN SU QUEJA:

¿Cuándo sucedió?
¿Cómo se pusieron en contacto con usted?
¿Qué te pidieron que hicieras?
¿Cuánto dinero le pidieron que proporcionara?
¿Cómo se le pidió que proporcionara el dinero?
¿Le informó este incidente a alguien más?
¿Se reembolsó parte del dinero que enviaste?
¿Hubo algún otro efecto (cuenta cerrada, robo de identidad)?

Descargo de responsabilidad: El Libro de Fraudes 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 ningún tercero. Es posible que haya otros recursos que también satisfagan sus necesidades.

NOTAS FINALES:

- **Fraud at a glance**
  - https://www.ic3.gov/AnnualReport/Reports
  - Financial Exploitation - NAPSA
  - [1]FinCEN Issues Analysis on Elder Financial Exploitation | FinCEN.gov
  - [1]FinCEN Joins Agencies in Issuing A Statement on Elder Financial Exploitation | FinCEN.gov
  - [1]https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/elder-fraud
  - [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 (Page 1)
  - [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 (Page 2)

- **How scammers are stealing people's money**
  - FBI Highlights Growing Number of Reported Elder Fraud Cases Ahead of World Elder Abuse Awareness Day — FBI
  - [1] https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts (Payment and Contact Methods)

- **Scams to watch out for**
  - FTC, Consumer Sentinel Network, All Fraud Reports by Payment Method, https:// public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/ PaymentContactMethods
  - Analysis of FTC data by Aging Committee staff. The analysis compares 2024 data to 2023 data. FTC data is available online at: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods
  - https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts (Top Reports)
  - https://www.usatoday.com/story/news/nation/2024/10/02/hurricane-helene-fraud-scams-theft/75459635007/ https://www.aging.senate.gov/hearings/modern-scams-how-scammers-are-using-artificial-intelligence-and-how-we-can-fight-back
  - The Big View: All Sentinel Reports | Tableau Public
  - https://abc7chicago.com/post/phantom-hacker-scam-fbi-issues-warning-chicago-hairstylist-milan-jackson-loses-20000-bank-america-impersonator/15804134/
  - https://www.seniorliving.org/research/common-elderly-scams/
  - https://public.tableau.com/app/profile/federal.trade.commission/viz/shared/4WS8HTYQ6
  - Fraud Reports | Tableau Public (1)

- **Other common scams**
  - Fraud Reports | Tableau Public (2)
  - Fraud Reports | Tableau Public (3)
  - Fraud Reports | Tableau Public (4)
  - Source: https://fred.stlouisfed.org/series/FYFSD

- **Scams by state**
  - https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/05/whos-who-scams-spring-roundup
  - https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts
  - chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf